Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

ICT IN THE CONTEXT OF CRIMINAL PROCEDURE: THE NETHERLANDS*

Tijs KOOIJMANS and Paul MEVIS[1]

1 Introduction

In this report, we aim to analyze (aspects of) the use of Information and Communication Technology (ICT) in the context of Dutch criminal procedure. The questionnaire underlying this report generally deals with cyber crime. 'Cyber crime' is understood to cover criminal conduct that affects interests associated with the use of ICT, such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offences concerning traditional computers as well as cloud cyber space and cyber databases.[2] Although the background of the questionnaire is related to cyber crime as a topic of substantive criminal law, it would not be expedient to narrow the focus of this report to the (legal) aspects of ICT in the context of criminal procedure insofar as it deals with specifically this type of crime. ICT (in the context of criminal procedure) is too broad a phenomenon to limit this report to cyber crime.

The use of ICT in criminal procedure in order to tackle criminal offences can take various forms. Investigation in criminals' computers will be made possible but, for instance, the interception of telecommunication, the access to a DNA-database and the use of ANPR-systems[3] can be brought under the broad description of ICT too. *Anno* 2013, one has to conclude that not many aspects of criminal procedure are imaginable which are not to some extent connected to ICT. From this point of view, writing a report about the use of ICT in criminal procedure might basically come down to writing a report about criminal procedure itself. Since this could not reasonably be the aim of a national report on this topic, we have chosen to rather strictly follow the questionnaire, in which the use of ICT in criminal procedure is somewhat narrowed down.[4]

In the next paragraphs, we'll sketch some characteristics of the Dutch law on criminal procedure (par. 2), we'll address the general questions of the questionnaire (par. 3), we'll pay attention to building information positions for law enforcement and we'll describe various aspects of ICT in the criminal investigation (par. 4), we'll search for rules on evidence that are specific for ICT-related information (par. 5). Furthermore, we'll describe the way ICT-related evidence should be introduced in the trial (par. 6). Finally, we'll draw some conclusions (par. 7).

2 Some characteristics of the Dutch law on criminal procedure

In this paragraph, we'll describe several characteristics of the Dutch criminal procedure, in order to subsequently be able to give an adequate overview of the various aspects of ICT in the criminal procedure.

The aim of Dutch criminal procedure is generally described in terms of 'assuring the correct application of substantive criminal law'. From this, it follows on the one hand that a guilty person should be convicted and punished, and on the other hand that the conviction and punishment of a person who is not guilty should be prevented.[5] Next to this main

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

[1] Prof.dr. T. Kooijmans is professor of criminal law at Tilburg University. Prof.dr. P.A.M. Mevis is professor of criminal law at Erasmus University Rotterdam.

[2] Definition derived from Association Internationale de Droit Pénal, Newsletter 1/2012, p. 33. For an overview of the specific cybercrime offences, we refer to the reports under Section 2.

[3] ANPR means Automatic Number Plate Recognition.

[4] See, a.o., B.J. Koops, 'Cybercrime Legislation in the Netherlands', in J.H.M. van Erp & L.P.W. van Vliet (eds.), *Netherlands Reports to the Eighteenth International Congress of Comparitive Law*, Antwerp: Intersentia 2010, p. 599-633.

[5] See, a.o., G.J.M. Corstens, *Het Nederlands strafprocesrecht*, seventh edition, by M.J. Borgers, Deventer: Kluwer 2011, p. 6-11; B.F. Keulen & G. Knigge, *Strafprocesrecht*, twelfth edition, Deventer: Kluwer 2010, p. 2.

goal of criminal procedure, several 'side goals' are described in the literature.[6] Firstly, to respect the rights and freedoms of the suspected/accused person. Secondly, the aim of procedural justice. Thirdly, to respect the rights and freedoms of other people (than the accused person) involved in a criminal procedure, such as victims.

The system of criminal procedure should be equipped to achieve these goals. In this respect, a pivotal characteristic of the Dutch law on criminal procedure is its fundament of 'investigating and deciding'.[7] Let us elaborate on this. The Dutch Code of Criminal Procedure (CCP) has created a general legal framework within which a criminal case should be disposed. This framework consists of several, subsequent stages of the criminal procedure. This series of stages is in itself a logical one. A judge will not decide on a specific matter if the public prosecutor doesn't point out that he wishes a decision on the matter. The public prosecutor will not ask a judge for a decision about an accusation if the police haven't investigated the criminal case. In short: there is a close relationship between the actions of the authorities. Their actions are initiated by the actions of other authorities. The logical order of the different stages of the criminal procedure makes clear that the criminal procedure is a continuous process consisting of investigation. In each stage, the aim of the investigating activities is to enable another authority to decide on the case. For instance, in the pretrial stage, the police investigate a criminal case in order to enable the public prosecutor to decide whether or not to prosecute the suspect. When the police have finished their investigating activities, they'll send the case file – mainly consisting of police reports (*processen-verbaal*) – to the public prosecutor. It's this authority who has to decide about the next step in the procedure: the prosecution of the suspected person. This logical order of these different stages includes – to a certain extent – a system of accountability: authorities within the criminal system can be kept accountable for their actions by other authorities in the next stages of criminal investigation.

Just like the other stages of the criminal procedure, the pretrial stage is dominated by the principle of legality: article 1 CCP. A legal basis by statutory law is required for criminal proceedings. For this reason, many investigative methods are provided for by the CCP. However, not all investigative methods have an explicit basis in statutory law. For instance, the CCP contains a specific legal basis for the surveillance/systematic observation (*stelselmatige observatie*) of a person by the police.[8] Such a specific statutory provision lacks for a non-systematic, superficial observation of a person. This difference can be explained by the fact that, as a legal basis of investigation methods – such as the superficial observation of a person – which only cause a light interference with a person's privacy (the right to respect for private life), the statutory description of the statutory duty (*taak*) of the police to investigate criminal cases[9] suffices.[10] In other words, the power to create slight interferences with human rights (by police investigation) can be derived from the statutory duty of the police. When it comes down to rather grave interferences with the right to respect for private life, a specific basis by statutory act is required.[11] In addition, such a specific statutory basis is – at least – also required for investigation methods which bear great risks for the integrity and controllability of the investigation.[12] This state of affairs raises the question whether the online gathering of information about a person via open sources by the police requires a specific statutory basis. This question and comparable questions will be addressed in the next paragraphs.

Another – yet related to the before mentioned specificity of a statutory basis – characteristic of the Dutch system of criminal procedure, is the influence of the principles of subsidiarity and proportionality. The more far-reaching (investigating) powers are (to be) applied, the heavier the seriousness of the criminal offence has to be. Generally, 'heavy' powers may only be applied in relatively severe criminal cases. In connection with this: the heavier the power, the higher[13] – or even independent[14] – the authority has to be who orders its application.

---

[6] See, a.o., B.F. Keulen, *Het Nederlandse stelsel van rechtsmiddelen in strafzaken* (preadvies NVVS), Nijmegen: Wolf Legal Publishers 2012, p. 8.

[7] P.A.M. Mevis, *Capita Strafrecht*, seventh edition, Nijmegen: Ars Aequi Libri 2013, p. 128-129.

[8] See art. 126g, art. 126o and art. 126zd CCP.

[9] See art. 141 CCP, art. 3 Police Act 2012 and Hoge Raad (Supreme Court) 13 November 2012, *Landelijk Jurisprudentie Nummer* BW9338.

[10] That is: according to the jurisprudence of the Supreme Court, followed by the legislator. It is not undiscussed.

[11] See, a.o., T. Kooijmans, 'Een Tilburgse observatie van een Tilburgse observatie', *Ars Aequi* 2013, p. 222-229.

[12] Hoge Raad (Supreme Court) 20 December 2011, *Nederlandse Jurisprudentie* 2012/159 (with a comment by T.M. Schalken).

[13] E.g., it's the public prosecutor – and not a policeman – who has the power to order that a person be systematically observed: art. 126g CCP.

[14] E.g., it's the examining judge (*rechter-commissaris*) who needs to give a written authorisation to the public prosecutor to order extremely sensitive information (see below). It is also the examining judge whohas the power to orders that a suspect be remanded in custody for (at most) 14 days: art. 63 CCP.

3 ICT in the context of criminal procedure: definitions and institutions

3.1 An overview instead of a definition

What is Information and Communication Technology? At first sight, it seems very hard to give an adequate description of this very broad concept. Instead of searching for such a definition, a more fruitful approach might be to sketch several aspects of ICT that might be relevant for the criminal procedure. Koops has distinguished several trends in technology in relation to criminal investigation.[15] For the purpose of this report, it's expedient to describe this author's findings.

The first trend is the development of new kinds of data which are useful for the purpose of criminal investigation.

In the first place, new kinds of data arise which didn't exist in the past or which were not recorded. More and more objects can be identified by a unique number. Objects contain RFID-chips[16] through which they can be read out from a short distance and through which they can be identified. This reading out and identifying of objects will increase, not only in logistic chains but also for the purpose of criminal investigations because RFID-goods leave traces on the places where they are read out. When it comes down to developments in identification, the automatic number plate recognition (ANPR) of cars should also be pointed out, just like 'trusted computing' and computer finger prints enabling the recognition of computers and software. Printers generate specific patterns, so a print can be deduced to a unique printer. The same goes for pictures taken by a camera, and even paper can be recognized by its specific grain structure. In general, objects are better traceable because of their identifying codes.

The same goes for human beings. RFID-chips can be used not only to identify and trace Rolex-watches, but also playing children, demented elderly people, or released paedophile persons. Another aspect related to the use of new kinds of data are biometrics, creating the possibility to identify people from their iris, fingerprint, ear channel or other body marks. Starting at the age of 14, citizens in the Netherlands are obliged to (be able to) identify themselves.[17] Among others lawyers, banks, jewelers and art-dealers are obliged to check and register their clients' identity. People can be identified not only by direct identity-numbers but probably also by objects, like their unique watch or digital camera. Walking around anonymously is not self-evident anymore.

Another example of a new type of data is data disclosing a location.[18] Telecommunication networks 'know' in which network-cell a cell phone is situated. These networks can – via techniques like triangulation – determine where a person is situated within the network-cell. GPS-devices or Galileo-devices can determine their own place using satellites. Furthermore, access-points of WiFi and Bluetooth devices can be used to determine a location. The location of objects – and of people – can be determined closer and closer by the attraction of location-related services, such as the weather forecast on a cell phone. The (perception of) security is an important motive for location techniques. For instance, in the US cellphones have to be equipped with a 'location-determinator' in case the emergency number is dialed; in the Netherlands (reports concerning) location data are used as evidence in criminal cases and the police requires information about the cell phones which were near a crime scene in order to send everybody nearby an SMS for the purpose of finding witnesses. Not only telephones but also cars are objects the location of which can be determined. For instance, insurance companies require a built-in transmitter for expensive cars. Furthermore, 'chip cards' for public transport facilitate tracing the places in which passengers got on the bus or train and stepped out. Security cameras also record their moves. Next, proposals have been done to authenticate computers. Whereas the location of people and objects used to be determined via eyewitnesses, currently – as a consequence of the aforementioned developments – the determination can also take place automatically (and) from a distance.

Several other examples of new kinds of data require attention. Everybody who surfs the Net, leaves traces. The visited web pages give a significant overview of the visitor's interests. The Dutch legislator has prescribed that those data – being traffic data (*verkeersgegevens*) – may be claimed (from the telecom provider).[19] In order for this power to be effective, the providers are required (by statutory law) to save the data for several months.[20]

---

[15] B.J. Koops, *Tendensen in opsporing en technologie. Over twee honden en een kalf* (inaugural lecture Tilburg), Nijmegen: Wolf Legal Publishers 2006, p. 7-12 (with references). The following section was substantially derived from this source.

[16] RFID means Radio Frequency Identification.

[17] Section 2 of the Compulsory Identification Act (*Wet op de identificatieplicht*) requires every person aged fourteen or over to present an official identity document to a police officer upon first demand. Article 447e of the Criminal Code makes failure to do so a minor offence punishable by a second-category fine (i.e. not exceeding EUR 3900).

[18] Cf. A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2006, p. 126-128.

[19] See art. 126n and art. 126nd CCP.

[20] According to section 3 of art. 13.2a Telecommunication Act, data concerning telephones have to be saved for twelve months and data concerning access to internet and e-mail have to be saved for six months. See the Act of 6 July 2011, *Staatsblad* 2011, 350 and the Decrete of 11 August 2009, *Staatsblad* 2009, 350.

These data have a deeper impact on a person's privacy than a telephone number or the length of a call. Furthermore, DNA contains information which can be disclosed. This enables criminal investigators to deduce somebody's sex, geographic origin, the color of his hair and his eyes, from a trail of blood.

The recording and storage of data is the second reason why data are increasingly available for the purpose of criminal investigation. An important example is the surveillance by cameras in public areas and the storage of the records. The internet is another prominent example of the recording of data for, in principle, indefinite periods. Allegedly, Google files all searching orders. Considering the possibilities offered by Google to store one's personal searching history, it's getting easier (from a technical point of view) and more attractive (from a policy point of view) to claim – from Google – the searching history and centrally stored documents of a suspect. In general, the internet is a huge source of diverse (recorded) data. The results of the use of webcams (and cameras in cell phones) and digital conversations can easily enter the public domain. Copyrights of music and movies are under pressure because of the possibilities to copy and spread the files via internet. This caused a counter reaction of Digital Rights Management-systems. When a person listens to the radio on the internet, the length and the channel can be registered. Not only objects like computers, internet and cameras register data. Built-in tachographs measure both the period a car is driving and its speed. Navigation systems are able to keep up with the route.

Technical possibilities and 'the market' have given a big impulse to the recording of data and of the technical equipment to do so. This trend is boosted by criminal law and the law concerning the battle against terrorism. According to European law, storage of telecommunication data is mandatory.[21] A similar remark can be made about user data of telecommunication (who uses which telecom provider?). The registration agency of wired phones and cell phones – CIOT – has been extended to internet numbers like IP-addresses. Because IP-addresses change quicker than telephone numbers, it is being considered whether it should be exactly registered at which times they were used by which user.

It follows form this overview that ICT is such a broad phenomenon that it can hardly be described in a one-size-fits-all formula.

3.2 Institutions involved in the implementation of ICT within the criminal justice system

Both the police force, the public prosecution service and the judiciary use their own internal ICT-related systems in order to support the criminal law system.

At the level of the police organization, the nationwide unit of the National Police (*Landelijke Eenheid van de Nationale Politie*; before 1 January 2013: *Korps Landelijke Politiediensten (KLPD)*) renders supportive services for other police units. On a regional level, police units use various digital systems to store and disclose information. One of the aims of the establishment on 1 January 2013 of the National Police, is to improve the cooperation between police forces when it comes down to computerization.[22]

The Dutch public prosecution service uses the so-called COMPAS/GPS-system in order to, among other things, store data concerning criminal cases and prepare the drafting of indictmens. The computerized support of the Dutch judiciary is carried out by Spir-it.[23] Criminal cases (and also cases of civil law and administrative law) can be introduced digitally by the parties. The electronic case file (*elektronisch dossier*) was introduced (see further below, par. 6.3). In addition, Spir-it makes it possible to track cases via internet. Another example of the computerized support that's given to the judiciary is the database for consistent punishment (*Databank Consistente Straftoemeting,* in the near future modernized to *'Gegevensbank Informatie over de Straftoemeting' (GIDS)*). This database consists of judicial verdicts of Courts of Appeal in which imprisonment of more than four years was imposed, and its aim is to facilitate the comparison of the concrete, current criminal case with the cases which have been stored in the database in order to impose an appropriate sentence.

---

[21] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ EU* L105/54, 13 April 2006.

[22] A few other organisations are hosted by *KLPD*. One of these organisations is Team High Tech Crime (THTC). In 2006, the Dutch government produced broader and less incident-focused analyses in the memorandum 'Draft National Infrastructure Fighting Cybercrime'. In this memorandum the following issues were indentified: inadequate (scientific) knowledge about the nature and extent of the problem and about the modalities to effectively combat it, ambiguities in the division of tasks between cooperation partners, a shortage of (operational) knowledge at investigative agencies and lack of urgency perception. In order to overcome these problems, a National High Tech Crime Center (NHTCC) and a reporting point (hotline?) for Cyber Crime were established at the police organisation. See.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012', *Justitiële verkenningen* 2012-1, p. 31.

[23] http://www.rechtspraak.nl/Organisatie/spir-it/Over-spir-it/Pages/default.aspx.

A prominent example of joint forces – from a point of view of ICT – is the nationwide Internet Research and Investigation Network (the iRN system).[24] This network – stemming from the Police, the National Combating Terrorism Coordinator, the Netherlands Forensic Institute (NFI) and the Tax Authorities – has become independent in 2012. Its aim is to let iRN grow domestically and internationally. The iRN enables Dutch investigative and supervising authorities to conduct investigative research and intelligence research on the internet in a forensically safeguarded way. Obtained evidence can be used in criminal proceedings. The iRN strengthens the cooperation between the aforementioned authorities by enabling them to share their knowledge swiftly and secure. There are currently 700 iRN workplaces which can be used by 4500 persons. In the coming years, iRN will be expanded via the so-called iColumbo-project.[25] Within this project, software tools are being developed that support the users with tracking and analysing relevant information on the internet. Appropriate tools from other sources will be made available via iRN as well.

One of those tools is XIRAF.[26] The amount of data that needs to be processed in a typical criminal investigation today – especially when fraud, murder or child pornography are involved – is immense and extremely diverse. Processing and analyzing all this complex data is difficult and time-consuming, and in the sheer mass of data, investigators may miss or lose track of important evidence. In addition, they are often under pressure from enforcement agencies to complete their analysis as quickly as possible. To enable faster and more effective processing of data within criminal investigations, the NFI has therefore developed XIRAF, an advanced software application that can automatically analyse large quantities of data from all types of equipment at high speed and render them directly searchable (data mining[27] and data matching). Specifically, XIRAF bundles data from digital sources, including laptops, external hard drives, mobile phones and CDs, into a central online database. Within the iRN-network, police or government investigators can then access and search this database from anywhere – all they need is a web browser. XIRAF also makes it possible to order data chronologically and sort images geographically. XIRAF is currently used by various police and investigative services and has proved its value in several criminal cases.

3.3 Private organizations that offer ICT related services to the criminal justice system

ICT-related services to the criminal justice system are primarily offered by agencies that belong to the specific institutions such as the police, the public prosecution service and the judiciary. The National Police Computer Center (*Landelijk Computercentrum Politie; LCP*) offers ICT-related service to the police organization.[28] The Service Facility Public Prosecution (*Dienstverleningsorganisatie Openbaar Ministerie; DVOM*) performs executive tasks – ICT services being one of which – for the entire prosecution service.[29] The judiciary is being ICT-supported by Spir-it.

Obviously, these governmental agencies can obtain their equipment and tools from several private organizations, such as computer suppliers. In addition, covenants between these authorities and private organizations can be established concerning the exchange of information. For instance, in January 2013 the police signed a covenant with the municipality of Soest and the security company Securitas.[30] Employees of this company are on patrol 24/7 on companies' premises, in residential area's and on connecting roads between the municipalities around Soest. In order to increase the performance of Securitas, the police provides this company with information about cars which and persons who have been come across in those municipalities under questionable circumstances. This information may include pictures of persons or vehicles. Privacy legislation doesn't allow the exchange of names and addresses of suspected persons. Securitas informs the police about registration numbers of spotted vehicles, about specific observations concerning questionable situations, and about other relevant information which could be of use for the police.

4 Information, Intelligence and Investigation

4.1 Introduction

Considering the broad overview (in paragraph 3) of the application of ICT in the criminal justice system, it wouldn't be expedient to even start describing the ICT-related techniques which are used in the criminal justice system. For this

---

[24] See J.E.J. Prins, 'Openbare orde handhaving na Haren', *Nederlands Juristenblad* 2013, p. 531 and http://www.forensischinstituut.nl/over_het_nfi/nieuws/2012/verzelfstandiging-internet-research-and-investigation-network.aspx. The following section was substantially derived from the latter source.

[25] See J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële Verkenningen*, September 2012, p. 35-49.

[26] http://www.forensicinstitute.nl/products_and_services/forensic_products/xiraf/index.aspx. The following section was substantially derived from the latter source.

[27] See R.C.P. van der Veer, H.T. Roos & A. van der Zanden, 'Datamining voor Informatie Gestuurde Politie', *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2009, and M.J.J. López, 'De mogelijkheden van *data mining* voor de Nederlandse politie', *Tijdschrift voor de Politie*, nr. 6, June 2000, p. 26-29.

[28] *Aanvalsprogramma Informatievoorziening Politie 2011-2014*, 19 September 2011.

[29] http://www.om.nl/organisatie/landelijke/item_148808/.

[30] See http://www.politie.nl/nieuws/2013/januari/16/03-soest-politie-sluit-convenant-met-securitas.html.

reason, in this paragraph we'll describe the legal rules concerning ICT-related techniques which are used in the criminal justice system.

4.2 Special powers of investigation[31]

The Special Powers of Investigation Act (*Wet bijzondere opsporingsbevoegdheden; Wet BOB*) came into effect on 1 February 2000 and relates to an amendment to the Dutch Code of Criminal Procedure. The act is a direct result of a parliamentary inquiry into criminal investigation methods. The inquiry underlined the fact that there seemed to be a number of investigative processes that were unknown to many parties. The committee of inquiry (named, after its chairman, the Van Traa committee) investigated the various, often unknown, investigative methods. The *Wet BOB* now legally regulates methods of this nature.

The *Wet BOB* confirms that the public prosecutor is the appropriate official to lead the criminal investigation. Every special power of investigation can be used once the public prosecutor has issued a warrant. Prior authorization of the examining magistrate is sometimes required, for instance if confidential communications or telecommunications are to be recorded. The Act determines that the public prosecutor must have the consent of the board of procurators general for civilian infiltration and matters involving laissez passer. The board must first present its decision to the Minister of Security and Justice.

The *Wet BOB* provides for three undercover powers: covert investigation (infiltration), pseudo purchase/services and systematically obtaining intelligence about suspects through undercover investigations. These powers involve situations in which an investigating officer is active in the milieu of the suspected persons without his identity as investigating officer being known. In addition, the *Wet BOB* covers all types of surveillance, or entering and 'looking into' premises and recording of confidential communications.

The Act defines surveillance as systematically following a person or systematically observing his whereabouts.[32] Systematically following or observing a person is only permitted in the case of a suspected crime and at the order of the public prosecutor. Surveillance is systematic if it enables a more or less complete picture to be gained of certain aspects of a person's life such as his financial activities or structural personal contacts with specific individuals. Systematic surveillance can include observing a person over a number of days using an observation team or following someone using a scanning device. Non-systematic surveillance is ordinary surveillance or the incidental observation of a number of actions or events. If technical aids are used which register signals of the person under surveillance, this is similar to systematically following or observing the individual. Surveillance of private homes is not permitted. Other locked premises such as office buildings or warehouses and storage buildings may be placed under surveillance, but only in the case of serious crimes. These locations may be entered without the owner's permission in order to place recording equipment or to perform other activities to enable the surveillance. As mentioned before, the legal basis for non-systematic surveillance/observation can be found in the statutory description of the statutory duty (*taak*) of the police to investigate criminal cases.[33] The question rises whether surveillance of 1) open sources on the internet and 2) sources on the internet that require registration can be qualified as systematic observation. In other words, does such an observation create (only) a light interference with a person's privacy, or a rather grave interference? In the latter case, an order of the public prosecutor is required. Currently, there's a debate going on in the Netherlands concerning this question.[34] Considering the fact that this type of surveillance doesn't take place manually anymore – instead: police systems (such as VIRTUOSO and iRN) are permanently searching the internet, obtaining unprecedented amounts of (combined) information – we would argue that an order of the public prosecutor is required.[35] If such an order is obtained by the police, the surveillance of open sources on the internet can be extended to data of computers which are located outside the Netherlands. The legal basis for this can be found in the Cyber crime convention of the Council of Europe.[36] [37]

---

[31] See http://www.om.nl/vast_menu_blok/english/special_powers_of/ from which the following was derived.

[32] Art. 126g, art. 126o and art. 126zd CCP.

[33] See art. 141 CCP, art. 3 Police Act 2012 and Hoge Raad (Supreme Court) 13 November 2012, *Landelijk Jurisprudentie Nummer* BW9338. See also T. Kooijmans, 'Een Tilburgse observatie van een Tilburgse observatie', *Ars Aequi* 2013, p. 222-229.

[34] See Oerlemans & Koops 2012 and B.J. Koops, 'Politieonderzoek in open bronnen op internet', *Tijdschrift voor Veiligheid* 2012 (11) 2, p. 30-46 (Koops 2012a). Cf. ECPS, *Opsporing op het internet. Het gebruik van gegevens binnen sociale media*, Erasmus University Rotterdam, April 2013. A similar discussion is taking place about the use of a 'stealth-sms'. See R.D. Chavannes & N. van der Laan, 'Kroniek Technologie en recht', *Nederlands Juristenblad* 2012, p. 2524

[35] When open source research has the character of systematic observation, the use of the technical tools – such as VIRTUOSO or iRN – have to meet requirements of the 'Technical tools criminal procedure Decree' (*besluit technische hulpmiddelen strafvordering*) which – according to art. 126ee CCP – applies to technical tools for systematic observation. See Koops 2012a, p. 38.

[36] Budapest, 23 November 2001. See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[37] Art. 32 Cyber crime convention: 'A Party may, without the authorisation of another Party:

Covert investigation or infiltration is defined as participating or cooperating with a group of people that is believed to be planning crimes or to have committed crimes.[38] If the officer involved in the covert investigation wishes to seem plausible to the group, he will have to take part in their activities. In a covert investigation there is a serious risk that the covert investigator will have to commit criminal offences. The Act lays down that actions that could give rise to a criminal offence should be listed in the warrant issued by the public prosecutor. As an infiltrator, the investigating officer cannot incite a person to commit criminal offences other than this individual had already planned: inciting the perpetration of an offence is ruled out. This is known as the *Tallon Criterion*.[39] Various types of infiltration are covered by the covert investigation regulation. The starting point is that the covert investigation is carried out by a police officer. The act provides for a regulation for the activities of a special investigating officer.

The *Wet BOB* defines pseudo purchase/services as the purchase of goods or electronically stored data from, or the supply of services to, the suspect. The characteristic feature of this power is that the investigating officer behaves towards the suspect in such a way that a criminal offence could result. For this reason, the Act incorporates the *Tallon Criterion* to regulate pseudo purchase/services in a similar way to covert investigation.[40] Pseudo purchase/services can also take place without being part of a covert investigation, which is why this power has been regulated separately to covert investigation.

Another special power of investigation is the systematically gathering intelligence undercover.[41] This means that a police officer systematically obtains intelligence on the suspect through undercover activities such as frequenting the suspect's haunts (sports club, bar or newsgroup) without it being apparent that he is acting as a police officer. The fact that the investigating officer is infringing the suspect's privacy and misleading him is of key relevance: the suspect does not know that a police officer has entered his environment, while the officer himself takes active steps to become involved in his life. Because the investigating officer is not committing criminal acts, undercover work poses far fewer risks to the integrity and security of the investigation than covert investigation and pseudo purchase/services. Therefore the power is bound by less serious conditions. In addition to the systematic observation, this power can be used to gather information about the suspected person online – iRN and VIRTUOSO have the functionality to shield IP-information – and offline.

The *Wet BOB* incorporates the power to enter locked premises (not private premises, but an office or warehouse) without the owner's permission.[42] The objective is to look around and secure traces, such as a sample, a fingerprint or a photo. But it could also provide an opportunity for the placement of technical aids (such as a scanner) in a vehicle in a garage. Opening cupboards and cabinets and breaking down doors is not permitted. In order to take samples, packaging can be opened, even if kept inside a container (which is not the same as a cabinet or cupboard). 'Looking in' also includes examining a location using technical equipment such as a robot, a rod or an infra red camera.

Furthermore, police officers have the special power to record confidential information.[43] This is only permitted in the case of a suspected rather grave crime at the order of the public prosecutor after the examining magistrate has given explicit authority. It involves recording confidential communications using technical equipment such as recording conversations and telecommunications in a closed network such as a company network. This category also includes bugging a personal computer to access messages before they are sent over the internet or encoded and 'scanning' (using a radio receiver to intercept mobile telephony). On the whole, recording confidential communications involves more risks than recording telecommunications. To record confidential information, technical equipment must be placed close to the suspects' environment. The regulation does not include communications that can be picked up without using technical aids, for example audible conversations in a bar or on the street. The regulation only concerns confidential communication: exchanges between persons or organizations that take place behind closed doors. Behind closed doors means that the parties involved have every right to believe that third parties cannot hear what they are discussing in normal circumstances. However, the regulation does include confidential communications in which the investigating officer takes part, for instance in cases of covert investigation. Recording confidential communication in a private house is only permitted under strict conditions: if it is urgently required for the investigation, if

---

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'

[38] Art. 126h, art. 126p and art. 126ze CCP.

[39] See Hoge Raad (Supreme Court) 4 December 1979, *Nederlandse Jurisprudentie* 1980/356 (with a comment by Th.W. van Veen).

[40] Art. 126i, art. 126q and art. 126zd CCP.

[41] Art. 126j, art. 126qa and art. 126zd CCP.

[42] Art. 126k, art. 126r and art. 126zd CCP.

[43] Art. 126l, art. 126s and art. 126zd CCP.

the offence carries a term of imprisonment of eight years or more and the examining magistrate has given explicit authority.

Investigating telecommunications involves telephone taps and claiming data concerning telephone traffic.[44] The power to claim data on telephone traffic can be applied at the order of the public prosecutor in the case of a suspected rather grave crime. It is also the public prosecutor who, after receiving authority from the examining magistrate, issues a warrant to tap a telephone and ensures that the data acquired thereby is stored and destroyed. It's not a condition that the suspect takes part in the telecommunication. The offence in question must pose a serious breach to law and order. Related to these investigation powers is the use of a so-called IMSI-catcher: a device with which a suspect's telephone number can be traced if the investigating authorities are aware of the residence of the suspect, and with which the residence can be recovered if the suspect's telephone number is known by the investigating authorities. Whereas the power to obtain the telephone number is regulated in art. 126nb CCP, a specific power to trace the residence of the suspect is not explicitly provided for in statutory law. It's generally assumed that the latter power can be derived from the statutory description of the statutory duty (*taak*) of the police to investigate criminal cases.[45]

The powers outlined above may not only be used to resolve concrete offences that have been committed (including attempt to and preparation of crime), but can also be applied to investigations into organized crime. This means that investigative efforts need not be restricted to the investigation of concrete crimes that have already been committed because organized crime involves the constant planning and perpetration of crimes that have serious impact on society. This so-called 'pro-active' investigation, investigation into offences that have not yet been committed, can only be deployed when tackling organized crime. For less serious forms of crime, special powers of investigation can only be used to investigate offences that have already been committed. Furthermore, the before mentioned powers may be used in case of 'indications' – a 'reasonable suspicion' is not required – of a terrorist offence. In that case, investigative efforts need not be restricted to the investigation of concrete crimes that have already been committed.

Art. 126gg CCP regulates the so-called exploratory investigation into the influence of more serious types of crime in a certain social sector, preparatory to a criminal investigation. Exploratory investigations are therefore not investigations and powers of investigation may not be applied.[46] An exploratory investigation covers the gathering, combining and analyzing of data from police and other records from which the investigative officer can obtain information, such as the registers of the Chamber of Commerce. Privacy legislation, specifically the Police Records Act and the Data Protection Act, offer a context for processing personal details. This legislation determines the purpose for which information may be provided and stored. The concept of 'exploratory investigation' is an examples of the fading boundaries between on the one hand (possibilities for) criminal investigation, based on the reasonable suspicion that a certain, concrete crime has been committed or is to be expected and on the other hand the more general aim of security-policy to prevent any crime or criminal or undesirable behavior from happening at all. The 'expansion' of legal powers to the latter area, is risky in the way that an 'effective' use of powers calls for a broad scope of possibilities to collect data.

4.3 To demand data and searching in order to record data

A specific cluster of special investigation powers the use of which can be linked to ICT, concerns the demanding of data.[47] Until several years ago, the police and the special investigation services experienced a number of problems as regards the competence of their criminal investigation departments to request information from third parties. The government installed the Committee '*Strafvorderlijke gegevensvergaring in de informatiemaatschappij*', also known as the Mevis-commitee[48], after its chairman, to study whether the CCP still offered a satisfactory legal framework for obtaining third party information in criminal investigations, particularly in view of new developments in ICT. The Committee concluded that adaptation of the CCP was indeed advisable, and drafted a bill accordingly. Parliament ultimately passed the proposal into new legislation: the [Investigative] Powers to Request Information Act (*Wet bevoegdheden vorderen gegevens, Wbvg*), effective from 1 January 2006. The Act's main purpose is to provide in the CCP a clear legal framework for the investigation services and the third parties from whom they request information, as well as to give the latter better legal guarantees. The powers defined by the *Wbvg* are part of the CCP.

The *Wbvg* offers competent police detectives, detectives working for the special investigation departments, and public prosecutors (either independently or with the consent of the investigative magistrate) six specific powers to

[44] Art. 126m and 126n, art. 126ta and 126u, art. 126zg and art. 126zh CCP.
[45] See art. 141 CCP, art. 3 Police Act 2012 and Chavannes & Van der Laan 2012, p. 2524.
[46] Subtle distinctions can be found in art. 126hh and 126ii CCP.
[47] See T. Spapens, M. Siesling & E. de Feijter, *Brandstof voor de opsporing. Evaluatie Wet bevoegdheden vorderen gegevens*, The Hague: Boom Juridische uitgevers 2011, p. 137-144. The following section was substantially derived from this source.
[48] Committee 'Strafvorderlijke gegevensvergaring in de informatiemaatschappij'. See also *Kamerstukken II* 2001/02, 28 366, nr. 1.

request information from third parties, other then a suspected person. First, a competent detective may request information for identification purposes.[49] Secondly, the public prosecutor has the power to request other types of information, both historical information registered by third parties[50] and information which they may register in the future as part of their regular business processes[51]. Thirdly, the public prosecutor may request a holder of information to assist in decrypting information that has been encrypted before storage.[52] Fourthly, he may order a search of electronically stored data.[53] If, however, the public prosecution service requests information regarded as extremely sensitive to privacy, for example concerning a person's race or his religious or ethnic background, a suspicion of a grave offence is needed and the public prosecutor also needs the consent of the investigative magistrate.[54] The parliamentary history of this legislation makes clear that not only photo's which directly contain data concerning a person's race are to be considered extremely sensitive, but also photo's from which information concerning a person's race can be distracted. A judicial consent is needed not only in cases in which the aim of obtaining the photo is to distract sensitive information from it.[55]

The more sensitive the information being requested and the more effort it takes a data holder to comply with a requisition demand, the more restricted the *Wbvg*. The *Wbvg* makes it possible to request information about suspects in criminal investigations, but also about other individuals if doing so contributes to the purpose of the investigation.[56] The types of information that can be requested are not limited to specific categories (such as financial information). The *Wbvg* does not limit the powers for the seizure of objects[57] such as (complete) computers in which data are registered. However, in concrete cases such a seizure could be a disproportional use of powers.

As mentioned before, the public prosecutor has the power to order a search of electronically stored data. According to art. 125i CCP, this power is related to a physical search of a location in which a data carrier can be found. In case of a search on such a location, the police has the power to investigate (and record) the contents of a device which is stored elsewhere.[58] This so-called network-search enables the police to search computers which are connected to the computer that was discovered during the search of the location.[59] This network-search should be distinguished from the power to confiscate objects; it cannot be applied after the confiscation of a computer. Concretely, in the Netherlands a network-search can take place during a search in a house. On that occasion, a device in that house can be se searched which is connected to a mediaserver, a gamecomputer or an external harddisk. The data which is stored on those devices and which can be used to find the truth about a criminal offence, can be copied and documented. This investigation power may only be applied in case of necessity. It should be expected that relevant data can be found in connected computersystems. The network-search can be executed in connected systems insofar the persons living of working in the searched location have legal access to those systems.[60] It's conceivable that a system operator (of a company) who has legal access, facilitates the network-search. According to art. 125k CCP, an order can be given to provide access of a secured computer and/or to decrypt relevant data. This order cannot be given to the suspected person. However, it is questionable whether an order, given to a suspected person, would be incompatible with the *nemo tenetur* principle.[61] The investigating authorities, when conducting a network-research, are not allowed to hack connected systems in order to obtain access to the data. In the Netherlands, the so-called 'computer-oriented principle of jurisdiction' prevails: the search of a computer is executed according to the law of the

---

[49] Art. 126nc CCP.
[50] Art. 126nd CCP. The request is limited to parties who register for other than personal use.
[51] Art. 126ne CCP.
[52] Art. 126nh CCP.
[53] Art. 125i CCP.
[54] Art. 126nf CCP.
[55] Hoge Raad (Supreme Court) 23 March 2010, *Nederlandse Jurisprudentie* 2010/355 (with a comment by P.A.M. Mevis). See also ECPS, *Opsporing op het internet. Het gebruik van gegevens binnen sociale media*, Erasmus University Rotterdam, April 2013, p. 33: the request to provide the police with a copy of an application of a travel document in order to obtain a photo of the suspected person, is not regulated by the 'extremely-sensitive-rules', but by the Passport Act and the Passport Execution Regulation. According to these regulations, investigating authorities have the power to require these data if that's necessary for the investigation of criminal offences.
[56] Art. 552a CCP allows holders of information to file a complaint against a requisition, albeit only in retrospect.
[57] Hoge Raad (Supreme Court) 31 January 2012, *Landelijk Jurisprudentie Nummer* BT7126, *Nederlandse Jurisprudentie* 2012/690 (with a comment by M.J. Borgers).
[58] Art. 125j CCP. See C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5. The following section was substantially derived from this source.
[59] Since the network-search is related to the physical search of a location, the conditions under which the network-search can be applied depend on the conditions under which specific locations van be searched. The latter conditions vary according to the category of locations that are to be searched.
[60] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 27-28.
[61] B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel*, The Hague: Boom Lemma uitgevers 2012 (Koops 2012b).

state in which that computer is located. Searching a computer in a foreign state may be incompatible with the law and/or sovereignty of that state and should, for that reason, be based on a treaty or on consent of that state.[62] Beforehand, it's not always clear whether a network-research will lead to the search of a computer which is located abroad. According to the legislator, in that case the obtained data can be used in the criminal investigation.[63] In addition to this, the Supreme Court has ruled that the question whether international law was complied with by the Dutch investigating authorities, is in prinicple not relevant in the criminal case against the suspected person, because the interests protected by international law, are not interests of the suspected person, but interests of the state on the territory of which the authorities conduct the research.[64]

The storage of data in the 'cloud' has given a new and somewhat problematic dimension to this theme. To illustrate this, we quote Koops and others:

> 'Experiences with cloud computing in investigation and prosecution practice seem to be scarce to date, both in the Netherlands and abroad. The only exception are web services, which have existed for a longer time and which regularly feature in criminal investigations. Still, cloud computing is expected to create considerable challenges for investigation in the foreseeable future.
>
> First, the statutory framework raises some legal questions and impediments. It is unclear when exactly a cloud provider will qualify as a communications provider or a public telecommunications provider. Moreover, the Dutch Code of Criminal Procedure (…) distinguishes between stored data and data in transit, and between communication and noncommunication. These distinctions are sometimes hard to apply in the case of cloud storage and processing services; they also seem to become less relevant. Besides, the rise of cloud computing, along with an increasing deployment of encryption, reinforces the question – which is already being discussed – whether a power should be introduced for the police to covertly acquire remote access to (i.e., to hack into) computers of suspects.
>
> Second, investigation practice will have to adapt in order to meet the shift of data storage from hard disk to cloud. In searches, the police will have to be more aware of the importance of searching and seizing computers while they are active, in order to secure the computer's temporary memory and activated network connections, including connections with cloud services. Classic searches and classic wire interceptions will gradually have to make room for Internet interceptions – something which legislation and legal practice are not yet very well catering for.
>
> Third, and most importantly, the most prevalent methods to collect digital evidence (searches, production orders, intercepting data) have limited effect with data that are stored in, or exchanged through, the cloud. The main bottleneck is the territorial boundaries to which Dutch investigation is still bound. Since cross-border network searches are not allowed (except in the rare cases of having permission from the suspect or voluntary co-operation by foreign service providers), law enforcement has to rely on mutual assistance with an order for foreign cloud providers to produce data. This is not something new: cyber-investigation has traditionally suffered from having to deal with questions of cross-border access to data. However, these questions become much more profound through the 'loss of location' that the cloud implies. Files are usually stored in the cloud among different servers, in multiple copies and carved in pieces; the system itself calculates, on the basis of demand and supply, the most efficient storage and continuously moves around file pieces accordingly. This makes it very hard to determine, also for the cloud provider itself, on which exact location(s) a file is actually stored. The location where data 'are' no longer works as the main clue for determining rights and duties in relation to the cloud.
>
> For investigation practice, the loss of location is particularly relevant, especially given the context of criminal procedure law, in which territorial sovereignty continues to play a very dominant role. When criminals migrate their data management to the cloud, Dutch investigation practice will run into the wall of territorial limitations. Both law and public policy will have to start addressing this problem. The Netherlands will have to invest in co-operation, both with foreign governments and with service providers. Further streamlining of mutual-assistance procedures is essential for cloud investigations.
>
> The loss of location provides a more fundamental challenge as well, as it also impacts on the abstract level of jurisdiction and sovereignty theory. One can roughly distinguish two schools of thought: 'territorialists', who emphasise the physical location of servers and routers, and 'cybernauts', who argue that physical locations are only accidental in cyberspace. The territorialists may have to cede ground to the cybernauts,

[62] Cf. *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23. See also B.J. Koops, R. Leenes, P. De Hert & S. Olislaegers, *Misdaad en opsporing in de wolken*, The Hague: WODC 2012, p. 36-37.
[63] *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23.
[64] Hoge Raad (Supreme Court) 5 Oktober 2010, *Nederlandse Jurisprudentie* 2011/169 (with a comment by T.M. Schalken).

> once cloud computing captures an established place in the Internet landscape. That would be in line with literature about the cloud, which seeks to establish jurisdiction based on the persons who have lawful access to data (such as providers and customers) rather than on the location of the server that hosts data.
>
> This implies as well that the cloud challenges the classic criminal-law regulatory model of mutual assistance. There is a need to reflect on the role of sovereignty in criminal investigation. Partly because of the difficulty of determining the location of data in the cloud, and partly because investigation in the cloud sometimes calls for more expeditious action than mutual assistance – however streamlined it may be – can offer, there is good reason to allow a cross-border network search. The Belgian model, in which network searches can, under certain conditions, be extended to foreign network connections with *ex post* notification to the foreign state at issue, could serve as a source of inspiration. Another question is under which conditions the Netherlands would consider it justified for law enforcement to contact foreign providers directly instead of walking the path of mutual legal assistance. Both issues can obviously only be addressed on the basis of reciprocity: the Netherlands could be allowed to collect data from abroad only if foreign countries could do the same on Dutch territory. In this manner, a new and modern meaning could be given to sovereignty in a networked world order.'[65]

4.4. Storage, use and provision of privacy related data; comparing of data

The storage, use and provision of privacy related data and information that results form criminal investigation is subjected to the Privacy Data Act (Wet bescherming persoonsgegevens) and the Act on police-data (Wet Politiegegevens). These acts do not provide for any investigative power to collect data. The legal basis for powers of investigation is the CCP, not these acts on data-protection. Both acts deal with the processing of data such as rules for storage, destruction of data afterwards, and possibilities to supply other official institutions with some police data in specific cases. We quote the underlying principles:

- The police will obtain enough space to process personal data in an efficient and effective way;
- Police data are processed only if that's necessary to properly conduct the police tasks;
- The data that are being processed are obtained legitimately and they are accurate; the data will be corrected or destroyed if they appear not to be correct;
- Police data will only be processed for well defined and legitimate purposes and only if processing the data is proportionate to the purpose;
- More protection against violations on privacy is offered as data processing becomes more specific;
- Access to police data is restricted by means of authorisation;
- Police data that are processed for various purposes can, under certain conditions, be connected and combined with each other;
- The police can provide other authorities and the Royal military police with data if the law specifically allows this or if this is necessary because of an important public interest.[66]

These principles illuminate the search for a balance between privacy-protection and adequate use of data in criminal investigations.

All these classic topics of data-processing are carried out nowadays by ICT-techniques. As such there is no need for special attention for these rules in this report with two exceptions.

First, the Act on police-data provides for the possibility of automated comparing data. On this point, ICT provides for the possibility to compare the content of huge data files within seconds and to draw conclusions out of the results of the comparing-process, for instance for the start of a criminal investigation or for the decision to use certain (special: see below) investigation powers in the CCP in a certain direction of a criminal investigation. On this point the Police data act may have a certain autonomous position where it provides a legal basis for this process of comparing data, a investigation method which, in the Dutch approach, one would expect to be codified in the CCP only. But in this respect it is relevant to know that the police task is broader then the investigation of criminal matters only. The police has a broader task, for instance to insure the maintenance of public order, task that is conducted under the authority of the local mayor in stead of the public prosecutor. The possibilities to compare relevant data form the Police Data Act can be used for this task as well. (As we will see below, there is a provision to compare data in criminal investigations in – for instance – art. 126hh CCP.) In the light of possible (further) criminal investigation it is relevant that – once police data are compared with each other, the way in which relevant relations between data is concluded and made visible to others, should be recorded for control afterwards.[67]

---

[65] Koops, Leenes, De Hert & Olislaegers 2012.
[66] Explanatory Memorandum to the Police Data Act (*Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 3).
[67] Par. 11 under 3c Police Data Act (*Wet politiegegevens*).

Secondly, art. 126dd CCP allows the police to preserve data for further use in other criminal investigations and to gain a certain picture of someone's possible involvement in severe crimes.[68] In the future, Dutch law might have to be adapted to upcoming EU-law, more specifically the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offence or the execution of criminal penalties, and the free movement of such data[69] and the proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).[70]

4.5. New ICT-related powers to tackle cyber crime?

On 15 October 2012, the minister of Security and Justice sent a letter to the Lower House (*Tweede kamer*) in which he announced the introduction of new investigative powers of the police and the public prosecution service on the internet.[71]

According to the minister, a more effective approach to cyber crime requires a closer look at possible expansions of powers.[72] Based on recent experiences of the police and the public prosecution service, the minister argues that the current powers for fighting cyber crime are no longer up to date and need to be shaped in such a way that these are manageable and effective in the current digital world. The number of cyber crimes is increasing and the capacity, knowledge and experience within the criminal justice chain is not keeping up. Criminal activities on the internet are moreover harder to trace, because it is relatively simple for criminals to cover digital tracks. Improvement is clearly necessary in order to strengthen the investigation and prosecution of cyber crime.

The minister argues that the new powers need to be surrounded by strict guarantees. For example, remotely hacking into a computer will require the advance authorisation of the examining judge. In addition, it will only be possible to exercise the power if there is a suspicion of criminal offences of a certain seriousness, for example crimes that are liable to pre-trial detention or that are liable to a maximum term of imprisonment of four years or more. All investigative activities will also have to be logged and stored, so that these can always be consulted and checked after the fact. The police and the public prosecution service conclude that in a practical sense they now need an expansion of the legal options for action. The law therefore needs to be updated.

The minister gives the following inventory of new investigative powers under criminal law on the internet:

- Remotely searching data that are accessible from a computer, irrespective of the location where these data are stored and with due observance of the agreements and rules concerning international legal assistance;

- Remotely rendering data inaccessible that are accessible from a computer, irrespective of the location of the automated work on which the data have been stored and with due observance of the agreements and rules concerning international legal assistance;

- Remotely entering computers and installing technical resources (including software) for the purpose of investigating serious forms of crime;

- Criminalising the purchase of stolen (digital) data.

A draft version of a new Act was presented in the first week of May 2013, just before this chapter was finalized.[73] The draft contains instruments to – for instance – crack encrypted data, tackle illegal actions on internet and fight child pornography online. As was announced before, according to this draft bill, the police and the judiciary will have the power to conduct remote investigation in criminals' computers and, if necessary, to take over data or to render them inaccessible. This concerns the so called 'investigating automated work' that enables criminal investigators to apply various forms of inquiry in the investigation of serious crimes.
It is not only about rendering data inaccessible or taking them over, such as child pornography or stored e-mail messages with information on crimes, but also about tapping communication or observation. Strict guarantees apply to the use of the new power, such as a prior judicial review and certification of the software being used and data logging.

One of the aims of the draft is to take better action against botnets. Botnets are large-scale networks of semi-autonomously working software robots on 'zombie computers' that can be operated from a distance to carry out illegal actions, such as sending spam, collecting (company) secrets, credit card details and passwords. DDos attacks

---

[68] Hoge Raad (Supreme Court) 6 maart 2012, *Landelijk Jurisprudentie Nummer* BQ8596, *Nederlandse Jurisprudentie* 2011/176.
[69] COM (2012) 10 final.
[70] COM (2012) 11 final.
[71] *Kamerstukken II* 2012/13, 28 684, nr. 363. See also B.P.F. Jacobs, 'Policeware', *Nederlands Juristenblad* 2012, p. 2761-2764.
[72] *Kamerstukken II* 2012/13, 28 684, nr. 363. See also http://www.government.nl/news/2012/10/16/opstelten-intends-to-strengthen-investigations-on-the-internet.html from which the following was derived.
[73] See http://www.government.nl/news/2013/05/02/minister-opstelten-strengthens-the-approach-of-computer-crime.html.

and the spreading of malware also belong to the options. To render a botnet harmless, it is necessary to get access to the servers that are a part of it. Taking action in cyber space may result in data being rendered inaccessible, also when they are on a server abroad. This may be the case if the actual location of the data cannot reasonably be traced back, as applies for example to data in the Cloud.

According to the minister, when tapping communication, police and the judiciary are more and more bothered by electronic data being encrypted. Special programmes are offered on internet to encrypt data files. Information systems and software often have standard settings for encrypted forms of communication, such as a Gmail and Twitter. Internet users can even transport data anonymously through certain services. This plays into the hands of criminals. The provider is obliged to cooperate in cracking encrypted communication, but he is sometimes not even able to do that or the provider is established abroad. That is why, according to the draft, the police and the judiciary will be able to tap the machine instead of the connection under strict conditions. The investigation in automated work makes that possible. The bill also allows for the possibility to oblige suspects of the possession and trade in child pornography or of terrorist activities to cooperate in opening encrypted files in their computer. The public prosecutor will be empowered to give a decryption order to the suspect in that case. Police and judiciary will get access then to shielded data and can fight the production, spreading and possession of child pornography more effectively and offer help to the victims. Strict guarantees apply here such as prior judicial review. Ignoring a decryption order from the public prosecutor will result in a maximum prison sentence of three years. According to the bill, healing of computer data is going to be a criminal offence, in order to prevent third parties having access to the stolen information after intrusion in a computer and placing it on websites. It is important for a conviction that the suspect knew or could have suspected that the information concerned stems from a crime. In practice, computer data are regularly used which were obtained through crime, such as computer hacking or clever snatching of passwords and user access codes. There will be a maximum prison sentence of one year for it.

4.6 Notice and take down[74]

Although it is not (yet) a specific procedural provision, it is worthwhile to notice that there is a 'notice an take down'-procedure in Dutch (substantive) criminal law. According to art. 54a of the Criminal Code (CC), a provider of telecommunication, such as an internet-provider, will not be prosecuted for any offence during storage or transfer (mere conduit, caching and hosting) of data if the provider, on order of the prosecutor (authorized by the examining judge), takes all measures to make certain data no longer accessible. The provision, initiated by Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (directive on electronic commerce), aims to protect the freedom of expression and to provide for any (self)censorship by the provider. The protection only exists because and in so far as the provider has no responsibility for the content of the data as such. Not obeying the order is a separate criminal offence.[75] The European Directive forbids the condition that the protection against criminal prosecution only exists when the provider apprises the 'offender' of the crime, that is: the person responsible for the content of the data, to the judicial authorities. Nor is the provider obliged to control the data before transferring it.

The aforementioned draft of a new act proposes a modern version of a 'notice and take down'-order in art. 125p CCP. The construction is generally the same as under the existing par. 54a CC although judicial control is transferred from the pre-order phase, and changed into a possibility of judicial review on remand afterwards only. The new provision is partly a codification of the 'Notice and Take Down'- Code of Conduct, agreed between government and providers in 2008.

5 ICT and Evidence

The Dutch legislation on trial proceedings and evidence does not contain specific provisions regarding aspects of ICT in the same elaborate and extensive manner as is needed (and was described above) for pre-trial investigation proceedings. Nevertheless, rules and their application in an 'ICT world' require attention. In this section, the topic of evidence will be discussed; in the next paragraph, several other procedural aspects will be covered.

5.1 Introduction: Dutch law on evidence in criminal cases

In the world of the Internet, the use of ICT and the application of the aforementioned different powers of investigation have increased possibilities for gathering information regarding cyber crimes during a criminal investigation.

One characteristic of the Dutch criminal procedure is that there is no separate procedure in which it could or should be decided what information is allowed as evidence in court. There is no possibility even to discuss the admissibility of information as evidence. Likewise, there are no rules of admissibility that would allow an investigating judge or any

[74] Koops 2010, II.d.1. and B.J. Koops, 'Tijd voor Computercriminaliteit III', *Nederlands Juristenblad* 2010, p. 2461-2466, publicationnumber 1982 (extensive version on www.njb.nl).
[75] Par. 184 CC.

pre-trial court to decide about the admissibility of information that might be either included − or excluded − as part of the trial's procedural documents.[76] This approach leads to the Dutch criminal procedure characteristic that all information gathered in pre-trial investigations is allowed to be presented in trial proceedings as possible evidence that can be used against the accused. By the same token, the information can be provided to other States at their request as part of an international cooperation in criminal matters. There are rules and procedures regarding the exchange of information within the scope of international cooperation, but none to govern and aid in a decision as to whether only information might be transferred that would be accepted as evidence under Dutch criminal procedural law.

There is in fact only one exception to this approach. In the event that the application of the previously mentioned special powers of investigation lead to information that is part of the recognised and protected communication between a citizen and members of a small group of professions to whom the law guarantees the right of confidential communication with any citizen that seeks their help, support, and advice (doctor, priest, and defence counsel in criminal matters), a statutory rule forbids use of the content of[77] this information, not only as evidence but also as information in a criminal investigation. Unless, by way of exception, the examining judge decides that the results of taped communication between the accused and his counsel are not considered protected communication (for instance, communication that might lead to the conclusion that the defence counsel is a 'partner in crime'), the information must be destroyed immediately.[78] This information therefore will never − nor should it − reach the trial court; this is the only exception to the rule that normally only the trial court decides about the use of information as evidence. In this exceptional situation, there is no room for a trial court decision or, for that matter, to save this kind of protected information during a pre-trial investigation to allow a court decision on this point; the protected information must be destroyed at once.[79] In practice, since 2012 ICT has been used for the development of a system of telephonenumber recognition. This makes it possible that in the event that telephone communication involving the accused is taped by court order, the communication between the accused and his defence counsel will no longer be taped.

The fact that no rules or procedures on the admissibility of evidence exist does not mean there are no criminal procedure-related rules regarding evidence that are especially relevant in the ICT world.[80] Conviction is only possible if the court, after the trial procedure, is *convinced* that the offender has committed the offence as charged by the public prosecutor.[81] This conviction by the court can be based only on the means of evidence that are enumerated and defined in the CCP.[82] The CCP allows only five of these:

- the court's own observation during a court trial;
- the statement of the accused in or out of court;[83]
- the statement of a witness in court;
- the statement of an expert in court;
- written materials.[84]

In the 'written materials' category, the CCP[85] distinguishes five specific categories, summarised by Tak[86] as:

- written decisions by members of the judiciary;
- reports by members of competent agencies: e.g. police reports on facts or circumstances personally perceived or experienced by these agencies;
- documents of public agencies concerning subjects related to their competence, containing the communication of facts and circumstances perceived or experienced by these agencies;
- reports of experts;
- all other written materials, although only to be used in relation to the content of other means of evidence.

---

[76] Hoge Raad (Supreme Court) 20 April 2010, *Landelijk Jurisprudentie Nummer* BK3369 en Hoge Raad (Supreme Court) 17 January 2012, *Landelijk Jurisprudentie Nummer* BU2046.
[77] Not the traffic data: Hoge Raad (Supreme Court) 20 December 2011, *Nederlandse Jurisprudentie* 2011/437 (with a comment by T.M. Schalken)
[78] Art. 126aa par. 2 CCP
[79] Supreme Court (Hoge Raad) 12 January 1999, *Nederlands Juristenblad* 1999, p. 268, nr. 24, and the special order to destroy the above-mentioned category of information (*Besluit bewaren en vernietigen niet-gevoegde stukken met het oog op de vernietiging van geheimhoudersgesprekken*) *Staatsblad* 1999, 548, changed by *Staatsbla*d 2013, 135.
[80] For more in general, see P.J.P. Tak, The *Dutch Criminal Justice System*, Nijmegen: Wolf Legal Publishers 2008, p. 105-107.
[81] Art. 338 CCP.
[82] Art. 338 CCP.
[83] There is no guilty plea in Dutch procedural law.
[84] Art. 339 CCP
[85] Art. 344 CCP
[86] Tak 2008, p. 106.

It should be mentioned that, according to a Supreme Court ruling dating from 1926,[87] hearsay testimony is widely accepted under Dutch law, provided that any statement by a witness takes the form of any other means of evidence: for instance, when it is reported by the police, and their hearing of a witness and his or her answers to the questions are 'personally perceived or experienced' by the police officer within the meaning of the above-mentioned Art. 344 CCP. The police report containing the witness's statement is accepted as written material, and thus as a means of evidence. It is therefore not crucial to hear the witness in court, although Art. 342 CCP suggests that it is necessary for use of the witness's information as evidence against the accused. Because of the consequences and differences regarding the right of the accused to challenge and question the witness for the prosecution under Art. 6 of the European Convention on Human Rights, this is a widely discussed aspect of Dutch criminal procedure, which is partly 'corrected' by some judgments given by the European Court on Human Rights.

While in this respect the Dutch CCP suggests, on the one hand, a certain 'closed' system of legally defined and − in a enumerative way – an elaborate system comprising only five means of evidence, it is clear that, on the other hand, all the results of ICT-related information gathered in a pre-trial investigation might be made ready for use as evidence in court. The only rule is that the information be presented to the court by one of the means of evidence provided for by the CCP. However, in particular the 'open' means of evidence of court observations and written materials offer numerous possibilities to introduce a wide variety of information as possible evidence.

Where there are few limitations on the admissibility of information as evidence in a trial, the court's responsibility concerning the use of information as evidence against the accused is greater. In this respect, under the Dutch criminal procedure system the trial court bears a heavy responsibility. The system depends on a high level of trust in the trial judge as an independent and 'just' professional. (For instance, the questioning of witnesses is done primarily by the court. After the courts interrogation, there is room for *additional* questioning by the prosecutor, the defence counsel, and the accused; cross-examination is unknown.) The court has to decide whether an offender can be convicted − or, and more precisely, whether the facts mentioned in the charge have been proven − on the means of evidence. The court has its own, separate, and full responsibility as regards making a correct decision, and its role can be demonstrated here by the presentation of a few different aspects of this obligation.

As the Dutch system traditionally belongs to the civil law tradition, the courts play an active role in gathering evidence and other relevant material. The court may undertake or order further investigation if it considers such an action necessary for a correct decision.[88] This provision is applicable in the court of first instance as well as in the appeal courts;[89] within certain limits, charges may be changed between a first instance court and the court of appeal. The prosecutor and the defence counsel can request such an investigation, but the court can and must order it on its own behalf if it is convinced that further investigation is necessary. What might be considered necessary is related to the task of the court to assess the evidence, during which the court might order further investigation if any points of evidence are being argued, or when there are indications for further investigations, especially in the advantage ('a décharge') of the accused.

Such an investigation is related to the court's task of determining the truthfulness of the evidence, and the court is free to examine evidence in this respect. Because there is no − pre-trial or otherwise − procedure to discuss and to decide the admissibility of evidence, this assessing of evidence as late as in a trial court session for the first time makes it necessary to give the trial enough access to the pre-trial investigation and its results. As a general point of interest, since January 2013 a new system of rules has been applicable concerning criminal case files. All materials that might be relevant for any decision of the trial judge must be in the file, and the accused may ask to add further material that he thinks might be pertinent. The accused has access to the complete contents of the file when preparing his trial defence, including proceeding-related documents saved only on data carriers.

A specific point of ICT interest is the ruling of Art. 126hh CCP, which dates from February 2007. The provision relates to the above-mentioned possibility of an exploratory investigation into the influence of more serious types of crime in a certain social sector, preparatory to a criminal investigation. As mentioned, exploratory investigations cover the gathering, combining, and analysing of data from police, along with other records from which the investigative officer can obtain information. This legislation determines in the first place the purpose for which information may be provided and stored. In addition, however, the CCP rules[90] that information will not be destroyed for as long as the information is necessary to control the process of obtaining the information, including the combining and analysing (data mining) afterwards. Controlling afterwards is – exclusively – part of the trial court's procedure of assessing the evidence. The system illustrates that the court's responsibility 'reflects' on the rules for the pre-trial investigation: control-

[87] Supreme Court (*Hoge Raad*), 20 December 1926, *Nederlandse Jurisprudentie* 1927/85 (*De auditu*-decision).
[88] Art. 315 CCP
[89] Art. 415 CCP.
[90] Art. 126hh par. 7 CCP.

ling afterwards should be made possible. It can be argued that, although the aforementioned provision of Art. 126hh par 7 is limited to the exploratory investigation, it covers more generally a vital aspect of the Dutch criminal procedure system: namely, where an assessment of all aspects of the evidence depends only on the trial court – that is, after the pre-trial investigation − the assessment must be made possible, and must be prepared truthfully and completely during the pre-trial investigation. (See also below *ICT in the trial stage*.)

5.2 Was the evidence lawfully obtained?

As regards ICT, it is important that the court not only determine the truthfulness of the evidence but be able to decide whether the evidence has been obtained legally, and is reliable and trustworthy. Hence, criminal courts have to consider the quality of the evidence in deciding whether the facts stated in the charge have been proven. This element of the court decision is also the result of the absence of a prior and separate procedure to decide on these aspects of the quality of evidence as part of the decision on the admissibility of evidence under Dutch law.

There is no rule under Dutch law that allows the use of evidence only if the court has found it to have been obtained in a lawful and legal manner. However, according to the statutory provision of Art. 359a CCP, there might be grounds to exclude evidence because it was obtained illegally during the pre-trial investigation. The trial court may find illegally obtained evidence as a result of objections and explicit defences from the counsel or the prosecutor, or when the way in which certain evidence was obtained can be derived from the file.[91] The Supreme Court did limit the need for the exclusion of illegally obtained evidence to – in short – extreme cases of serious breaches of fundamental rights of the accused.[92] As to ICT, it is worth noting that – in accordance with EcrtHR law – the Supreme Court ruled that the use of evidence gained in a way that forms a breach of Art. 8 of the ECHR does not include a breach of Art. 6 of the Convention (fair trial); in the opinion of the ECrtHR, there is no need for an exclusionary rule under Art. 6.[93] Nevertheless, because an exclusion of evidence might result, it is necessary for the trial court to deal with the legality of evidence, even irrespective of whether illegally obtained evidence might therefore no longer be reliable. In other cases, evidence obtained unlawfully may result in the court mitigating the sentence. This 'sanction' is outside the range of the decision on the evidence, but it urges the court to decide and, under certain circumstances, to investigate the lawfulness of the way in which evidence was gained during the pre-trial investigation. If the counsel or the prosecutor made an explicit defence on this point during the trial, the decision to deny it must be reasoned in the court's verdict.[94]

As mentioned, the use of ICT methods is technically new, and is not in all cases elaborated upon in adequate constitutional, privacy- and data-protecting, and procedural rules and rights. Because of the provision in Art. 359a CCP, in the Netherlands many ICT-related methods of investigation, such as the above-mentioned use of ANPR systems, and the development of the 'non-systematic following of persons', are discussed and elaborated upon under the responsibility of the trial courts in criminal cases to discuss and decide upon the legality of evidence, and thus to decide and discuss certain methods of criminal investigation. This often leads to a certain 'testing' of new technological methods of investigation by the police during pre-trial investigations (in the Netherlands, under the prosecutor's authority), and waiting for a supreme court's ruling on the legality of the method under accustomed law; ultimately, criminal investigators tend towards a 'creative' interpretation and use of legal powers, up to the limits of what is known as the problem of 'noble cause corruption'.[95] Only when disapproved by the courts, there might be the need for a statutory provision. The problem in this 'reverse approach' is that the discussed method of investigation is already more or less part of the investigation practice at the time that the court has to decide whether it is legal − with the possibility of an acquittal in a concrete, severe criminal case as result − and at a time when parliament still has to decide whether it can be accepted. The need for a certain method is then almost inevitable.

As part the broad responsibility of the trial court for its decision on questions of evidence, the court is also responsible for the quality of the evidence. An assessment of the reliability of evidence is part of this. Here too, the court is free to act: that is, there are no rules in the CCP to guide the court, nor any rules that oblige the court to reason its decision expressly in the verdict. The only exception in this regard is the previously mentioned obligation to reason the denial of an explicit defence on this point; for instance, the defence that the statement of a certain witness is not

[91] For instance, before the accused is questioned, he or she should be informed of his or her rights; in particular, the accused should be informed that he or she is not obliged to answer any questions. This informing of the accused should be filed as well. The results of a police interrogation are unlikely to be used in court against the accused if the file does not inform the trial judge that the accused was aware of his or her right not to answer any questions.

[92] Supreme Court (*Hoge Raad*) 30 March 2004, *Nederlandse Jurisprudentie* 2004/376 (with a comment by Y. Buruma), and Supreme Court (*Hoge Raad*) 19 February 2013, *Landelijk Jurisprudentie Nummer* BY5321.

[93] For instance ECrtHR (Grand Chamber) 10 March 2009, Appl. Nr. 4378/02 (Bykov v. Russia), par. 88-89.

[94] Art. 359 par. 2 CCP.

[95] R.Chr. van Halderen & K. Lasthuizen, 'Creatief gebruik van bevoegdheden', *Tijdschrift voor Veiligheid* 2013 (12) 1 , p. 16-34.

reliable, or that evidence was gained by technical methods that are argued among technical specialists, especially as to the reliability of the results and conclusions of the method.

On this point, some specific provisions in the CCP concerning technical evidence are significant, since ICT investigation is increasingly carried out by means of technical methods and the like. By January 2010, the CCP rules and provisions concerning the use of technical experts in criminal investigation had changed. The new system aims to provide for more safeguards; for instance,[96] expert investigation is only undertaken by persons recognised as experts in their field, and who are adequately certified and registered. Their reports and findings should state what method has been used, why and to what extent that method is reliable and leads to reliable results in general and/or in the concrete case, and to what extent a certain expert is sufficiently competent to apply this specific method.[97] Although the strict regime is in all its details not applicable to more or less standard methods of technical research (e.g. tests for alcohol in the blood or a test as to whether a certain amount of 'white powder' contains elements of cocaine),[98] this difference is marginal rather than substantial. The trial court can use these provisions to investigate and determine the reliability of the evidence gathered in every expert investigation, as far as the method of investigation and the professionalism of the expert is concerned, despite the difference between technical and other expert evidence.[99]

5.3 Reliability: technical demands

If ICT-related evidence is at stake, technical equipment will be used regularly to collect the information. As mentioned above, open-source research on the modality of systematic observation is done by means of technical tools, such as VIRTUOSO or iRN firmware. In this respect, it is relevant that in the Code of Criminal Procedure the legislature provides for demands regarding the use of technical tools in criminal investigations. According to Art.126ee CCP, concrete rules shall be set by way of Order or Decree of State/Order of Council for the use of technical tools.[100] Technical tools are defined as equipment that can be used to record – in a manner other than by way of sense reaffirming only[101] − signals for observation purposes. These tools must meet the requirements of the 'Decree technical tools criminal procedure' (*Besluit technische hulpmiddelen strafvordering*), which - according to Art. 126ee Sv − apply to technical tools for systematic observation.[102]

Safeguards should be provided to insure that the collected data can not be changed, that only reliable and approved tools are used, and that the registration and data mining of the results can be controlled afterwards.

The fact that a provision in the CCP provides for strict technical requirements governing the use of technical tools in criminal investigations highlights again the above-mentioned characteristic of the Dutch criminal justice system. The trial court has to assess the evidence in a number of ways. In determining the reliability of the evidence, the court must control whether the strict technical requirements have been observed in the use of specific technical equipment. If these requirements have not been observed strictly, this will normally lead[103] to the conclusion that the results of using certain technical tools in terms of information and evidence are not reliable. Information gathered as a result of a criminal investigation in which technical tools are used is reliable only when and to the extent that the use of the tools have met with the requirements. It is for the trial court in criminal cases to verify this as part of its responsibility for the quality of evidence. The reliability is to be assessed because the rules for technical tools aim to protect the traceability of data as well as to avoid the danger of data being manipulated. This traceability must be made possible for the trial judge. Even when explicitly approved and attested technical equipment is used, there is still room for the defence to assert that the equipment has not been used in a proper way, or for a purpose other than that for which it was intended.[104]

---

[96] The Bill that changed the CCP also introduced a better system for possibilities to have the results of expert investigations influenced by the defence counsel or to have it cross-examined. This provision might be ordered by the trial court on its own behalf if it thinks it necessary (Art. 315 CCP) under its tasks and responsibility concerning the proper assessment of evidence.

[97] Art. 51l CCP.

[98] Art. 150 CCP in relation to a specific guideline of the General Procuracy (*Aanwijzing van het College van Procureurs-Generaal*) from St. Peters and Pauls Day (June 29th) 2009, *Staatscourant* 2009, 18632.

[99] Cf. M.J. Dubelaar, 'Aantekening 2 bij art. 150', in: C.P.M. Cleiren & M.J.M. Verpalen (eds.), Tekst en Commentaar Strafvordering, 9th edition, Deventer: Kluwer 2011.

[100] Decree on technical tools in the criminal procedure (*Besluit technische hulpmiddelen strafvordering), Staatsblad* 2006, 524.

[101] Camera or binoculars.

[102] E.J, Koops 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift Voor Veiligheid* 2012 (11) 2, p. 38.

[103] It might be different if the outcome is of little relevance in a concrete case. See for instance Rb. Den Bosch June 14. 2012, LJN BW8620: use of uncertified equipment for stealth sms simply to insure the outcome of other, already available, evidence.

[104] Hoge Raad (Supreme Court) 12 July 2011, *Nederlandse Jurisprudentie* 2011/383.

Under the strict regime of the Supreme Court concerning the exclusionary rule relating to illegally obtained evidence, it might currently be easier to challenge the evidence on this point of its technical reliability. The above-mentioned rule of Art. 359 par. 2 CCP is applicable: namely, if during the trial the counsel or prosecutor makes an explicit defence regarding the reliability of evidence − for instance, based on demands concerning the use of technical tools − the decision to deny the defence must be reasoned in the court's verdict.

6 ICT in the Trial Stage

Although the structure of the trial stage and its procedure in the CCP – at least until 2013 – has not been changed fundamentally to include ICT elements, there have nevertheless been relevant developments in this respect.

6.1. Lady Justice goes digital:[105] long-distance interrogation by video conference

In a criminal procedure, the hearing of persons concerned (accused, witness, experts, family of victims, and so forth) is often a vital part of fair proceedings. A 'meeting' for a face-to-face hearing must be organised, and it takes time to gather all parties concerned together simultaneously. These practical problems are magnified when one of the 'stakeholders' is abroad: for instance, in pre-trial detention in another country. Despite the extend to which far-reaching traditional ways of mutual assistance in criminal matters (commissions rogatory) has increased especially within the European Union, it is essential that the trial court itself hear the person involved, being connected live by way of video communication.

A general possibility for a video conference (long-distance interrogations if necessary by satellite or another technical connection) was inserted into the Dutch CCP − and the CC as well − in 2007.[106] Video conferencing is possible for any hearing of persons in criminal proceedings, except in certain cases indicated by special decree:[107] for instance, in specific cases of sexual offences, in offences in which somebody was killed, or in the event the accused is a minor, and so on. The official (judge, prosecutor, investigating police officer) to whom the hearing is entrusted is empowered to decide on the use of a video conference, on the argument of it being in the interest of the investigation, which includes notions of fair trial. Before deciding, the official is required to consult with other parties in the criminal proceedings, but no special judicial provision for this decision is at hand, nor for the event that the official decides against the wish of any party in the proceedings.

More recently, video conferencing has used in the new political approach to speed up the completion of criminal cases involving less serious offences. A trial within three to ten days after initial arrest is one of the political aims. A video conference with the arrested person at the police station is then very useful. As a result of the Salduz ruling, it is also important that the accused be assisted by counsel in person (rather than the counsel being present only by way of a video conference). According to the applying rules,[108] confidential communication between the accused and counsel shall then be made possible, notwithstanding the open video connection with the interrogating judge or officer.

6.2. Electronic serving of documents

Could ICT help the world function better if the electronic serving of documents were possible, by email for instance, with a 'reminder mail' on the day someone is expected in court? Many people and institutions dream of this possibility. Nevertheless, the development of ICT in the Netherlands, especially in the field of criminal law, is still in the embryonic stage. We quote a recent report on the serving of documents, which highlights the situation in the Netherlands:

> 'The first step in recognizing the possibilities of electronic serving of documents should be taken by the legislator; it is not recommended to impose this modality on the field. Moreover, electronic service of documents in criminal cases due to the relevance of the judicial consequences of a legal valid serving can be considered a complicated variety of reciprocal "two-way communication", which should comply with the demands of safe communication. Therefore electronic serving of documents should be considered to be the final piece of a smooth, inevitable, and already visible development, rather than a trendsetter of a precautious development of the electronic communication between government and its citizens in many countries'.[109]

---

[105] Under this title in Dutch, see H.C. Wiersinga, 'Vrouwe Justitia gaat digital: vooruitgang?', *Nederlands Juristenblad* 2005, p. 1835-1837. See also J. Gakeer, 'De videoconferentie in kort bestek', *Trema* 2005, p. 258-262, M. van der Ende (a.o.), *Ex ante evaluatie van videoconferencing in het strafrecht en vreemdelingenbewaringszaken*, The Hague: WODC 2007.

[106] Art. 131a CCP and Art. 78a CC, respectively.

[107] See Degree on videoconferences (*Besluit videoconferentie), Staatsblad* 2006, 275 and 610.

[108] Art. 2 par 1, section b, of the Degree om videoconferences (*Besluit videoconferentie*), *Staatsblad* 2006, 275.

[109] P.A.M. Mevis, J.H.J. Verbaan & L. Postma, *Modaliteiten van betekening in rechtsvergelijkend perspectief,* The Hague: WODC 2013 (with a summary in English). The document can be found on www.wodc.nl.

Nevertheless, further steps towards introducing the possibility of lawful and effective serving of documents by means of the Internet and email may be expected in the future in the Netherlands, as well as in other countries.[110]

6.3. Use of a digital file in the trial stage

The development regarding possibilities for the electronic serving of documents is one element in a current move towards a more innovative judiciary in the Netherlands, especially involving the use of ICT tools. This process covers the civil as well as the administrative and criminal judiciary. One aspect is the move towards a general 'MyCase' portal, in which each party concerned can study the case to see the actual state of affairs.

A part of this development already in use involves a solely electronic digital process file. In some courts, a trial is conducted exclusively on a solely electronically available set of procedural documents, set down in a specially developed portal, the 'Geïntegreerd Processysteem Strafrecht' (GPS). The recognition of electronic − police and other – files, and the denunciation or accusation of a criminal act by a citizen as an official and legally recognised file (for instance, as mean of evidence), finds a basis in the CCP.[111] For this recognition, the electronic signing of a file − which must be certified properly is − necessary.[112]

Adequate preparation of the defence?

In criminal cases to date, the electronic version of the procedural documents is mainly used in minor cases dealt with in the single-judge section (*politierechter*). In these cases, the accused will normally not be kept in pre-trial detention, although it will be made possible[113] to hold someone in this manner to assure his presence in court in an accelerated procedure in which the trial must be set for a period ranging from within fifteen hours of and 17 days after the arrest. In this instance, and if the use of electronic files increases in the future and they are used in more severe criminal cases in which the accused is in pre-trial detention,[114] a serious problem under Art. 6 of the ECHR 'fair trial' guarantee may arise. A complete electronic file is of course more easily searched and accessible than a hard copy. This contributes to the guarantee for the accused regarding proper means to prepare his defence in trial. Nevertheless, to enjoy this advantage, the accused needs to have at least a computer available, even if he is in pre-trial detention. And where it is necessary to have access to all kinds of records on the literature and on court decisions − with the comments relevant to them − that are increasingly only available online, it might be an arguable plea to assert that the accused, even when in pre-trial detention, should have access to an internet connection as part of his right to prepare his defence. The Dutch prison system is not yet that far advanced on all these points.

6.4. Challenging ICT evidence: controlling the sources

After hearing the case in open court proceedings, the court may decide only on the basis of these proceedings, and on the facts and files discussed during the proceedings. This provision guarantees the right of the accused not to be convicted on evidence that has not been discussed during the trial.[115] He will at least be given the opportunity to discuss it. As an elaboration of the EcrtHR guarantee to challenge all evidence against the accused, the trial court is required to present the contents of the complete file, and must at least must refer to those contents. Any element not indicated during the trial can not be used as evidence against the accused in the court's post-trial decision.[116]

Within the cont during the pre-trial investigation ext of this right, it is essential that the accused in a given criminal case have access to all separate elements of the file. Due to a change in the CCP, which came into force in January 2013,[117] the right of access to the file is defined expressly to include access to all information recorded on electronic data carriers. Nevertheless, certain rules and possibilities restrict the right of access to the file, especially during the pre-trial investigation. These restrictions also apply to the right of access to electronic data carriers.

The complete file will consist of the results of the pre-trial investigation, as these are filed by the responsible authorities, especially by the police criminal investigators. However, since the above-mentioned adaptation of the CCP on 1 January 2013, the CCP states that the file shall contain all relevant material and information 'that might be in any way relevant for any decision the trial judge has to make'.[118] In terms of the trial court's broad responsibility regarding the assessment of evidence and of other information pertinent to its decision, it is clear that the new paragraph is highly relevant. One could argue, for instance, that this provision might indicate that if the process file contains police re-

[110] The above-mentioned publication contains an overview of and a comparison with the law of several other European Countries.
[111] Art. 153, par. 2 , and Art. 163, par. 3 CCP, respectively.
[112] Decree on the electronic report (*Besluit elektronisch proces-verbaal*), *Staatsblad* 2011, 15, effective from 1. February 2011.
[113] A proposal is still under discussion in parliament (*Kamerstukken* 33 360).
[114] It is worth noting that the use of bail or other alternatives to pre-trial detention are little known or used in the Netherlands.
[115] Art. 338, Art. 348, and Art. 350 CCP.
[116] Art. 301 CCP.
[117] Act revising rules on the pleadings in criminal matters (*Wet herziening regels betreffende de processtukken in strafzaken), Staatsblad* 2011, 601.
[118] Art. 149a par. 2 CCP

ports describing information as a summary of relevant electronic data (e.g. telephone interception, data mining, and so on), the original sources of this information should be readily available to the trial judge. He might, for instance, need to determine whether the filed summary is a proper and reliable synopsis of the complete original information. (This point was touched on earlier in the discussion of the Art. 126hh CCP provision.) In this respect, it is important that the trial court can order that new material be added to the official case file. Indeed, the court will be obliged to do so if this material and information is considered relevant for its decision. The accused and his counsel may ask the judge for such an order.

7 In conclusion

This report aims to provide a useful overview regarding current ICT developments within the Dutch criminal procedure. In this section, the most prominent conclusions are summarized.

Although no specific current legal or socio-legal definition exists for applications of ICT within the context of the Dutch criminal justice procedure, the widespread influence of ICT is visible everywhere. Especially within the police organization and the public prosecution service, specialized bodies and offices have been created, such as the High Tech Crime unit of the national police. Other offices have attempted to implement ICT in the judiciary: for instance, on the move towards the use of electronic files and the use of a MyCase app.

We have addressed the possibilities of building the information position for law enforcement agencies. In particular, the possibilities under the Special Powers of Investigation Act are relevant, including the specific ICT-related cluster of special investigation powers that can be employed for the demanding of data. Within these powers, and as a result of them, private actors such as internet providers or telecom companies are obliged to provide law enforcement agencies with data and to retain information for extended periods.

Techniques labelled as 'data mining' and 'data matching', along with other coercive measures (e.g. interception of telecommunications), can be used to build up information positions. By means of these techniques and powers, the creation of profiles of potential perpetrators or risk groups is to a certain extent possible.

During the pre-trial investigation, judicial control on building information positions can be found where the application of certain powers of investigation requires advance authorization of the examining judge. This, however, is an exception: most powers can be used by the police and the public prosecution service without (prior) judicial consent.

The Dutch legislation on trial proceedings and evidence does not contain specific provisions regarding aspects of ICT in the same elaborate and extensive manner as is needed (and was described above) for pre-trial investigation proceedings. Nevertheless, the rules and their application in an 'ICT world' require attention. The results of ICT-related information gathered in a pre-trial investigation may be made ready for use as evidence in court. Dutch law doesn't contain fixed guidelines on the admissibility of information as evidence in court. The only rule is that the information be presented to the court by one of the traditional means of evidence (*bewijsmiddelen*) that the CCP has provided for since 1926. In particular, the 'open' means of evidence of court observations and written materials − including hearsay evidence − offer unlimited possibilities to introduce all kinds of information as potential evidence in a court of law.

There is a development towards a broader use of electronic files, including possibilities for the electronic serving of documents, as well as other possibilities regarding digitalization of trial proceedings. Among them is the broad recognition of the use of video conferences: for instance, long-distance interrogations if necessary by satellite connection.

Judicial control in criminal cases is mainly part of the scope of a decision on the part of the trial court. Its broad task is to assess all aspects of the evidence, including, to a certain extent, whether the evidence was obtained legally, and whether technical conditions, formulated for the use of certain methods, were adequately observed. Included in this task of assessing evidence, the chain of collecting, storing, retaining, and producing electronic information and evidence is – to a certain degree – under the control of the trial judge. In the necessary connection between this control and the use of electronic information as evidence, there are certain limits. For example, any aspect that, for whatever reason, is not relevant for the decision on evidence is beyond this judicial control. Within the criminal system, there is scarcely any alternative judicial control relating to the chain of stages that can be distinguished where ICT and information/evidence are concerned.

In conclusion, all of the above illustrates that the possibilities relating to the use of ICT are omnipresent in the current criminal justice procedure in the Netherlands. Using ICT in a prudent, responsible, and carefully controlled manner is a challenge now, and – given the developments in criminal justice policy as well as in technical opportunities – will remain a challenge in the future.