

Published: Bert-Jaap Koops (2005), 'Cybercrime Legislation in the Netherlands', in: Pauline C. Reich (ed.), *Cybercrime and Security*, Vol. 2005/4, Dobbs Ferry, NY: Oceana Publications, p. 1-20

Cybercrime Legislation in the Netherlands

Bert-Jaap Koops¹

The Netherlands has had extensive Cybercrime legislation since the early 1990s. Particularly in the field of ICT-related investigation powers, the Netherlands has been a forerunner, providing inspiration to, for instance, the Council of Europe's 1995 Recommendation on IT-related investigation.² Since the first Dutch Computer Crime Act, however, numerous changes have taken place to meet the ongoing developments in Cybercrime. Moreover, a major revision is on its way to update the law and to implement the Council of Europe's Cybercrime Convention (CCC),³ which the Netherlands signed on 23 November 2001.

In this article, I will present an overview of Dutch Cybercrime legislation, starting with the provisions in substantive laws that criminalize Cybercrime. Next, I will describe cyber-related investigation powers. Throughout, I shall explain the current state of the law, including jurisprudence that illustrates or interprets and refines the legal provisions, as well as indicate pending proposals for changing the law.⁴

1. Preliminaries

1.1. Overview of legislative history

The main act regarding computer crime is the Computer Crime Act (*Wet computercriminaliteit*) of 1993.⁵ This is not a separate Act, but a law that adapted the Dutch Criminal Code (CC) (*Wetboek van Strafrecht*) and the Code of Criminal Procedure (CCP) (*Wetboek van Strafvordering*).⁶

The Computer Crime Act was the result of an extensive legislative process, which started in 1985 with the establishment of a Computer Crime Committee (*Commissie computercriminaliteit*), also named, after its chairman Hans Franken, the *Commissie-Franken*. The committee made a thorough analysis of both the Criminal Code and the Code of Criminal Procedure, and presented an extensive report and recommendations in 1987.⁷ This led to the Computer Crime Bill that was submitted to Parliament on 16 May 1990. The Bill largely followed the committee's recommendations, except for the search and seizure provisions.⁸ Various amendments and a heated debate in Parliament led to the definitive version of the Computer Crime Act that came into effect on March 1, 1993.

In July 1999, a follow-up bill was introduced in Parliament, the Computer Crime II Bill (*Wet computercriminaliteit II*, hereafter CCII).⁹ This is intended to refine and update several provisions of the Computer Crime Act. The parliamentary handling of the bill has been severely slowed down, however. First, the provisions on ISP liability had to be withdrawn because of the provisions on ISP liability enacted in the European Directive on electronic commerce.¹⁰ Next, the debate on the bill was postponed because of the drafting of the Cybercrime Convention, since it was thought wiser to integrate the Computer Crime II Bill with the implementation of this convention. A draft CCC Adaptation Bill to implement the Cybercrime Convention was circulated for comments in February 2004,¹¹ and was subsequently reviewed by the Council of State (*Raad van State*), which customarily

¹ Dr. Bert-Jaap Koops is Associate Professor, in Criminal Law & Technology, at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.

² Council of Europe, *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology*, September 11, 1995, available at <http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html>.

³ Council of Europe, *Convention on Cybercrime*, Budapest, November 23, 2001, <<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>>.

⁴ This article presents the state of affairs as of August 1, 2005. All translations in this article are mine.

⁵ *Staatsblad* 1993, 33. The *Staatsblad* is the Official Journal in which all Netherlands laws and most decrees are published.

⁶ The CC (*Wetboek van Strafrecht*) and the CCP (*Wetboek van Strafvordering*) are available in Dutch via <<http://www.wetten.nl>>. Case law is available in Dutch at <www.rechtspraak.nl>.

⁷ *Informatietechniek & Strafrecht. Rapport van de Commissie Computercriminaliteit*, Staatsuitgeverij, Ministerie van Justitie 1987.

⁸ See *infra*, section 3.1.2.

⁹ *Kamerstukken II* 1998/99, 26 671, nrs. 1-3. The *Kamerstukken* are Parliamentary Documents. "II" refers to the Second Chamber, "I" to the First Chamber. All documents later than January 1, 1995 can be found at <<http://www.overheid.nl/op/>>, by searching on the series number, in this case 26671.

¹⁰ Directive 2000/31/EC, *Official Journal* 17 July 2000, L178/1.

¹¹ *Wetsvoorstel Aanpassing aan het Cybercrime-Verdrag*, February 2004, <http://www.justitie.nl/images/aanpassing_aan_het>

advises the legislature on legislative proposals. Finally, on March 15, 2005, a bill to ratify the Convention was submitted to Parliament,¹² and a week later a Memorandum of Amendments to the CCII Bill was published to implement, where necessary, the CCC.¹³ Now, the CCII Bill is being discussed in Parliament again and is expected to become law sometime in 2006.

1.2. Definitions

The Computer Crime Act inserted two definitions in the Criminal Code. First, data were defined in art. 80quinquies CC as;

any representation of facts, concepts, or instructions, be the representation in an agreed-upon way or not, which is suitable for transfer, interpretation, or processing by persons or automated works.

One of the most fundamental choices in the Dutch legislation, and one of the most heatedly discussed topics in the literature, was the choice to consider data as falling outside of the scope of the term “good” (*goed*). After all, a good in the criminal law need not be tangible as such, but it is definitely unique: only one person has control over money in a bank account or electricity at the same time. Data, on the other hand, are multiple: when you “take away” data from someone, you usually copy them and the original owner may still have access to them. Likewise, goods are the subject of property law, but data are the subject of intellectual property law. The consequence of this distinction was that all provisions in the CC and CCP had to be reconsidered if they contained an element of “good”, such as theft, damage to property, and seizure.

Second, a computer – in the terminology of the Act an “automated work” (*geautomatiseerd werk*) – was defined in art. 80sexies CC as

a construction [*inrichting*] designed to store and process data by electronic means.

An earlier proposed definition was broader, but ultimately the definition was restricted to electronic devices. “The restriction to ‘electronic’ was suggested by the wish to exclude merely mechanically functioning information systems from the scope of the definition.”¹⁴ The minister noted that this was a more technology-specific definition, since the earlier “explanation spoke of the biochip. It does not seem a difficulty that this now falls outside the scope. It [the biochip] is still so far in the future that it does not have to be taken into account in the definitions now”.¹⁵

It is true that biocomputers still seem a long way off, but quantum computers are perhaps more feasible in the not too distant future. Once quantum computers appear on the market, the definition will have to be adapted.

A flaw in the current law is that these definitions are contained only in the Criminal Code, and hence are not as such applicable in the Code of Criminal Procedure. Paul Wiemans has therefore suggested to the incorporation of the same definitions in the CCP as well.¹⁶

2. Substantive cybercrime legislation

An important characteristic of Dutch criminal law is the right to exercise prosecutorial discretion (*opportuiniteitsbeginsel*). This means that the Public Prosecutor decides whether it is expedient to prosecute someone for an offense or not. A consequence of this principle for substantive law is that criminal provisions may be formulated broadly, covering many acts that may not in themselves be very worthy of criminal prosecution – the snapping of someone else’s match or the tearing apart of someone else’s newspaper are cases of damage to property (art. 350 CC), but will usually not be prosecuted by the state.

cybercrime verdrag_tcm35-45832.pdf>.

¹² *Kamerstukken II* 2004/05, 30 036, nrs. 1-3.

¹³ *Kamerstukken II* 2004/05, 26 671, nr. 7.

¹⁴ *Kamerstukken II* 1991/92, 21 551, no. 26.

¹⁵ *Handelingen II* 24 June 1992, 93-5868. The *Handelingen* are the Parliamentary Proceedings of the debates in the Second (II) and First (I) Chambers.

¹⁶ F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2004, p. 240.

2.1. Specific Cybercrime legislation

2.1.1. Hacking

Hacking is penalized in art. 138a CC. It is only punishable if someone infringes a (minimal) security measure (*enige beveiliging*). The maximum penalty is six months' imprisonment or a fine of 4,500 Euros for "simple" hacking (para. 1), and four years' imprisonment or 11,250 Euros if the hacker copies data (para. 2), or if he/she hacks via public telecommunications and uses processing capacity or hacks onwards to a third computer (para. 3).

In the legislative process leading to the Computer Crime Act, there was a debate about what level of security should be required: an absolute, maximum, adequate, minimal, or *pro forma* level of protection. The outcome was that a minimal level was sufficient. This means that there must be some form of protection, and not merely a sign saying "do not trespass", however, the protection need not be sophisticated. The security requirement was considered relevant as an incentive to induce people and companies to protect their computers, something which in the early 1990s was for many far from self-explanatory.

Currently, however, the minister has proposed to do away with the security requirement altogether. The CCII Bill will penalize trespassing in a computer as such, and mentions the breach of a security measure as an example of such trespassing.¹⁷ I consider that an odd construction, since infringing a security measure does not in itself constitute trespass. Moreover, in my opinion, it is still relevant to retain the security requirement as a sign that people should not leave their computers open to anyone who cares to drop by (or if they do, the computer owner should not complain that his/her computer was being "hacked").

It seems that several people have been convicted for hacking, but few cases have been published in the regular case-law journals.

2.1.2. Illegal interception

Interception of direct communications or non-telecom data transfer is penalized by art. 139a CC (for closed areas) and by art. 139b CC (for other areas). This currently concerns the interception by technical means of voice communications ("*gesprek*") or of data communications ("*gegevensoverdracht*"). The maximum penalty is six months or a fine of 11,250 Euros (for closed areas) or three months or a fine of 4,500 Euros (for other areas). There are exceptions for, among others, participants to the communications, employers, and security services.

Interception of telecommunications is penalized by art. 139c CC. It concerns the interception by technical means of public telecommunications. The maximum penalty is a year's imprisonment or a fine of 11,250 Euros. There are similar exceptions for, among others, participants to the communications, employers, and security services, but also for scanning wireless telecommunications without a special effort.

According to the CCII Bill, these provisions will be reshuffled, in that art. 139a-b will be restricted to intercepting conversations, and 139c will cover the interception of all other forms of communications, including data. Several other articles contain related penalizations; it is prohibited to place eavesdropping devices (art. 139d CC), to pass on eavesdropping equipment or intercepted data (art. 139e CC), and to advertize for interception devices (art. 441 CC).

2.1.3. Data manipulation and viruses

Intentional manipulation of computer-related data is penalized in art. 350a CC. This includes deleting, changing and adding data. The maximum penalty is two years' imprisonment or a fine of 11,250 Euros. If the manipulation was committed after entering the computer through a public telecommunications network and if it results in serious damage, the maximum penalty rises to four years or 45,000 Euros (para. 2). "Serious damage" includes an information system not being available for several hours.¹⁸

Non-intentional (negligent) manipulation of computer-related data is penalized by art. 350b CC, if serious damage is caused, with a maximum penalty of one month or a fine of 2,250 Euros.

Computer viruses are considered a special case of data manipulation. The intentional making available or dissemination of computer viruses is penalized by art. 350a para. 3 CC, with a maximum

¹⁷ *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 1-2.

¹⁸ Dutch Supreme Court (*Hoge Raad*) 19 January 1999, *Nederlandse Jurisprudentie* 1999, 25. *Nederlandse Jurisprudentie* is the main Dutch journal in which case law is published.

penalty of four years or a fine of 45,000 Euros.¹⁹ The unintentional (negligent) making available or dissemination of computer viruses is penalized by art. 350b para. 2 CC, with a maximum penalty of one month or a fine of 2,250 Euros.

Unfortunately, the wording of these provisions is flawed: literally, they would only cover worms, not viruses or Trojan horses; however, it is generally assumed that the provisions do cover all forms of computer viruses. In any case, the CCII Bill proposes to correct the formulation by describing viruses as data “designated (*bestemd*) to cause damage in an automated work”.

In 2001, the maker of the Kournikova virus was convicted by the Leeuwarden Court of intentional virus dissemination. He was sentenced to do 150 hours of public service (*taakstraf*). The verdict was upheld by the Supreme Court.²⁰

2.1.4. System interference, e-bombs, and DoS attacks

System interference, also referred to as computer sabotage, is penalized in various provisions, depending on the character of the system and of the interference. If the computer and networks are for the common good (“*ten algemene nutte*”), intentional interference is punishable, according to art. 161sexies CC, if the system is impeded or if the interference causes general danger (“*gemeen gevaar*”) to goods, services, or people. The maximum penalty varies from six months²¹ for impeding a system to fifteen years if the interference causes someone’s death. Negligent system interference in similar cases carries a maximum of three months to a one year imprisonment (art. 161septies CC). Another provision prohibits intentional computer sabotage (destruction or damage) of computers and telecom systems for the common good (“*ten algemene nutte*”), regardless of the effect, with a maximum punishment of three years or a fine of 11,250 Euros (art. 351 CC); negligent sabotage of such computers is penalized in art. 351bis CC with lesser penalties.

Another form of system interference, “e-bombs”, will be penalized if the Computer Crime II Bill is enacted. The proposed art. 138b CC originally prohibited the sending via the public telecoms network of data that are intended to block the recipient’s access to the telecommunications network or service. This, however, only covers e-mail bombing of specific targets, but not denial-of-service (DoS) attacks. In a DoS attack, after all, it is not so much the recipient – the server’s owner – whose access to the system is blocked, but third parties, notably the users of a website. Since the CCC, as well as the EU’s Framework Decision on attacks on information services,²² require the penalization of the “serious hindering of the functioning of a computer system”, art. 138b must be broadened. According to the amended CCII Bill, therefore, art. 138b will penalize the “intentional and unlawful hindering (*belemmeren*) of the access to or functioning of an automated work by offering or sending data to it”.²³ This will also cover DoS attacks. The new provision will have a maximum penalty of one year or a fine of 11,250 Euros.

2.1.5. Spam

Spamming as such is not covered by a penal provision, since the legislature does not consider the simple sending of spam as criminal. The newly proposed provision on e-mail bombing and DoS attacks (see section 2.1.4) will cover only serious forms of spam, notably the sending of large quantities of spam so that the functioning of a computer or network is seriously hindered; moreover, this hindering must also be the intention of the spammer for the act to be criminal. For combating all other forms of spam, Dutch law relies on private and administrative law. In private law, a specific provision on spam was inserted in the Civil Code (*Burgerlijk Wetboek*) to implement the Electronic Commerce Directive and the Directive on Privacy and Electronic Communications.²⁴ Art. 7:46h of the Civil Code broadly provides that in the context of distance selling, sending a commercial message is only allowed with prior consent of the consumer (opt-in) or, for existing customers, a continuing possibility of opting-out. Moreover, each message has to include the true identity of the sender and a

¹⁹ It is not illegal if this act is committed with the intention of restricting the damage that the virus may cause, according to art. 350a para. 4 CC.

²⁰ District Court (*Rechtbank*) Leeuwarden, September 27, 2001, LJN-number AD3861, <<http://www.rechtspraak.nl/ljn.asp?ljn=AD3861>>. Supreme Court (*Hoge Raad*) September 28, 2004, LJN-number AO7009, <<http://www.rechtspraak.nl/ljn.asp?ljn=AO7009>>. The LJN number refers to the case number on the official website on which case law is published, www.rechtspraak.nl.

²¹ To be raised to one year of imprisonment, according to the CCII Bill, *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 3.

²² Council Framework Decision 2005/222/JHA of February 24, 2005 on attacks against information systems, *Official Journal* 16 March 2005, L69/67, <http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf>.

²³ *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 2.

²⁴ Directive 2000/31/EC, *Official Journal* July 17, 2000, L178/1 (Directive on Electronic Commerce); Directive 2002/58/EC, *Official Journal* July 31, 2002, L201/37 (Directive on Privacy and Electronic Communications).

valid address for opting out. Possibly tort law (art. 6:162 Civil Code) may function as a general private law safety-net for other forms of spam that are not in line with generally accepted standards.

Art. 11.7 of the Telecommunications Act (*Telecommunicatiewet*) contains administrative provisions that mirror the civil rules of art. 7:46h of the Civil Code. A single spam-related penalization has been enacted as a corollary: art. 1 sub 2 of the Economic Offenses Act (*Wet op de economische delicten*) penalizes the anonymous sending of commercial or charitable email as an infringement of art. 11.7 para. 3 Telecommunications Act, with a maximum of six months' imprisonment or a fine of 11,250 Euros.

2.1.6. Misuse of devices

Misuse of devices, as provided for in art. 6 CCC, is currently penalized in only a few special cases:

- payment cards: art. 232 CC penalizes the provision, possession, receiving, obtaining, transport, sale or transport of a forged payment card (maximum six years' imprisonment) (art. 232 para. 2 CC);²⁵
- devices for telecom fraud: art. 326c para. 1 CC penalizes the public offering, possession with the goal of distribution or import, and making or keeping for profit (art. 326c para. 2 CC) (maximum one year imprisonment). If this happens on a professional basis, the maximum penalty increases to three years' imprisonment (para. 3);
- devices for oral or wire interception: art. 441a CC penalizes the making of publicity, with a maximum penalty of two months' imprisonment;
- devices for software-protection circumvention: art. 32a Copyright Act penalizes the public offering, possession with the goal of distribution, import, transport, export, and keeping for profit, with a maximum penalty of six months' imprisonment. This holds true only if the devices are exclusively designed ("*uitsluitend bestemd*") to circumvent software-protection measures.

The implementation of the Cybercrime Convention, however, requires a more general penalization of misuse of devices. The CCII Bill proposes to penalize:

- by art. 139d para. 2 and 3 CC: misuse of devices or access codes, with intent to commit hacking, e-bombing or DoS attacks, or illegal interception, with up to six months' imprisonment. The punishment is raised to maximum of four years if the intent is to commit aggravated hacking (as in art. 138a para. 2 or 3, see *supra*, 2.1.1);
- by art. 161sexies section 2 CC: misuse of devices or access codes, with intent to commit computer sabotage (as in art. 161sexies para. 1), with up to one year's imprisonment or a fine of 45,000 Euros.

In these provisions, following the CCC, "misuse of devices" covers the manufacture, sale, obtaining, importation, distribution or otherwise making available or having in one's possession devices that are primarily (*hoofdzakelijk*) made suitable or designed to commit a certain crime.

2.2. Relevant traditional legislation

2.2.1. Forgery

No specific penalization exists for cyber-forgery or cyber-fraud. The age-old penalizations of forgery and fraud also cover computer-related crime.

Computer-related forgery falls within the scope of the traditional provision on forgery ("*valsheid in geschrifte*"), art. 225 CC. The maximum penalty is six years' imprisonment or a fine of 45,000 Euros. The term 'writing' ("*geschrift*") has been interpreted in case law as covering computer files.²⁶

There is a specific penalization of forgery of payment cards, however. As provided in art. 232 CC,²⁷ the intentional forgery of a payment card (*betaalpas*) or value card (*waardekaart*) carries a maximum penalty of six years' imprisonment or a fine of 45,000 Euros.²⁸ The use of such a card is punishable with the same penalty (para. 2). The Computer Crime II Bill will extend this provision to cover all kinds of chip cards that are available to the general public and that are designed for payments or for other automated service provision.

²⁵ The acts of provision and possession were penalized by the Act on concentrated penalization of fraudulent acts (*Wet concentratie strafbaarstelling frauduleuze gedragingen*), *Staatsblad* 2000, 40; the other acts were penalized by the Fraud in non-circulating currency Act (*Wet fraude niet-chartaal geldverkeer*), *Staatsblad* 2004, 180.

²⁶ Supreme Court (*Hoge Raad*) January 15, 1991, *Nederlandse Jurisprudentie* 1991, 668.

²⁷ See also *supra*, section 2.1.6, on misuse of devices.

²⁸ See also Supreme Court (*Hoge Raad*) April 20, 1999, *Nederlandse Jurisprudentie* 1999, 471.

2.2.2. Fraud

Computer-related fraud falls within the scope of the traditional provision on fraud (*oplichting*), art. 326 CC. The maximum penalty is three years' imprisonment or a fine of 45,000 euros. Fraud includes the falsely obtaining of computer data that have a commercial value in the regular market (*'geldswaarde in het handelsverkeer'*). The unauthorized withdrawing of money from an ATM with a bank card and pin-code is fraud.²⁹ However, the falsely obtaining of pin codes or credit card numbers ("phishing") is not covered by the provision, as these data are not a good, nor are they tradeable on the regular market.

Other fraud-related offenses that also cover computer-related crime are extortion (*afpersing*, art. 317 CC) and blackmail (*afdreiging*, art. 318 CC). The provision on extortion was changed in 2004 in order to include obtaining of pin codes and other data under threat of violence.³⁰

Telecom fraud has been specifically penalized in art. 326c CC.³¹ The use of a public telecoms service through technical means or false signals, with the intention of not fully paying for it, is punishable with up to three years' imprisonment or a fine of 45,000 euros.

2.2.3. Content-related offenses and child pornography

Content-related offenses are punishable regardless of the medium in which the content has been published. These offenses include discrimination (art. 137c-g CC), defamation of royalty (art. 111-113 CC), defamation of friendly heads of state (art. 118-119 CC), and defamation, libel and slander (art. 261-271 CC). The aggravating circumstance of libel in writing (*smaadschrift*) will in all likelihood include publishing libellous statements by electronic means, such as in a message to a newsgroup.

Child pornography is penalized in art. 240b CC, with a maximum penalty of four years' imprisonment or a fine of 45,000 Euros. This includes the manufacture, distribution, publicity offering, and possession of pictures that show a minor in a sexual act. Doing this on a professional or habitual basis raises the maximum penalty to six years' imprisonment.

A minor is someone below 18 years of age; the age limit used to be 16 years, but following the Cybercrime Convention, the legislature chose to raise the limit to 18 years. Also following the Convention, the provision now includes virtual child pornography, which was legal until October 1, 2002.³² Virtual child pornography is indicated through inclusion of the italicized words in the clause "an act that involves *or seems to involve* someone who apparently has not reached the age of eighteen years".

2.2.4. Liability of Internet Service Providers

The liability of Internet Service Providers (ISPs) for illegal or unlawful content has been regulated as a consequence of the Electronic Commerce Directive.³³ The major portion concerns civil liability, as regulated in art. 6:196c of the Civil Code (*Burgerlijk Wetboek*). "Mere conduit" providers are not liable; caching providers are not liable if they do not change information and if they operate according to generally recognized procedures; and providers of information services are not liable if they have no knowledge of unlawful content and if they remove or make inaccessible the information as soon as they do gain knowledge.

One specific exemption from liability for ISPs has been inserted in the criminal law. Art. 54a CC determines that intermediaries who offer a telecommunications service consisting of transport or storage of data shall not be prosecuted as such³⁴ if they do all that can reasonably be asked of them to ensure that the data are made inaccessible, in response to an order from the public prosecutor. The prosecutor requires a warrant from the investigating judge for such an order, so that there is an independent check by the courts on whether the information at issue really is illegal or unlawful.

3. Procedural Cybercrime legislation

Investigation and prosecution of Cybercrime can take place through a variety of means. The whole gamut of investigation powers can be used, including search and seizure. The traditional investigation powers have been supplemented – and are still being supplemented – by several ICT-related

²⁹ Supreme Court (*Hoge Raad*) November 19, 1991, *Nederlandse Jurisprudentie* 1992, 124.

³⁰ Fraud in Non-circulating currency Act (*Wet fraude niet-chartaal geldverkeer*), *Staatsblad* 2004, 180.

³¹ See also *supra*, section 2.1.6, on misuse of devices.

³² Public Decency Revision Act of 2002 (*Wet partiële wijziging zedelijkheidswetgeving*), *Staatsblad* 2002, 388.

³³ Directive 2000/31/EC, *Official Journal* July 17, 2000, L178/1, implemented in Dutch law by the Amendment Act Electronic Commerce Directive (*Aanpassingswet richtlijn inzake elektronische handel*), *Staatsblad* 2004, 210.

³⁴ "As such" meaning that they will not be prosecuted as a liable intermediary; they may, however, be prosecuted as a content provider if they have made or selected the content themselves.

investigation powers, such as a network search and production orders for traffic data. Many of these powers can be used for crimes mentioned in art. 67 para. 1 of the Code of Criminal Procedure (CCP), that is, crimes for which pre-trial detention is allowed (hereafter “pre-trial detention crimes”). This usually concerns crimes with a maximum penalty of four years or more, plus a number of crimes with a lesser penalty that are specifically included in the pre-trial detention provision. According to the CCII Bill, almost all cybercrimes with minor penalties will be included in art. 67 para. 1, so that pre-trial detention will be allowed, even for petty forms of the crimes, and so that most investigation powers can be used to investigate the crimes.³⁵

Because the field of ICT-related investigation is very broad and complex, I can only give a brief overview of the field in this contribution, restricting myself to the major investigation powers at issue.

3.1. Powers for retrieving stored data

3.1.1. Production and preservation orders

The easiest way to retrieve information is to ask for it. In Dutch law, there is no power to request information, but there is a power to order production of data, similar to the age-old power to order production of a seizable good.

The production order used to be regulated by art. 125i Dutch CCP.³⁶ This enabled the investigating judge to order someone – who probably had access to the data sought – to provide the data or to give the judge access to the data. It could only be used for data with a certain relationship to the crime, data inserted by or meant for the suspect, data available to the suspect, or logging data. It is questionable whether, for instance, user data are covered by these, since address information does not normally fall under one of these categories. The order cannot be given to a suspect, in view of the privilege against self-incrimination (art. 125m CCP).

This article will soon be replaced by a much broader set of provisions, through the Act on Data Production Orders (*Wet bevoegdheden vorderen gegevens*), which was accepted by the First Chamber on 5 July 2005.³⁷ This allows the ordering of:

- *identifying data* by any investigating officer in case of a crime (but not a misdemeanor), according to art. 126nc CCP. Identifying data are name, address, zip code, date of birth, gender, and administrative numbers;
- *other data* by the public prosecutor in cases for which pre-trial detention is allowed, according to art. 126nd CCP; moreover, *future data* can also be ordered, including – in urgent cases and with permission of the investigating judge – real-time delivery of future data, for an extendible period of four weeks, art. 126ne CCP. This enables law enforcement officers to require production of all data that will come into being in the next few weeks or months;
- *sensitive data* by the investigating judge in case of a pre-trial detention crime that seriously infringes the rule of law, according to art. 126nf CCP. Sensitive data are data relating to religion, race, political or sexual orientation, health or labor union membership.

The orders can be given to people who process the data in a professional capacity; an order of 'other' stored data and of sensitive data, however, can also be directed at people who process data for personal use. Suspects can not, however, be ordered to provide data. If the data are encrypted, the people targeted by the production order – excluding suspects – can be ordered to decrypt them, according to art. 126nh CCP.

All of these provisions have a pendant for investigating plotted organized crime, articles 126uc-126uh CCP.

In the CCII Bill, as amended in 2005, the power to order the preservation of data is proposed.³⁸ Art. 126ni of the Dutch CCP would enable the assistant public prosecutor, in cases of crimes for which pre-trial detention is allowed and which seriously infringe the rule of law, to order someone to preserve data stored in a computer that are particularly vulnerable to loss or change. The preservation can be ordered for at most 90 days, and the order can not be given to a suspect (para. 1). If the data relate to telecommunications, the provider is also required to get the identity of other providers whose networks or services were used in the relevant communication (para 2). For investigating plotted organized crime, a similar power is proposed (art. 126ui CCP).

³⁵ *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 5.

³⁶ Inserted by the Computer Crime Act in 1993, amended by the Search and Seizure by the Investigating Judge Act (*Wet inbeslagneming en doorzoeking door r-c*), *Staatsblad* 2004, 577.

³⁷ See <<http://www.gegeven.nl>> for a website in Dutch with all relevant proposals, legislation, and critiques.

³⁸ Note that the articles mentioned (126nc-nf CCP) are articles provided by the Act on Data Production Orders, and replace existing provisions with similar production orders that were limited to financial sector information.

³⁹ *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 8-9.

3.1.2. Search and seizure

There are currently no specific provisions on searching and seizing computer-related data. When the Computer Crime Act of 1993 was debated, the legislature decided that traditional search provisions cover computer searches (see articles 96b, 96c, 97, and 110 CCP). The general seizure provisions (art. 95, 96, 96a, and 104 CCP) can be used to seize data-storage devices. Data as such can not be seized, since they are not considered “goods” (see *supra*, section 1.2), but they may be copied by law enforcement officers during a search – comparable to the copying of, for instance, fingerprint marks.

A technicality is that a search can currently only be effected for seizure or for arresting a suspect. Since data cannot be seized, a search for data investigation is theoretically impossible. (In practice, a search to seize storage devices will suffice.) The Bill on Data Ordering Provisions (*Wet bevoegdheden vorderen gegevens*), adopted by the First Chamber on July 5, 2005, will introduce in art. 125i of the CCP the power to search in order to secure data (replacing the old art. 125i CCP, *supra*, section 3.1.1).

Since in certain cases there is a need to “seize” rather than merely copy data (e.g., child porn or a virus program), the CCII Bill proposes to introduce powers to “make data inaccessible” (“*ontoegekkelijk maken*”), art. 125o CCP. This can be done with data that are the object or the means of a crime, by first copying and then deleting the data on the original device, or by encrypting them. The final deletion of the data – or the restoration – must be ordered by a judge in court, art. 354 CCP.

In 1993, a power was introduced to search a network by the Computer Crime Act. Art. 125j CCP allows the person who conducts a search to also search computer networks from computers located at the search premises. The network search, however, may only be conducted to the degree that the network is lawfully accessible to the people who regularly stay in those premises.⁴⁰ Under the current interpretation, the network search can not go beyond the Dutch borders.

Two further ancillary powers were introduced by the Computer Crime Act to the search and seizure procedures. These enable the investigating officer to order the undoing of a security measure (art. 125k para. 1 CCP) and to order the decryption, or handing over of a decryption key, of encrypted data (art. 125k para. 2 CCP). The orders may not be given to suspects (art. 125m-old para. 1 CCP).⁴¹

As general safeguards in the procedures for investigating computers and data, obligations exist to delete retrieved data as soon as they are no longer relevant for the investigation, except if they have to be used for a different case or registered in a serious crime register (art. 125n CCP), and to inform the administrator (*beheerder*) of an automated work from which data have been copied (art. 125m-old para. 3 CCP). This notification requirement is broadened by the Act on Data Production Orders (*Wet bevoegdheden vorderen gegevens*) to cover notification of suspects, the controller of the data, and the right-holders of the place searched, except in cases in which notification is not reasonably possible (art. 125m-new CCP).

3.2. Powers for retrieving telecommunications data

3.2.1. Interception

Interception of public telecommunications is regulated by art. 126m CCP. This enables the public prosecutor, with authorization from the investigating judge, to order telecommunications to be recorded, in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. There is no restriction as to suspects; in theory, everyone may be intercepted, although in practice, judges are cautious in allowing interception of people without reasonable suspicion. Art. 126t CCP contains a similar power to that in art. 126m concerning investigation of plotted organized crime.

This power is currently restricted to communications via public networks; private networks are only interceptable through direct eavesdropping (*infra*, section 3.3) or with voluntary cooperation of the private network owner. The CCII Bill, as amended in 2005, contains, however, a major revision of the interception provision. Art. 126m CCP will be amended to enable the interception with a technical device of communications not targeted at the general public which take place through the help of a communication service provider. A communication service provider is defined as someone who in a

⁴⁰ The formulation of this clause in para. 2 is rather awkward; it was improved by the Act on Data Production Orders (*Wet bevoegdheden vorderen gegevens*) of 2005.

⁴¹ This article is replaced by the Act on Data Production Orders (*Wet bevoegdheden vorderen gegevens*) of 2005. The provision that the security-undoing order may not be given to suspects is now proposed in art. 125k para. 3, according to the CCII Bill (*Kamerstukken II 2004/05*, 26 671, nr. 7, p. 5); in the period between the coming into force of the Act on Data Production Orders, expected before the end of 2005, and the coming into force of the CCII Act, which will not be before mid-2006, the security-undoing order may perhaps be given to suspects. The provision that a decryption order may not be given to suspects seemed to disappear in the legislative process, although this does not seem to be a conscious decision by the legislature.

professional capacity offers the opportunity to communicate through an automated work, or who processes or stores data on behalf of such a service or for service users (art. 126la CCP). Para. 3 of art. 126m – as proposed by the CCII Bill – determines that public telecommunications will be intercepted with the cooperation of the telecom provider, unless such cooperation is not possible or is contrary to the interest of the investigation. For all other forms of communications, the service provider will be offered the opportunity to cooperate in the interception, unless this is impossible or undesirable. Basically, the new regulation comes down to a general power to intercept transported communications (other than oral communications), whether they are transported in public or in private. According to the Explanatory Memorandum, this extension of the interception power to include private networks is mandated by the Cybercrime Convention.⁴²

Since July 1, 2004, art. 126m has included three sections on cross-border interception, following the EU Mutual Assistance between Member-States Treaty.⁴³ This allows interception from the Netherlands of someone located abroad, after the other state has given consent. Also, interception and direct transmission from another state to the Netherlands can be requested, and, conversely, the Netherlands can grant interception and direct transmission from the Netherlands to another state. In the CCII Bill, these cross-border provisions are moved from art. 126m into a separate, new article 126ma CCP.

If the intercepted communications turn out to be encrypted, an order to decrypt may in future be directed at the person who is likely to know the decryption means, but not at the suspect, according to art. 126m para. 6 and 7 CCP, as proposed in the CCII Bill.

Wiretap material has to be stored until two months after the case has definitively ended. It then must be destroyed (art. 126cc CCP), unless it is used for a different case or registered in a serious-crime register (art. 126dd CCP).

Persons with a right to non-disclosure (lawyers, public notaries, clergy, medical practitioners) cannot be wiretapped, unless they are themselves suspected of committing a crime. If in a regular wiretap a conversation with such a person acting in his or her professional capacity is recorded, it should be deleted right away. In practice, however, this has not always been done, and it is still a contentious issue.

Interceptability, that is, making sure that telecommunication networks and services are technically equipped to allow interception, as well as ensuring that telecommunications providers cooperate, is regulated by chapter 13 of the Telecommunications Act (*Telecommunicatiewet*). Art. 13.1 requires providers of public telecommunications networks or services to ensure that their network or service enables interception. This includes Internet providers. The obligation is detailed in an Order in Council and a Decree.⁴⁴ The costs for making and keeping their networks or services interceptable are borne by the telecommunications providers themselves; operational costs for concrete intercepts are borne by the state (art. 13.6 Telecommunications Act). The interceptability legislation is currently being evaluated and may be adapted in future to meet ongoing technical and market developments in telecommunications.

3.2.2. User data

The power to order production of subscriber data in general is regulated by art. 126nc and 126uc CCP, which cover identifying information (see *supra*, section 3.1.1). For telecommunications data, however, separate powers exist to order production of subscriber or user data.⁴⁵ Art. 126n, concerning traffic data (*infra*, section 3.2.3), also enables the collection of user data. A provision specifically targeted at user data, however, is art. 126na CCP. This allows any investigating officer, in case of a crime, to order a public telecommunications provider to produce user data, that is, subscriber data or data related to users of pre-paid cards.

If the provider does not have these user data available – which will often be the case with pre-paid cards – he/she may be ordered, on the basis of art. 126na para. 2 CCP, to retrieve the phone number

⁴² *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 41.

⁴³ Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Brussels, 29 May 2000, *Tractatenblad* 2000, nr. 96.

⁴⁴ Intercepting Public Telecommunications Networks and Services Decree (*Besluit aftappen openbare telecommunicatienetwerken en -diensten*), *Staatsblad* 1998, 642, adapted *Staatsblad* 2001, 262; Regulation on Intercepting Public Telecommunications Networks and services (*Regeling aftappen openbare telecommunicatienetwerken en -diensten*), *Staatscourant* 2001, nr. 107, p. 20.

⁴⁵ Traditionally, the term "subscriber data" is used for data that identify people who use telecommunications. Since people can also use telecommunications without a subscription, notably through prepaid cards in mobile telephony, currently the term "user data" is preferred.

of a pre-paid card user by data mining⁴⁶, if the police provide him/her with two or more dates, times, and places from which the sought person is known to have called. To make sure that providers have these data available, a 3-month data retention obligation is in effect (*infra*, section 3.2.3). As an alternative, the police can also, if data mining by the telecommunications provider is impossible or too inefficient, use an IMSI catcher, that is, a device that resembles a mobile phone base station and that attracts the traffic of mobile phones in its vicinity. This power is regulated by art. 126nb and art. 126ub CCP, complemented by art. 3.10 para. 4 of the Telecommunications Act to sanction the disturbing of the radio frequency spectrum. An IMSI catcher may only be used to collect someone's unknown telephone number (or IMSI number), but not to collect traffic data or to listen in on communications.

3.2.3. Traffic data and data retention

A power to order the production of telecommunications traffic data was already introduced in 1926, when the Code of Criminal Procedure was replaced by a completely new one. It is currently regulated by art. 126n CCP, which allows the public prosecutor, in cases of crimes for which pre-trial detention is allowed, to order the production of traffic and user data from public telecom providers. This can apply to not only stored data, but also incoming future data for a period of up to three months, which have to be provided real-time. Art. 126u of the CCP contains a similar power in cases of plotted organized crime.

There is a limited obligation for public telecom providers to retain data. Based on art. 13.4 para. 2 of the Telecommunications Act (*Telecommunicatiewet*) and the underlying Order in Council,⁴⁷ providers of mobile telecommunications are required to store the dates and times, cell locations, and phone numbers of pre-paid card callers, for a period of three months. This obligation was created in order to enable the retrieval of identifying data of pre-paid card users (*supra*, section 3.2.2).

The introduction of a general data-retention measure for traffic data is hotly debated in the Netherlands, as it is in the European Union. Initially, data retention was rejected by the government, but, presumably under influence of the 9/11 attacks in the United States, since late 2001, the administration has favored some sort of general mandatory data retention. Parliament, however, is more reticent, having voiced grave doubts about the effectiveness and cost-benefit ratio of such a measure.⁴⁸

3.3. Other ICT-related investigation powers

The main ICT-related investigation power (other than the powers to investigate telecommunications), is direct eavesdropping, which is similar to the U.S. power of oral interception. This is regulated by art. 126l CCP. It allows the public prosecutor to order an investigating officer to record confidential communications with a technical device, in cases for which pre-trial detention is allowed and that seriously infringe the rule of law. The prosecutor needs authorization from the investigating judge for this. A similar power exists for investigating plotted organized crime, art. 126s CCP.

Confidential communication is defined as “communication between two or more persons that takes place in private” (*in beslotenheid*); this includes communication between a keyboard, computer, and monitor, and so it covers data in transport as well. There is no restriction to suspects; in theory, everyone may be eavesdropped upon, although, in practice, judges will likely not allow eavesdropping without probable cause (*redelijke verdenking*).

Examples of relevant technical devices are directional microphones, bugs, and hardware keystroke loggers. If necessary, the power includes entering premises to place an eavesdropping device. If the premise is a dwelling (*woning*), this can only be done in cases of crimes with a maximum punishment of eight years' imprisonment or more, and the judge has to authorize it explicitly.

⁴⁶ Data mining can be defined as: “An information extraction activity whose goal is to discover hidden facts contained in databases. Using a combination of machine learning, statistical analysis, modeling techniques and database technology, data mining finds patterns and subtle relationships in data and infers rules that allow the prediction of future results. Typical applications include market segmentation, customer profiling, fraud detection, evaluation of retail promotions, and credit risk analysis.” See <http://www.twocrows.com/glossary.htm#anchor314309> (visited August 10, 2005). See also, e.g., B. Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers 2004.

⁴⁷ Decree on Special Collection of Telecommunications Number Data (*Besluit bijzondere vergaring nummergegevens telecommunicatie*), *Staatsblad* 2002, 31, in force since March 1, 2002.

⁴⁸ Overviews in Dutch of the debate and documents on data retention in the Netherlands are available at <http://www.bof.nl/verkeersgegevens.html> and at the First Chamber, in dossier 4.0.6, at <http://www.europapoort.nl/9345000/1f/j9vvy6i0ydh7th/vgq8mlyezvzt>. The EU debate on data retention is monitored – and criticized – by European Digital Rights (EDRI) at <http://www.edri.org/issues/privacy/dataretention>.

Other relevant ICT investigation powers, introduced by the Special Investigation Powers Act of 2000,⁴⁹ are:

- *undercover operations*: art. 126j and 126qa of the CCP allow law enforcement officers to systematically gather information undercover. This includes participating in Internet forums, chat groups, etc.;
- *infiltration and pseudo-purchase*: infiltration (art. 126h and 126p CCP) and pseudo-purchase (art. 126i and 126q CCP) allow investigating officers to infiltrate criminal organizations, based on the order of the public prosecutor. This includes infiltration in computer child-porn networks, chat groups, etc.; Since pseudo-purchase of data is not possible (data is not a purchasable “good”), the Computer Crime II Bill proposes to include in arts. 126i and 126q the power to buy computer data from someone via a telecommunications network. The same is also proposed for civil undercover agents (*burgerinfiltranten*) in art. 126ij CCP;⁵⁰
- *observation by technical means*: arts. 126g and 126o of the CCP allow the public prosecutor to order systematic observation. A technical device may be used for the observation, as long as this does not record confidential communication (for that, the power of direct eavesdropping, *supra*, should be used). This includes location-tracking devices, but these may not be attached to persons, only to objects;
- *preliminary investigation (verkennend onderzoek)*: art. 126gg of the CCP allows law enforcement officers to collect information about potential crime in certain sectors of society. This may include data mining;
- *hacking*: this is not allowed for law-enforcement purposes.

4. Conclusion

The 1993 Computer Crime Act has been a landmark in Dutch law, providing the necessary criminalizations and investigatory powers to meet the advent of the computer age. The substantive legislation has withstood time well: it appears to cover a good range of computer-related criminal activities. Only occasionally does it turn out to contain gaps, so that new provisions are necessary – ISP liability and DoS attacks are the most notable examples. The Cybercrime Convention furthermore necessitates penalization of the misuse of devices – evidence of a trend to increase the scope of activities considered punishable. The only omission being overlooked by the Computer Crime II Bill seems to be that “phishing” is insufficiently covered by the criminalization of fraud.

In procedural law, we see a more dynamic picture. The Netherlands was a forerunner in establishing legislation to update investigatory powers by using ICT-related investigation, including network searches and data investigation. Roughly since 2000, however, there has been an increasing trend to broaden the ICT-related investigation powers,⁵¹ notably with the Special Investigation Powers Act of 2000, and subsequently with substantial broadening of the powers to order the production of data in the Act on Data Production Orders (*Wet bevoegdheden vorderen gegevens*) of 2005. Moreover, the Computer Crime II Bill contains a major extension of the power to wiretap, by allowing interception of private-network communications as well. With ongoing discussions about data retention, the end of the trend to “computer-criminalize” society⁵² is not yet in sight.

Abbreviations used

CC	Dutch Criminal Code (CC) (<i>Wetboek van Strafrecht</i>)
CCII	Computer Crime II Bill (<i>Wetsvoorstel computercriminaliteit II</i>)
CCC	Cybercrime Convention
CCP	Dutch Code of Criminal Procedure (CCP) (<i>Wetboek van Strafvordering</i>)
IMSI	International Mobile Subscriber Identity

⁴⁹ Special Investigation Powers Act (*Wet bijzondere opsporingsbevoegdheden*), *Staatsblad* 1999, 245, in force since February 1, 2000.

⁵⁰ *Kamerstukken II* 2004/05, 26 671, nr. 11, p. 1-2.

⁵¹ See the historical analysis in B.J. Koops (2003), “The shifting ‘balance’ between criminal investigation and privacy. A case study of communications interception law in the Netherlands”, *Information Communication & Society* 6 (3) 2003, p. 380-403.

⁵² The trend is referred to in B.J. Koops (2003), ‘Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij’, *Computerrecht* 2003 nr. 2, p. 115-123, <<http://arno.uvt.nl/show.cgi?fid=5720>>.

General literature on Cybercrime in the Netherlands

English

H.W.K. Kaspersen (1994), "Computer Crimes and Other Crimes against Information Technology in the Netherlands", in: Ulrich Sieber (ed.), *Information Technology Crime*, Köln etc: Carl Heymanns Verlag 1994, pp. 343-376.

Dutch

Commissie computercriminaliteit, *Informatietechniek & Strafrecht. Rapport van de Commissie Computercriminaliteit*, Staatsuitgeverij, Ministerie van Justitie 1987.

Chr.H. van Dijk & J.M.J. Keltjens (1995), *Computercriminaliteit*, Zwolle: Tjeenk Willink 1995

H.W.K. Kaspersen (red.) (1986), *Computermisdaad en strafrecht*, Antwerpen-Deventer: Kluwer rechtswetenschappen 1986.

H.W.K. Kaspersen (1990), *Strafbaarstelling van computermisbruik*, Antwerpen/Deventer: Kluwer 1990

H.W.K. Kaspersen (1993), 'De Wet Computercriminaliteit is er, nu de boeven nog', *Computerrecht* 1993, p. 134-145.

B.J. Koops & M.H.M. Schellekens (1999), 'Computercriminaliteit II: de boeven zijn er – nu de wet weer', *Nederlands Juristenblad* 74(37), p. 1764-1772, <<http://arno.uvt.nl/show.cgi?fid=5717>>

B.J. Koops (2003), 'Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 2003/2, p. 115-123, <<http://arno.uvt.nl/show.cgi?fid=5720>>

B.J. Koops (ed.) (2004), *Strafrecht en ICT*, Monografieën Recht en Informatietechnologie deel 1, The Hague: Sdu 2004

W.Ph. Stol, R.J. van Treeck & A.E.B.M. van der Ven (1999), *Criminaliteit in Cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland*, Elsevier bedrijfsinformatie 1999.

F.P.E. Wiemans (ed.) (1991), *Commentaren op het wetsvoorstel Computercriminaliteit*, Maastricht: Cipher Management 1991.

F.P.E. Wiemans (2004), *Onderzoek van gegevens in geautomatiseerde werken*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2004

WODC (2004), *Cybercrime, Justitiële Verkenningen* 2004/8, <<http://www.wodc.nl/onderzoeken/index.asp?loc=/publicatie/justitieleverkenning>>