

Tilburg University

Cybercrime legislation in the Netherlands

Koops, E.J.

Published in:

Netherlands Reports to the Eighteenth International Congress on Comparative Law

Publication date:

2010

Document Version

Peer reviewed version

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):

Koops, E. J. (2010). Cybercrime legislation in the Netherlands. In J. H. M. van Erp, & L. P. W. van Vliet (Eds.), *Netherlands Reports to the Eighteenth International Congress on Comparative Law* (pp. 595-633). Intersentia.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Cybercrime Legislation in the Netherlands

Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes'

Prof. Bert-Jaap Koops
Professor of Regulation and Technology
TILT – Tilburg Institute for Law, Technology, and Society
Tilburg University, The Netherlands

Table of Contents

I. Introduction: Cybercrime and Cybercrime Legislation in the Netherlands	2
A. Background and aim	2
B. General characteristics of Dutch criminal law	3
C. History of Dutch cybercrime legislation	4
II. Analysis of National Cybercrime Legislation	6
A. Substantive criminal law	6
1. Offences against the confidentiality, integrity, and availability of computer systems	7
a) Hacking	7
b) Illegal interception	8
c) Data interference	8
d) System interference	9
e) Misuse of devices	10
2. Computer-related traditional offences	11
a) Computer fraud.....	11
b) Computer forgery	12
c) Data theft	13
d) Identity theft.....	14
e) Sexual offences: grooming.....	14
3. Illegal content	15
a) Child pornography.....	15
b) Racism.....	17
4. Infringements of copyright and related rights.....	18
5. Privacy (or “data protection”) offences	19
a) Privacy offences	19
b) Data protection offences	20
6. Liability of Internet service providers	20
B. Criminal procedure.....	21
1. Coercive investigation powers.....	21
a) Production and preservation orders.....	22

b) Search and seizure.....	23
c) User and traffic data.....	25
d) Interception of content data.....	26
e) Other.....	28
2. Law of evidence.....	29
3. Obligatory retention of traffic data and location data.....	30
C. Jurisdiction.....	30
D. Self-regulation and co-regulation in relation to illegal content.....	31
1 Notice and take-down.....	31
2 Filtering and blocking websites.....	32
III. The Process of Harmonisation.....	32
IV. Conclusion.....	36
Literature.....	39

I. Introduction: Cybercrime and Cybercrime Legislation in the Netherlands

A. Background and aim

In the history of cybercrime legislation, the Council of Europe’s Cybercrime Convention presents a landmark effort to harmonise national criminal law in the area of cybercrime. Its wide range of substantive, procedural, and mutual-assistance provisions as well as its supra-European scope – having been ratified, for example, by the United States – make it a potentially very valuable instrument in the fight against the intrinsically cross-border phenomenon of cybercrime. The convention, however, allows for reservations and variations in national implementation. Moreover, a series of other supranational instruments exist that also aim at harmonising specific aspects of cybercrime, including several EU Framework Decisions and EC Directives. We therefore face a patchwork of national implementations of various international legal instruments, which may result in gaps in harmonisation, variations in implementation, and a consequent lack of clarity on national standards when mutual legal assistance is being sought.

To get a grip on this international patchwork of national cybercrime laws, and to overcome undesirable divergences among countries that hamper mutual legal assistance, it is important to comprehensively map national cybercrime laws. To contribute to that mapping, this chapter provides a country report for the Netherlands, written on the occasion of the 2010 International Academy of Comparative Law Congress (Cybercrime Section). In this report, I aim to give a comprehensive overview of Dutch cybercrime legislation, both substantive and procedural, as of December 2009. I will particularly focus on the questions of how Dutch law regulates cybercrime and cyber-investigation, whether any shortcomings

exist in the legislation, and how the legislation relates to international harmonisation instruments in the area of cybercrime. This analysis will articulate in which respects the Dutch implementation falls short of its obligations under international legal instruments, and, conversely, suggest issues in Dutch cybercrime legislation that are as yet unaddressed by the international cybercrime harmonisation effort.

B. General characteristics of Dutch criminal law

For a good understanding of cybercrime legislation, some general characteristics of Dutch criminal law may be useful to mention. Criminal law is primarily codified in the Dutch Criminal Code (*Wetboek van Strafrecht*, hereafter: DCC) and the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, hereafter: DCCP).¹ Substantive law distinguishes between crimes (Second Book DCC), to which almost all cybercrimes belong, and misdemeanours (Third Book DCC). The Criminal Code has a system of maximum penalties but does not use minimum penalties. Another important characteristic of Dutch criminal law is the right to exercise prosecutorial discretion (*opportuiniteitsbeginsel*). This means that the public prosecutor decides whether or not it is expedient to prosecute someone for an offence. A consequence of this principle for substantive law is that criminal provisions may be formulated broadly, covering acts that may not in themselves be very worthy of criminal prosecution; for example, changing a single bit in a computer without authorisation already constitutes damage to data (art. 350a DCC) but will usually not be prosecuted.

The sources of Dutch law are domestic statutes and international treaties. The Dutch Constitution is not a direct source, since the courts are not allowed to determine the constitutionality of legislation (art. 120 Dutch Constitution).² Courts can, however, apply standards from international law, most visibly the European Convention of Human Rights and Fundamental Freedoms (ECHR), when deciding cases. For the interpretation of domestic statutes, parliamentary history is a leading

¹ Both Codes are available in Dutch via <http://wetten.overheid.nl>, as are all other laws and regulations of the Netherlands.

² A bill is pending to change art. 120 of the Constitution and allow constitutional review; see *Kamerstukken I*, 2004/05, 28 331, No. A. This bill has been accepted by both Chambers of Parliament in first reading, but still requires acceptance in second reading by a two-thirds majority of a newly elected Parliament.

The *Kamerstukken* are Parliamentary Documents. “II” refers to the Second Chamber, “I” to the First Chamber. All documents from after 1 January 1995 can be found at <https://zoek.officielebekendmakingen.nl/>, by searching the series number, in this case 28331. Documents from before 1995 can be found at <http://www.statengeneraaldigitaal.nl/>.

source, followed by case law³ (particularly that of the Dutch Supreme Court) and doctrinal literature.

C. History of Dutch cybercrime legislation

With respect to cybercrime legislation in the Netherlands,⁴ the most important laws are the Computer Crime Act (*Wet computercriminaliteit*) of 1993⁵ and the Computer Crime II Act (*Wet computercriminaliteit II*) of 2006.⁶ Both are not separate acts but laws that adapted the Criminal Code and the Code of Criminal Procedure. As can be observed, the term most often used in the Netherlands to indicate crimes committed with computers as a target or substantial tool is “computer crime” rather than cybercrime, which was not yet in use at the time legislation was initiated in the 1980s.

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 the *Commissie-Franken* after its chairman, Hans Franken. The committee made a thorough analysis of both the Criminal Code and the Code of Criminal Procedure, and it 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 1 March 1993.

One of the most fundamental choices in this act, and one of the most heatedly discussed topics in the literature in the 1980s and 1990s, was the choice to consider data as falling outside of the scope of the term “good” (*goed*).⁹ After all, a good in the criminal law need not be tangible as such, but it is definitely unique: only one

³ Case law is available in Dutch at <http://www.rechtspraak.nl>, indicated with reference numbers LJN.

⁴ For a comprehensive discussion of Dutch cybercrime legislation, see Koops 2007. Extensive earlier discussions can be found in Kaspersen 1990 (substantive law), Wiemans 1991, Van Dijk and Keltjens 1995, Schellekens 1999 (substantive law), and Wiemans 2004 (procedural law).

⁵ *Staatsblad* 1993, 33. The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published.

⁶ *Staatsblad* 2006, 300.

⁷ *Commissie computercriminaliteit* 1987.

⁸ See *infra*, section II(B)(1).

⁹ See, *inter alia*, *Gerechtshof* [Appeal Court] Arnhem 27 October 1983, *Nederlandse Jurisprudentie* 1984, 80 (controversially, understanding data to be a “good” that could be the object of embezzlement); *Commissie computercriminaliteit* 1987; Groenhuijsen and Wiemans 1989; Kaspersen 1990.

person has possession of money in a bank account or electricity at any one 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. Therefore, the Dutch legislator decided that computer data were not to be considered as a “good,” meaning that all provisions in the DCC and DCCP were reconsidered when they contained an element of “good,, such as theft, damage to property, and seizure. It was not until 1996 that a case reached the Dutch Supreme Court for a final verdict on the matter, and the court determined that data are indeed not a “good.”¹⁰

In July 1999, a new bill was introduced in Parliament, the Computer Crime II Bill.¹¹ This bill was intended to refine and update several provisions of the Computer Crime Act. The parliamentary handling of the bill was slowed down because of the drafting of the Cybercrime Convention (hereafter: CCC), since it was thought wiser to integrate the Computer Crime II Bill with the implementation of this convention. On 15 March 2005, a bill to ratify the convention was submitted to Parliament,¹² and a week later a Memorandum of Amendments to the Computer Crime II Bill was published that implemented, where necessary, the CCC.¹³ The Computer Crime II Act (*Wet computercriminaliteit II*) was accepted by Parliament on 1 June 2006 and entered into force on 1 September 2006.¹⁴ The Cybercrime Convention Ratification Act was accepted at the same time;¹⁵ it entered into force on 1 March 2007 for the Netherlands.

In terms of other relevant international cybercrime instruments, the Netherlands, being member of the European Union, has implemented EU Framework Decision 2005/222/JHA on attacks against information systems (hereafter: FD-AIS) in the Computer Crime II Act. It has signed but not yet ratified the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts (CETS 189); it is

¹⁰ Hoge Raad [Supreme Court] 3 December 1996, *Nederlandse Jurisprudentie* 1997, 574. The court decided that computer data could not be the object of embezzlement, since they are not a “good”: “After all, a ‘good’ as mentioned in these provisions has the essential property that the person who has actual control over it necessarily loses this control if some else takes over actual control. Computer data lack this property.” [All translations in this chapter are mine, BJK.] Incidentally, this did not help the defendant, since the court subsequently liberally interpreted the facts as embezzlement of *carriers* of computer data, and the Court of Appeal’s conviction of the defendant for embezzlement was upheld.

¹¹ *Kamerstukken II* 1998/99, 26 671, Nos 1-3.

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

¹³ *Kamerstukken II* 2004/05, 26 671, No. 7.

¹⁴ *Staatsblad* 2006, 301. The amendment to art. 273d(2) DCC (criminalising interception of communications by non-public communication providers) entered into force on 1 September 2007.

¹⁵ *Staatsblad* 2006, 299.

generally felt that Dutch law already conforms to the protocol provisions given the technology neutrality of the Dutch provisions criminalising racism. The Netherlands has also ratified the Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201); an Act to implement this convention entered into force on 1 January 2010.¹⁶

II. Analysis of National Cybercrime Legislation

A. Substantive criminal law

The Computer Crime Act inserted two definitions in the Criminal Code. First, data are defined in art. 80quinquies¹⁷ DCC as “any representation of facts, concepts, or instructions, in an agreed-upon way,¹⁸ which is suitable for transfer, interpretation, or processing by persons or automated works.”

Second, a computer – in the terminology of the Act an “automated work” (*geautomatiseerd werk*) – was defined in art. 80sexies DCC as “a construction [*inrichting*] designed to store, process, and transfer¹⁹ data by electronic means.” An earlier proposed definition was broader, but ultimately the definition was restricted to electronic devices. “The restriction to ‘electronic’ was prompted by the wish to exclude merely mechanically functioning information systems from the scope of the definition.”²⁰ 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.”²¹ The restriction to electronic functioning implies that, if somewhere in the future quantum computers appear on the market, the definition will have to be adapted.

¹⁶ *Staatsblad* 2009, 544.

¹⁷ The numbering system in Dutch Codes may seem odd to common-law countries, for example. The Criminal Code dates from 1886 and has frequently been amended since. To retain some system in the Code, new provisions have been inserted where they seem most appropriate, and they have to be numbered “in between” existing articles. In the past, this numbering was often done by adding Latin numerals – “bis”, “ter”, “quater”, “quinquies” etc. – to the article number which they follow. Currently, adding Roman letters is preferred, e.g., 138a (hacking) was inserted after 138 (trespass), subsequently followed by 138b (denial-of-service).

¹⁸ The 1993 definition used the rather cryptic formulation “whether or not in agreed-upon form” (*al dan niet op overeengekomen wijze*) to indicate the form of representation of facts, etc. Following criticism by Kaspersen (1993, p. 135) that this is a vacuous formulation, the clause “whether or not” was deleted by the Computer Crime II Act in 2006.

¹⁹ The clause “transfer” was added to the definition in 2006.

²⁰ *Kamerstukken II* 1991/92, 21 551, No. 26.

²¹ *Handelingen II* 24 June 1992, 93-5868. The *Handelingen* are the Parliamentary Proceedings of the debates in the Second (II) and First (I) Chambers.

1. Offences against the confidentiality, integrity, and availability of computer systems

a) Hacking

Hacking is penalized in art. 138a DCC as the intentional and unlawful entry into a computer or a part thereof. The maximum penalty is one year's imprisonment for "simple" hacking (para. 1), and four years' imprisonment if the hacker copies data after entry (para. 2), or if he/she hacks via public telecommunications and uses processing capacity or hacks onwards to a third computer (para. 3).

In 1993, the legislator considered hacking punishable only if someone infringes a security measure or otherwise enters a computer by devious means. As a result, the breaking of "some security measure" (*enige beveiliging*) or using a technical intervention, false signals or key, or false identity was included as a requirement for the crime. In the legislative process leading to the Computer Crime Act, the debate focused on 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, i.e., that some sort of protection exist, not merely a sign saying "do not trespass." The security requirement was considered relevant as an incentive to encourage people and companies to protect their computers, something which was far from self-explanatory for many in the early 1990s.

In 2006, however, the legislator decided to abolish the security requirement altogether. The argument held that the Cybercrime Convention and the Framework Decision on attacks against information systems did allow countries to pose a requirement of infringing security measures, but not a requirement of other types of deviance, such as using a stolen password or false identity. As a result, since the entry into force of the Computer Crime II Act, unlawfully "entering" a computer as such is punishable. The text now mentions as examples of "entry": the breach of a security measure, technical intervention, false signals or key or identity. I consider this an odd construction, since infringing a security measure or using a stolen password (which is considered a "false key") does not in itself constitute trespass. Moreover, the argument is still relevant that a security requirement functions as a warning to computer users that they should not leave their computers open to anyone who cares to drop by (or they should not complain that their computer is being "hacked").

b) Illegal interception

Illegal interception is criminalised in art. 139c DCC.²² This includes intercepting public telecommunications or data transfers in computer systems, including the interception of data between computer and keyboard or of the residual radiation from a computer screen. It excludes, however, intercepting radio waves that can be picked up without special effort, as well as interception by persons with authorised access to the telecom connection, such as employers. Covert monitoring by employers of employees is only an offence if they abuse their power.

Besides art. 139c, several other provisions contain related penalisations. Oral interception by technical devices is criminalised in art. 139a (non-public premises) and 139b (public spaces). It is also prohibited to place eavesdropping devices (art. 139d DCC), to pass on eavesdropping equipment or intercepted data (art. 139e DCC), and to advertise for interception devices (art. 441 DCC). Despite this comprehensive framework regarding illegal interception, very few cases are published in which illegal interception is indicted.

c) Data interference

Data interference is penalised in art. 350a DCC, with a maximum penalty of two years' imprisonment. This includes intentionally and unlawfully deleting, damaging, and changing data, but it goes further than the CCC and the FD-AIS by also including "adding data" as an act of interference. Although adding data does not interfere with existing data as such, it does interfere with the integrity of documents or folders, so that it can be seen as a more abstract form of data interference. There is no threshold – even unlawfully changing a single bit is an offence – but minor cases will most likely not be prosecuted, given the prosecutor's right to execute prosecutorial discretion.

If the interference was, however, committed through hacking and resulted in serious damage, the maximum penalty is higher, rising to four years' imprisonment (art. 350a, para. 2 DCC). "Serious damage" includes an information system not being available for several hours.²³ Non-intentional (negligent) data interference is penalised by art. 350b DCC if serious damage is caused, with a maximum penalty of one month's imprisonment.

Worms, computer viruses, and trojans are considered forms of a special case of data interference that is criminalised in art. 350a, para. 3 DCC. The Computer

²² Originally, the criminalisation was spread across different provisions by the Computer Crime Act, including penalisations of computer communications interception in closed premises (art. 139a para. 2) or in public spaces (art. 139b para. 2) and of public telecommunications interception (art. 139c). They were integrated into art. 139c by the Computer Crime II Act.

²³ Hoge Raad [Dutch Supreme Court] 19 January 1999, *Nederlandse Jurisprudentie* 1999, 25.

Crime Act of 1993 used an awkward formulation to criminalise viruses: “data intended to cause damage *by* replicating themselves in a computer” [emphasis added]. Since only worms cause damage by the act of replication, this effectively only covered worms but not viruses or trojans. Still, it was generally assumed that the provision covered most forms of malware through a teleological interpretation, in view of the intention of the legislator to penalise viruses. The Computer Crime II Act of 2006 replaced the text with a better formulation by describing viruses as data “designated to cause damage in a computer.” Even though trojans or logic bombs do not as such cause damage *per se* in a computer, they are covered by this provision, according to the explanation in the Explanatory Memorandum.²⁴

d) System interference

System interference is penalised in various provisions, depending on the character of the system and of the interference. If the computer and networks are for the common good, intentional interference is punishable if the system is impeded or if the interference causes general danger (*gemeen gevaar*) to goods, services, or people (art. 161sexies DCC). Negligent system interference in similar cases is also criminalised (art. 161septies DCC). Even if no harm is caused, computer sabotage is still punishable when targeted at computers or telecommunication systems for the common good (art. 351 and 351bis DCC).

Whereas these provisions, all dating from the first wave of cybercrime legislation, concern computers with a “public value,” a relatively new provision concerns any computer interference. Art. 138b DCC was included in the Computer Crime II Act to combat e-bombs and particularly denial-of-service (DoS) attacks: the “intentional and unlawful hindering of the access to or use of a computer by offering or sending data to it.”

Although DoS attacks were thus criminalised only in 2006, prosecutors and courts were able to apply the “public-value” provisions to some DoS attacks before 2006. The blockers of several government websites used for official news – including www.regering.nl (“administration.nl”) and www.overheid.nl (“government.nl”) – were convicted on the basis of art. 161sexies DCC to conditional juvenile detention and community service of 80 hours.²⁵ Another district court interpreted, somewhat creatively, the hindering of an online banking service as constituting “common danger to service provisioning.”²⁶ However, a DoS attack on a single commercial website was found not punishable under the pre-2006 law.²⁷

²⁴ *Kamerstukken II* 1998/99, 26 671, No. 3, p. 48.

²⁵ Rechtbank [District Court] The Hague 14 March 2005, LJN AT0249.

²⁶ Rechtbank [District Court] Breda 30 January 2007, LJN AZ7266 and AZ7281.

²⁷ Gerechtshof [Appeal Court]’s-Hertogenbosch 12 February 2007, LJN BA1891.

Spamming is not criminalised in the Criminal Code but regulated in art. 11.7 Telecommunications Act with an opt-in system (or opt-out for existing customers); violation of this provision is an economic offence (art. 1(2) Economic Offences Act). The supervisory authority, OPTA, has fined spammers with hefty fines in several cases.

e) Misuse of devices

Misuse of devices has been penalised through the Computer Crime II Act in art. 139d, paras. 2-3 and 161sexies, para. 2 DCC. Art. 139d, para. 2 covers the misuse of devices or access codes with the intent to commit a crime mentioned in art. 138a (hacking), 138b (e-bombing or DoS attacks), or 139c (illegal interception) with punishment of up to one year imprisonment. In para. 3, the punishment is raised to a maximum of four years if the intent is to commit aggravated hacking (as in art. 138a, para. 2 or 3, see above). Misuse of devices or access codes with the intent to commit computer sabotage (as in art. 161sexies, para. 1) is covered by art. 161sexies, para. 2 DCC.

In these provisions, following the Cybercrime Convention, “misuse of devices” covers the manufacture, sale, obtaining, importation, distribution or otherwise making or having available devices that are primarily (*hoofdzakelijk*) made suitable or designed to commit a certain crime, or the sale, obtaining, distribution, or otherwise making or having available computer passwords, access codes, or similar data that can be used to access a computer.

An omission of the legislator is the misuse of devices with intent to commit data interference, such as spreading computer viruses. This is covered by the Cybercrime Convention, but the target offence of data interference in art. 350a DCC is not included in the new provisions on misuse of devices. The legislator argued that spreading viruses (art. 350a, para. 3 DCC) is itself a preparatory crime, and therefore refrained from criminalising misuse of devices for data interference.²⁸ The legislator’s argument is flawed, however, because the Dutch criminalisation of spreading a virus was introduced as criminal attempt of data interference rather than as a preparatory crime.²⁹ Moreover, preparation of spreading viruses, such as making or possessing a virus toolkit, is not covered by art. 350a, para. 3 DCC, but it certainly falls within the scope of art. 6 CCC as part of the black market of cybercrime tools that art. 6 is supposed to combat.³⁰ This constitutes one of the rare instances where the Netherlands has insufficiently implemented the Cybercrime Convention.

²⁸ *Kamerstukken II* 2004/05, 26 671, No. 7, p. 36.

²⁹ *Kamerstukken II* 1990/91, 21 551, No. 6, p. 39.

³⁰ Explanatory Memorandum to the Cybercrime Convention, §71.

Besides the new provisions on misuse of devices to implement art. 6 CCC, three provisions already existed that criminalised specific types of misuse of devices:

- art. 234 DCC penalises misuse of devices (goods or data) that the perpetrator knows to be designated for the commission of aggravated forgery (art. 226, para. 1 sub 2-5) or card forgery (art. 232, para. 1), with a maximum of four years' imprisonment;³¹
- art. 326c, para. 2 DCC penalises with a maximum of two years' imprisonment the public offering of, possession with the goal of distribution or import of, and making or having available for profit devices or data that are ostensibly designated for the commission of telecommunications fraud (art. 326c, para. 1 DCC). If this happens on a professional basis, the maximum penalty increases to four years' imprisonment (para. 3);
- art. 32a Copyright Act penalises the public offering of, possession with the goal of distributing, importing, transporting, exporting, and making available for profit devices for software-protection circumvention, 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.

2. Computer-related traditional offences

a) Computer fraud

Computer-related fraud falls within the scope of the traditional provision on fraud or obtaining property or services through false pretences (*oplichting*), art. 326 DCC, with a maximum penalty of four years' imprisonment. For example, the unauthorized withdrawing of money from an ATM with a bank card and pin-code is fraud.³² The Computer Crime Act of 1993 added that fraud includes deceiving someone into providing computer data with economic value in the legal market (*geldswaarde in het handelsverkeer*), such as computer programs or address databases. However, falsely obtaining pin codes or credit card numbers was not covered by this provision, as these data are not tradable on the legal market but only on black markets. As a result, phishing for personal or financial data did not constitute fraud if the data were merely being collected without being used.³³ This lacuna was only recently addressed by, oddly enough, an omnibus anti-terrorism

³¹ The term “data” was included in this provision by the Act of 21 April 2004 (*Staatsblad* 2004, 180) to cover, for example, computer programs designated for forging traveller's cheques or shares, thus implementing the European Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment, *OJ* 2.6.2001, L149/1.

³² Hoge Raad [Supreme Court] 19 November 1991, *Nederlandse Jurisprudentie* 1992, 124.

³³ Koops and Wiemans 2005.

law, which replaced “data with economic value in the legal market” simply with “data.”³⁴

Other fraud-related offences that also cover computer-related crime are extortion (art. 317 DCC) and blackmail (art. 318 DCC). The provision on extortion used a similar clause as that for fraud, but here the clause “data with economic value in the regular market” had already been replaced by “data” in 2004,³⁵ so that it includes the obtaining of pin codes and other data under threat of violence. For blackmail, this clause was similarly changed by the aforementioned anti-terrorism Act in 2009.³⁶

A special case of fraud is telecommunications fraud, which is specifically penalised in art. 326c, para. 1 DCC: the use of a public telecommunications service through technical intervention or false signals, with the intention of not fully paying for it. This is punishable with up to four years’ imprisonment.

b) Computer forgery

Computer-related forgery falls within the scope of the traditional provision on forgery (art. 225 DCC), which criminalises “forgery in writing” (*valsheid in geschrift*) with a maximum penalty of six years’ imprisonment. In a landmark case, the term “writing” (*geschrift*) in this provision was interpreted as covering computer files.³⁷ This so-called “Rotterdam computer fraud” case concerned an administrative civil servant working for the municipality of Rotterdam, who added fraudulent payment orders to the automated payment accounts system. The court formulated two criteria for a computer file to serve as a “writing” in the sense of art. 225 DCC: it should be able to be made readable (i.e., the electronic or magnetic signs should be translatable into any understandable language, including computer languages), and it should be stored on a medium with sufficient durability. Even though, in the present case, the fraudulent orders were inserted in a temporary, intermediate file that only existed for a few minutes, the court held that the file had a legal purpose, since it was an essential link in the chain of proof of the accounts system, and that, under these circumstances, the file had been stored with sufficient durability. Since this case, computer forgery can be prosecuted on the basis of art. 225 DCC.

Apart from the general provision on forgery, there is a specific penalisation of forgery of payment or value cards (art. 232, para. 1 DCC), introduced by the Computer Crime Act in 1993. In the Computer Crime II Act, this provision was

³⁴ Act of 12 June 2009, *Staatsblad* 2009, 245, entry into force on 1 July 2009 (*Staatsblad* 2009, 263).

³⁵ *Staatsblad* 2004, 180.

³⁶ *Staatsblad* 2009, 245.

³⁷ Hoge Raad [Supreme Court] 15 January 1991, *Nederlandse Jurisprudentie* 1991, 668.

extended 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 provisioning. This provision has been used in several cases to prosecute phone debit-card fraud and skimming. Art. 232, para. 2 DCC penalises the use, provision, possession, receiving, obtaining, transport, sale, or transfer of a forged payment or service card with a maximum of six years' imprisonment.³⁸

c) *Data theft*

Although theft – taking away property – does not cover appropriation of data (see *supra*, Introduction), the Dutch legal doctrine that data are not a “good” seems ripe for revision. With the advent of virtual worlds like Second Life and World of Warcraft, in which data constituting virtual property increasingly seems to acquire real-life economic value, the arguments underlying the doctrine no longer seem entirely convincing. In these virtual worlds, objects exist that do not consist of “multiple” data but of data that are in the (almost³⁹) unique possession of a platform or game user. Moreover, some of these objects, like valuable weapons or shields or fancy clothes, can only be acquired by investing significant time and/or money in the virtual world, and a market is emerging where such objects are traded.

Two Dutch cases have been published that apply a new interpretation of “goods.” The most notable one concerned two boys playing the multiplayer online role-playing game of Runescape, who joined another boy at his home, where they hit the boy and forced him to log on to the game. They subsequently pushed him away from the computer and transferred a virtual amulet and mask from the victim's account to their own account. The District Court and Appeal Court Leeuwarden held that the two boys had stolen goods, since they had taken away data that were unique (only one person could possess them at one point in time) and that had economic value.⁴⁰ The other case concerned three fourteen-year-old boys who, in Habbo Hotel, a popular virtual platform for children, had taken away pieces of furniture from other users by logging into their accounts with passwords acquired through a phishing website. The juvenile court convicted the offenders for hacking as well as for aggravated theft (art. 311 DCC).⁴¹

³⁸ The acts of provision and possession were penalised by the Act on concentrated penalization of fraudulent acts, *Staatsblad* 2000, 40; the other acts were penalised by the Fraud in Non-circulating Currency Act, *Staatsblad* 2004, 180, implementing European Framework Decision 2001/413/JHA.

³⁹ They are usually also under the control of the platform or game provider.

⁴⁰ Rechtbank [District Court] Leeuwarden 21 October 2008, LJN BG0939; Gerechtshof [Appeal Court] Leeuwarden 10 November 2009, LJN BK27764 and BK2773.

⁴¹ Rechtbank [District Court] Amsterdam 2 April 2009, LJN BH9789, BH9790, and BH9791.

These cases have been endorsed by some in the literature as a sensible re-interpretation of the doctrine concerning “computer data as goods.”⁴² It will be interesting to see whether and, if so, under what kinds of circumstances other courts will follow this line of reasoning.

d) Identity theft

Identity theft or, somewhat broader, identity fraud refers to committing an unlawful act, typically fraud, by using the identity of someone else or of a non-existing person. It is largely a two-stage process of collecting identification and personal data (stage 1) and using them to commit the unlawful activity (stage 2). Usually, the activities of stage 2 will be punishable under a variety of existing criminal provisions, such as fraud, theft, forgery, or impersonation. The stage 1 activities could fall under cybercrime provisions, such as hacking or illegal interception; they could also, perhaps, be considered criminal attempts to commit the target offence.

The patchwork of potential offences to qualify identity theft is not an ideal situation, particularly not for victims reporting the crime to the police. It is therefore being discussed in the Netherlands whether a separate criminal offence of identity theft should be introduced.⁴³ So far, however, no proposals have been published for a separate identity theft offence.

e) Sexual offences: grooming

Grooming consists of paedophiles establishing a trust relationship with a minor in order to subsequently meet for sexual abuse. Online grooming, i.e., using the Internet to establish trust, is criminalised by the Lanzarote Convention (CETS 201), in art. 23: “the intentional proposal, through information and communication technologies, of an adult to meet a child (...) for the purpose of committing [a sexual offence], where this proposal has been followed by material acts leading to such a meeting.” The sexual offences at issue are having sex with a child under the legal age for sexual activities and producing child pornography. In this provision, the preparatory act of arranging a meeting and, for example, booking a train ticket constitutes a crime, regardless of whether the meeting actually takes place or not. Of course, a key issue is whether it can be proven that the meeting has the purpose of having sex or creating (child-porn) images, which requires considerable circumstantial evidence.

⁴² Hoekman and Dirkzwager 2009. Contra: Moszkowicz 2009.

⁴³ De Vries *et al.* 2007, p. 254; Dutch Cabinet, *Tweede Voortgangsrapportage Veiligheid begint bij voorkomen*, 30 October 2009, p. 67. Similar discussions are taking place at the EU level; see, e.g., Commission Communication *Towards a general policy on the fight against cyber crime*, COM (2007) 267final, p. 8.

The Netherlands has swiftly implemented the Lanzarote Convention, criminalising grooming in a new provision, art. 248e DCC.⁴⁴ The provision is somewhat broader than the Lanzarote Convention in that it criminalises using *a computer or a communication service* to propose a meeting with a minor under the age of 16 with the intention of committing sexual abuse or creating child pornography, if any act is performed to effectuate such a meeting. The maximum penalty is two years' imprisonment.

3. Illegal content

Content-related offences are punishable regardless of the medium in which the content has been published. These offences include discrimination (art. 137c-g DCC), defamation of royalty (art. 111-113 DCC), defamation of friendly heads of state (art. 118-119 DCC) as well as defamation, libel, and slander (art. 261-271 DCC). 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.

a) Child pornography

In Dutch law, child pornography is penalised in art. 240b DCC, carrying a maximum penalty of four years' imprisonment. This includes producing, distributing, publicly offering, and possessing images that show a minor engaged in a sexual act. Doing this on a professional or habitual basis raises the maximum penalty to eight years' imprisonment.⁴⁵ In order to conform with the Cybercrime Convention's recommended standard, the age limit for child pornography was raised from 16 to 18 years in 2002.⁴⁶

Although prosecutorial priority is given to child-porn production and commercial distribution, many prosecuted cases involve intentional possession of child pornography by individual users. Of particular relevance from the perspective of computer crime evidence is *when* a computer user can be considered to intentionally possess child-porn images found on his hard disk, given that computer users are not always aware of, for example, temporary Internet files or unallocated clusters (deleted files that can be retrieved with forensic software). The courts generally apply the standard that someone is criminally liable for possessing child

⁴⁴ *Staatsblad* 2009, 544.

⁴⁵ This penalty was raised by the omnibus anti-terrorism Act of 12 June 2009, *Staatsblad* 2009, 245, from six to eight years, in order to allow the special investigation power of direct interception (see *infra*, section B(1)(e)), in particular breaking into a house to place a bug in a suspect's keyboard, for example, in order to retrieve passwords or encryption keys. This investigation power, when it involves trespassing a house, can only be used in cases carrying a maximum penalty of at least eight years' imprisonment. See *Kamerstukken II* 2007/08, 31 386, No. 3, p. 9.

⁴⁶ *Staatsblad* 2002, 388.

pornography on his hard disk if he is aware of the presence of these files, has power of disposal over these files, and has the intention of possessing them; in other words, he should know, be able, and want. In applying this standard, the courts look at a range of factors, many of which relate to whether or not the defendant had been actively involved in child pornography, for example, by searching for or frequently viewing child porn on the Internet.⁴⁷

Until recently, watching child pornography without actually possessing it was not criminalised. This has changed with the implementation of the Lanzarote Convention that came into effect on 1 January 2010.⁴⁸ Art. 240b DCC has been extended to include “intentional access” as a criminal act. To prevent accidental stumbling across online child pornography from being criminalised, evidence should show that the defendant was actively focusing on accessing child pornography, for example by paying for access to a restricted-access website.⁴⁹

In 2002, to implement the Cybercrime Convention, virtual child pornography was included as a punishable offence in art. 240b as sexual images “seemingly involving” a minor (*waarbij (...) schijnbaar is betrokken*). “Seeming” to involve a minor is a vaguer standard than the term “realistic image” used in the Cybercrime Convention, raising questions as to how this element should be interpreted. The legislator has given different explanations, ranging from a high level of realism – “The image looks like the image of a real child. The image is indistinguishable from a real picture”⁵⁰ to “the image should *at first sight* be indistinguishable from real”⁵¹ and even to a considerably lower level of realism: “Children’s interest can be equally at issue in cases where the images are less realistic. Also images that are not evidently lifelike [*levensecht*] can, for example, suggest sexual child abuse or be part of a subculture that advances sexual child abuse.”⁵²

To date, only one case of criminal virtual child pornography has been published; in this case, the latter (lower) standard was applied. A man possessed a cartoon movie, “Sex Lessons for Young Girls,” showing a young girl engaged in sexual activity with an adult man. The court considered this sufficiently realistic because an average child would not be able to distinguish between real and cartoon people. The “average child,” in this court’s opinion, is a relevant yardstick for cartoon movies like this one that are intended – as indicated by the title and form – as a sex course for young children. A conviction for virtual child pornography therefore

⁴⁷ Stevens and Koops 2009, based on a survey of over fifty Dutch cases of hard-disk possession of child pornography.

⁴⁸ *Staatsblad* 2009, 544.

⁴⁹ *Kamerstukken II* 2008/09, 31 810, No. 3, p. 4.

⁵⁰ *Kamerstukken II* 2001/02, 27 745, No. 6, p. 16.

⁵¹ *Kamerstukken II* 2001/02, 27 745, No. 6, p. 14 [emphasis added].

⁵² *Aanwijzing kinderpornografie* (artikel 240b WvSr) [Guideline child pornography (art. 240b DCCP), *Staatscourant* [Official Gazette] 2007, No. 162, p. 8.

fitted the rationale of combating a subculture that promotes child abuse.⁵³ The particular circumstances of the case – such as the title of the movie and the fact that it was actually shown to a young child – are likely to have played a role in the emphasis of this decision on this rationale. To date, this is the only conviction for virtual child pornography in the Netherlands, and it remains to be seen whether courts will adopt this particular court’s interpretation using the perspective of a minor to interpret the term “realistic” in future cases.

b) Racism

A bill is pending for ratification of the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts (CETS 189).⁵⁴ The acts covered by the protocol, however, are already criminal under existing legislation, since the provisions on racism do not refer to the media and hence are also applicable in an online context.⁵⁵ These provisions are thus regularly applied to Internet publications.⁵⁶ Art. 137c DCC penalises insult to communities, i.e., utterances in public – orally, in writing, or with images – that are intentionally insulting to population groups on the basis of their race, religion, philosophy of life, sexual orientation, or handicap. Art. 137d DCC similarly penalises discrimination or inciting hatred of people on these grounds. Both offences are punishable by a maximum imprisonment of one year, or, if done professionally or customarily or in alliance with others, two years. Art. 137e DCC criminalises the publication of discriminatory statements as well as dissemination or stocking of data carriers with discriminatory utterances for dissemination purposes, if done other than for the purposes of professional reporting. This offence is punishable with a maximum of six months’ imprisonment, or, if done professionally or customarily or in alliance with others, one year imprisonment. Finally, participating in or supporting discriminatory activities is punishable on the basis of art. 137f DCC with maximally three months’ imprisonment, and discriminating people in the performance of a profession or business is punishable with six months’ imprisonment (art. 137g DCC).

The only provision from the protocol that is not as such criminalised yet in the Netherlands, is art. 6, concerning denial, gross minimisation, approval or justification of genocide or crimes against humanity. This offence is also included in art. 1 para. 1 sub (c) and (d) of the EU Framework Decision on racism and

⁵³ Rechtbank [District Court]’s-Hertogenbosch 4 February 2008, LJN BC3225.

⁵⁴ *Kamerstukken II* 2008/09, 31 838, Nos 1-4.

⁵⁵ For a general overview, see De Roos, Schuijt and Wissink 1996.

⁵⁶ See, for example, Gerechtshof [Appeal Court] Amsterdam 17 November 2006, LJN AZ3011 on convicting someone for publishing discriminatory statements about Jews and homosexuals on a website.

xenophobia.⁵⁷ Often, genocide denial is nevertheless punishable on the basis of art. 137c, 137d, or 137e DCC, since these statements are generally insulting or discriminatory for the groups subjected to the genocide or crimes against humanity.⁵⁸ To make genocide denial more visibly punishable, a bill was proposed to criminalise “negationism” in a new provision, art. 137da DCC, which would fully cover the acts mentioned in art. 6 of the protocol.⁵⁹ This bill has largely lain dormant since its submission in June 2006 and, despite reintroduction in July 2009, still awaits discussion in Parliament.

4. Infringements of copyright and related rights

In Dutch law, copyright law is usually enforced by private law, but the Copyright Act 1912 (*Auteurswet 1912*, hereafter: Copyright Act) contains several relevant criminal provisions. Art. 31 of the Copyright Act criminalises intentional infringement of someone else’s copyright, which is punishable with a maximum imprisonment of six months. Intentionally offering for dissemination, stocking for multiplication or dissemination, importing or exporting, or keeping for pursuit of gain of an object containing a copyright infringement is punishable with maximally one year of imprisonment (art. 31a Copyright Act), which increases to four years’ imprisonment if done as a profession or business (art. 31b). Articles 34 through 35d contain further offences, the most important of which is the intentional altering of copyrighted works in a way that is potentially harmful to their creator (art. 34).

For cybercrime purposes, the aforementioned art. 32a Copyright Act is particularly relevant. This provision criminalises misuse of devices, without consent, for circumventing copyright-protection measures that protect software. This offence, punishable with up to six months’ imprisonment, was introduced to comply with the Software Directive, 91/250/EEC (1991). In contrast to the misuse of devices of art. 6 Cybercrime Convention, art. 32a only concerns devices *exclusively* (rather than primarily) targeted at software-protection circumvention.

The Copyright Directive 2001/29/EC contains a provision more similar to art. 6 Cybercrime Convention in that it declares unlawful misuse of devices primarily targeted at circumventing copyright-protection measures of copyrighted works. This provision has been implemented in Dutch private law rather than criminal law: Art. 29a Copyright Act defines as tort the intentional circumvention of effective technical measures (paragraph 2) and the misuse of devices primarily designed to circumvent effective technical measures (paragraph 3(c)).

⁵⁷ Framework Decision 2008/913/JHA of 28 November 2008, *OJ* L328/55, 6.12.2008.

⁵⁸ See, for example, Rechtbank [District Court]’s-Hertogenbosch 21 December 2004, LJN AR7891 on finding someone guilty of discrimination (art. 137c DCC) for publishing a website in Dutch with a text titled “The Holocaust that never was”.

⁵⁹ *Kamerstukken II* 2005/06, 30 579, Nos 1-3.

5. Privacy (or “data protection”) offences

a) Privacy offences

Several offences in the Criminal Code concern violations of spatial or relational privacy, such as trespass (art. 138 DCC), but they generally do not relate to computer crime, with the exception of unlawful communications interception.⁶⁰ Of relevance for cybercrime, however, is the criminalisation of stalking in art. 285b DCC. This is defined as the unlawful systematic violation of another person’s privacy (*persoonlijke levenssfeer*) with the objective of forcing that person to do, or not to do, or to tolerate something, or of intimidating him/her; it carries a maximum penalty of three years’ imprisonment. Few court cases have been published concerning cyberstalking as such; in practice, most stalking cases comprise combinations of physical and electronic means of harassment. The Supreme Court has hinted that repeatedly making obscene phone-calls to someone might constitute stalking.⁶¹ A lower court ruled that posting threatening messages on the fan website of a famous person could not be considered stalking, since the duration of the posting (two days) was too brief for the behaviour to be considered systematic.⁶² Sending loads of email, sms, and Hyves⁶³ messages over months or years, however, is a clear case of stalking.⁶⁴ Various courts have also punished the placing of announcements on dating websites by a user purporting to be another person, thus causing that person to receive unsolicited email responses, such as stalking.⁶⁵ Similarly, creating a profile page with pictures of someone else on the social-network site Hyves – in combination with other harassing activities – can also be considered stalking.⁶⁶

Somewhat related to cybercrime are the offences of secretly making visual images of people. If a person uses a camera, the presence of which has not been explicitly been made known, to intentionally and unlawfully take pictures or make video recordings of someone, he/she can be punished with up to six months’ imprisonment if the pictures were recorded in non-public places (art. 139f DCC) or up to two months’ imprisonment if they were recorded in public spaces (art. 441b DCC).

⁶⁰ See *supra*, section II(A)(1)(b).

⁶¹ Hoge Raad [Supreme Court] 9 December 2003, LJN AL8452.

⁶² Rechtbank [District Court] Rotterdam 28 April 2009, LJN BI2713.

⁶³ Hyves is the most popular social-network site in the Netherlands.

⁶⁴ Rechtbank [District Court] Breda 30 October 2009, LJN BK1696.

⁶⁵ Rechtbank [District Court] Zutphen 13 July 2004, LJN AQ1722; Gerechtshof [Appeal Court] Arnhem 21 November 2006, LJN AZ4330; Gerechtshof [Appeal Court]’s-Hertogenbosch 28 May 2009, LJN BI5701.

⁶⁶ Rechtbank [District Court] Groningen 1 November 2007, LJN BB6924.

b) Data protection offences

Behaviour that violates informational privacy – or data protection – could, in some cases, be prosecuted on the basis of data interference (art. 350a DCC, see above), but there is no provision in the criminal law that specifically targets data protection violations. The Data Protection Act (*Wet bescherming persoonsgegevens*, hereafter: DPA) is largely enforced by private or administrative measures. The DPA criminalises only three acts in art. 75:

- failure to notify the Data Protection Authority of personal data processing (unless an exemption applies);
- processing of personal data on Dutch territory by a data controller established outside of the European Union, if the controller has not designated a person or organisation in the Netherlands who complies with the DPA on his behalf;
- transfer of personal data to a third country outside of the EU if this has been prohibited by ministerial order.

These activities can be punished with a maximum fine of 3,350 Euros or, when committed intentionally, with imprisonment of at most six months. The literature has suggested, on the basis of examples from other EU Member States, that more types of violations of data-protection rules should be enforced by criminal provisions rather than civil or administrative measures.⁶⁷

6. 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.⁶⁸ The major part 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 of it.

One specific exemption from liability for ISPs has been inserted into the criminal law. Art. 54a DCC determines that intermediaries who offer a telecommunications service consisting of transport or storage of data shall not be prosecuted as such⁶⁹ if

⁶⁷ Nouwt 2005.

⁶⁸ 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.

⁶⁹ “As such” means that they will not be prosecuted as liable intermediaries; they may, however, be prosecuted as content providers if they have made or selected or otherwise contributed to the content themselves. Cf. *Gerechtshof [Appeal Court] Leeuwarden* 20 April 2009, LJN BI1645.

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.

B. Criminal procedure

In contrast to the Criminal Code, the Code of Criminal Procedure lacks definitions of “data” and “computer,” and the DCC definitions do not as such apply to the DCCP. Paul Wiemans has therefore suggested incorporating the same definitions in the DCCP as well.⁷⁰

1. Coercive investigation powers

Investigation powers can be used for investigation offences, depending on the invasiveness of the investigation power and the seriousness of the offence under investigation. A commonly used threshold for allowing investigation powers is that the crime allows pre-trial detention, which is generally the case for crimes carrying a maximum of at least four years’ imprisonment (art. 67, para. 1 under a DCCP), but which is also possible for certain specifically mentioned offences (art. 67, para. 1 under b DCCP). Because digital investigation powers may also be required for “simple” cybercrimes, for example hacking without aggravating circumstances, the Computer Crime II Act has inserted almost all cybercrimes specifically into art. 67, para. 1 under b DCCP. As a result, for most cybercrimes, pre-trial detention is allowed, regardless of their maximum penalty, and most investigation powers can be used to investigate them.

Investigation and prosecution of cybercrime can take place through a variety of means. The entire gamut of investigation powers can be used, including search and seizure. Traditional investigation powers have been supplemented by several computer-related investigation powers, such as a network search and production orders for traffic data. Many powers were introduced in 2000 by the Special Investigatory Powers Act (*Wet bijzondere opsporingsbevoegdheden*),⁷¹ which inserted a complex set of provisions into the DCCP. This set has subsequently been extended several times. It comprises:

- investigation powers focused on criminal investigation of a *concrete crime* based on probable cause in articles 126g through 126ni;
- by and large the same provisions focused on investigating committed or *planned organised crime* in articles 126o through 126z;

⁷⁰ Wiemans 2004, p. 240.

⁷¹ *Staatsblad* 1999, 245.

- again the same type of provisions but now focused on investigating *terrorist crimes* (which can start on the basis of mere “indications” rather than on the normal standard of “reasonable suspicion” (*redelijke verdenking*)) in articles 126za through 126zu; and
- some *general provisions* on, for example, notification, data storage, and data mining, in articles 126aa through 126ii.

In this section, I will restrict myself to the set of provisions for investigating a concrete crime.

a) *Production and preservation orders*

The Computer Crime Act created a data production order in art. 125i DCCP, enabling the investigating judge to order someone – who probably had access to the data sought – to provide data or to give the judge access to data if these data had a certain relationship to the crime or the suspect or logging data. The power was somewhat restricted and appeared insufficient, and therefore a much broader set of provisions entered into force in January 2006 with the Data Production Orders Act (*Wet bevoegdheden vorderen gegevens*).⁷² These provisions allow the ordering of:

- *identifying data* by any investigating officer in case of a crime (but not a misdemeanour), according to art. 126nc DCCP. 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 DCCP; 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 DCCP). 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 DCCP. Sensitive data are data relating to religion, race, political or sexual orientation, health, or labour-union membership.

The orders can be given to persons who process the data in a professional capacity; an order for “other” stored data and sensitive data can, however, also be

⁷² *Staatsblad* 2005, 390. The provisions established in this Act (126nc-nf DCCP) replaced existing provisions with similar production orders that were limited to financial service providers. These provisions had been introduced earlier than the general production orders, by Act of 18 March 2004, *Staatsblad* 2004, 109, to implement in time the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C326 of 21.11.2001, see *Kamerstukken II* 2001/02, 28 353, No. 3, p. 1-2.

directed at persons who process data for personal use. Suspects cannot, however, be ordered to provide data, in view of the privilege against self-incrimination. If the data are encrypted, the persons targeted by the production order – excluding suspects – can be ordered to decrypt them, according to art. 126nh DCCP.

The Computer Crime II Act introduced a power to order the preservation of data, as required by the Cybercrime Convention. Art. 126ni DCCP enables the 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 a period of at most 90 days (extendible once). If the data relate to communications, the communications provider is also required to provide the data necessary for retrieving the identity of other providers whose networks or services were used in the relevant communication (para 2).

b) Search and seizure

There are no specific provisions on searching and seizing computer-related data. When the Computer Crime Act of 1993 was debated, the legislator decided – contrary to the suggestions of the Computer Crime Committee – that traditional search provisions cover computer searches (see articles 96b, 96c, 97, and 110 DCCP). After all, a search comprises the systematic and in-depth looking for something, and it includes the power to break, where necessary, security measures; a computer, in this respect, is no different from a closet or safe. The general seizure provisions (art. 95, 96, 96a, and 104 DCCP) can be used to seize data-storage devices. Data as such cannot be seized, since they are not considered “goods,”⁷³ but they may be copied by law-enforcement officers during a search – comparable to making images of, for instance, the crime scene or fingerprint marks.

A theoretical technicality was, however, that a search could only be effected for seizure or for arresting a suspect. Since data cannot be seized, a search for data investigation purposes was theoretically impossible. (In practice, though, a search to seize storage devices sufficed.) The Data Production Orders Act therefore introduced in art. 125i DCCP (replacing the old art. 125i DCCP, *supra*, section B(1)(a)) the power to search in order to “secure” (*vastleggen*) data.

Since, in certain cases, there is a need to “seize” rather than merely copy data (e.g., child porn or a virus program), the Computer Crime II Act introduced powers to “make data inaccessible” (*ontoegankelijk maken*), art. 125o DCCP. 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 definitive deletion of the data – or their restoration, if the making inaccessible was unjustified – must be ordered by a judge in court (art. 354 DCCP).

⁷³ See *supra*, section I.

The Cybercrime Convention also includes a power to conduct a network search if, during a search, relevant data appear to be stored elsewhere on a network. The Netherlands had already enacted such a power in the 1993 Computer Crime Act. Art. 125j DCCP 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 are regularly present on those premises.⁷⁴ Under the current interpretation, the network search cannot go beyond the Dutch borders. No information or experience is available yet on how the Netherlands will interpret the Cybercrime Convention's exception for an extraterritorial network search with lawful consent from a lawful authority (art. 32 CCC).

A further ancillary power to the search and seizure procedures was introduced by the Computer Crime Act. It enables the investigating officer to order the undoing of a security measure (art. 125k, para. 1 DCCP) and to order the decryption of, or handing over of a decryption key for, encrypted data (art. 125k, para. 2 DCCP). The orders may not be given to suspects, in view of the privilege against self-incrimination (art. 125k, para. 3 DCCP).⁷⁵ These orders could initially be given *while* the officer conducted a search or network search, which was felt to be too restrictive, since computers were often seized and investigated at the office only some time *after* the search. Therefore, the formulation was adapted in the Computer Crime II Act, but for some reason or other the legislator replaced "during a search" with "when article 125i or article 125j has been applied." The legislator apparently overlooked the fact that art. 125i only concerns a search to secure data, not a regular search on the basis of articles 96b, 96c, 97, or 110, and that, in practice, a search will most often be conducted based on one of these other articles. This implies that security-undoing or decryption orders cannot be given for computers or data carriers seized during normal searches. This was undoubtedly not the intention of the legislator, but the clear wording of art. 125k hardly allows for an analogous, teleological interpretation to cover other forms of searches. Moreover, it does not cover other situations in which computers are seized, for example when someone is stopped or arrested on the street and his/her laptop or pda is seized; this gap already existed under the old Computer Crime Act legislation⁷⁶ but has so far not been addressed by the legislator.

⁷⁴ The formulation of this clause in para. 2 was rather awkward; it was improved by the Data Production Orders Act of 2005.

⁷⁵ Something went wrong in the legislative process when the provision that the orders may not be given to suspects was transferred from art. 125m-old to art. 125k, para. 3, since the former had been abolished by the Data Production Orders Act as of 1 January 2006 and the latter only came into effect with the Computer Crime II Act on 1 September 2006. During the interval, the security-undoing order could theoretically have been given to suspects.

⁷⁶ Koops 2000, p. 19.

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 be registered in a serious crime register (art. 125n DCCP) – and to inform the persons involved when data have been copied or made inaccessible. The persons to be notified are suspects (unless they are automatically informed through the case file), 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 DCCP).

c) *User and traffic data*

When the general and comprehensive regime for production orders (*supra*, under (a)) was prepared in the mid-2000s, a separate regime was established for telecommunications data, based on the argument that this sector had an longstanding, well-functioning, and in some respects singular practice of providing data to law enforcement, in particular providing real-time access to future traffic data.

The provision specifically aimed at obtaining user data is art. 126na DCCP. In case of a crime, it allows any investigating officer to order a communications service provider⁷⁷ to produce user data: name, address, telecommunications number, and type of service. Art. 126n, concerning traffic data (*infra*), also comprises the collection of user data.

If the provider does not have these user data available – which is often the case with prepaid cards – he/she may be ordered, on the basis of art. 126na, para. 2 DCCP, to retrieve the phone number of a prepaid card user by comparing registries; the police then supplies the provider with two or more dates, times, and places from which the sought person is known to have called. In order to make sure that providers have these data available, a three-month data retention obligation was established (*infra*, under 3). As an alternative, if the comparison of registries by the telecommunications provider is impossible or too inefficient, the police can also 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 DCCP and complemented by art. 3.10, para. 4 Telecommunications Act (*Telecommunicatiewet*) to sanction the interference 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 eavesdrop on communications.

The power to order the production of communications traffic data is regulated by art. 126n DCCP, 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

⁷⁷ See *infra*, note 83 and surrounding text.

communications service providers. This can apply to stored data but also to incoming future data for a period of up to three months, and they have to be provided real-time. Traffic data are listed in an Order in Council as comprising names and telecommunications numbers of sender (and of the person who pays for his/her subscription) and recipient,⁷⁸ data, time, duration, cell location in the mobile network,⁷⁹ numbers of peripheral equipment, and types of services used.⁸⁰

d) *Interception of content data*

Interception of communications content is an important investigation power in the Netherlands, which is used very frequently – more than in most other countries.⁸¹ Art. 126m DCCP enables the public prosecutor, with authorisation from the investigating judge, to order the recording of communications that are generated by means of a communications service provider's service. Interception is permitted in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. If the intercepted communications turn out to be encrypted, an order to decrypt may 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 DCCP.

Since 2000, there is no longer a restriction that the interception has to target suspects; in theory, everyone may be intercepted, as long as this measure can be considered as contributing to the investigation, for example when people in the vicinity of a suspect are likely to reveal relevant information. Persons with a right to nondisclosure (lawyers, public notaries, clergy, medical practitioners), however, cannot be intercepted, unless they are themselves suspects; if, during a regular wiretap, a conversation with such a person on duty is recorded, it must be deleted (art. 126aa, para. 2 DCCP). In practice, however, conversations with attorneys frequently appear to be stored and included in case files; to address this long-standing contentious issue, a system has now been proposed in which designated phone and fax numbers of attorneys are automatically recognised and excluded from interception.⁸²

⁷⁸ Recipient number includes Internet addresses, such as which websites were visited, including the URLs of individual pages within a website. *Kamerstukken II 2001/02*, 28 059, No. 3, pp. 7-8.

⁷⁹ The cell location of mobile phones is considered traffic data when the phone is used for an actual (or attempted) communication, but not when the phone is merely in stand-by mode. *Kamerstukken II 2001/02*, 28 059, No. 3, p. 8.

⁸⁰ Art. 2 Telecommunications Data Production Decree (*Besluit vorderen gegevens telecommunicatie*), *Staatsblad 2004*, 394.

⁸¹ Interception statistics have only been officially published since late 2007. In 2008, 26,425 interception orders were given; on average, 1946 intercepts were in operation every day. *Kamerstukken II 2008/09*, 30 517, No. 13.

⁸² *Kamerstukken II 2008/09*, 30 517, Nos. 8 and 12.

Until 2006, interception was restricted to communications via public telecommunications networks. To meet the demands of the Cybercrime Convention, the power was broadened by the Computer Crime II Act to include all communications service providers. A communications service provider is defined in art. 126la DCCP as a natural or legal person who professionally offers to the users of his service the opportunity to communicate by means of a computer, or who processes or stores data for the benefit of such a service or the service's users. This comprises both public telecommunications providers and private providers of closed communication networks, such as internal company networks. The Explanatory Memorandum notes that the definition has been closely modelled on the definition of a service provider in art. 1 under c of the Cybercrime Convention.⁸³

For the default mode of interception, a distinction is made between public and private service providers. Art. 126m, para. 3 DCCP 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 communication, para. 4 stipulates that the service provider will be offered the opportunity to cooperate in the interception, unless this is impossible or undesirable.

Since 1 July 2004, some forms of cross-border interception are allowed,⁸⁴ following the EU Mutual Assistance between Member-States Treaty.⁸⁵ Art. 126ma CCP 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.

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 networks or services enable interception. This includes Internet providers. The obligation is detailed in an Order in Council and a Decree.⁸⁶ The costs for making and keeping

⁸³ *Kamerstukken II* 2004/05, 26 671, No. 7, p. 41.

⁸⁴ *Staatsblad* 2004, 107, adding three paragraphs to art. 126m DCCP, which were transferred to a new article, art. 126ma DCCP, by the Computer Crime II Act in 2006.

⁸⁵ Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 29 May 2000, *OJ C*197/1, 12.7.2000.

⁸⁶ Intercepting Public Telecommunications Networks and Services Decree (*Besluit aftappen openbare telecommunicatienetwerken en -diensten*), *Staatsblad* 1998, 642; Regulation on Intercepting Public Telecommunications Networks and Services (*Regeling aftappen openbare telecommunicatienetwerken en -diensten*), *Staatscourant* 2001, No. 107, p. 20, both amended subsequently several times.

their networks or services interceptable are borne by the telecommunications providers themselves; operational costs for concrete interceptions are borne by the state (art. 13.6 Telecommunications Act). The interceptability legislation was evaluated in 2005, in light of technical and market developments in telecommunications, but this did not lead to substantial changes.⁸⁷

e) Other

Another major computer-related investigation power is direct interception. Art. 126l DCCP allows the public prosecutor, with authorisation from the investigation judge, 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. 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 thus covers data in transport as well. Examples of relevant technical devices are directional microphones, bugs, and keystroke loggers. If necessary, the power includes entering premises to install an eavesdropping device; if the premise is a dwelling, this can only be done if the crime carries a maximum punishment of at least eight years’ imprisonment and the judge has explicitly authorised the measure.

Other than breaking into a premise to install a technical interception device (such as a keystroke logger) and the power to conduct an online network search while doing a regular search (*supra*, under (b)), the police has no power to remotely search or hack into computers.⁸⁸

The police do have several other relevant computer-related investigation powers, introduced by the Special Investigation Powers Act of 2000:

- *Undercover operations*: Art. 126j DCCP allows law-enforcement officers to systematically gather information undercover. This includes participating in Internet forums, chat groups, etc.
- *Infiltration and pseudo-purchase*: Infiltration (art. 126h DCCP) and pseudo-purchase (art. 126i DCCP) allow investigating officers to infiltrate criminal organisations on the public prosecutor’s order.⁸⁹ This includes infiltration of computer child-porn networks, chat groups, etc., and the officers can pretend they want to buy or pay for access to online child pornography (art. 126i was extended by the Computer Crime II Act to include the pseudo-purchase of computer data).

⁸⁷ See Koops *et al.* 2005 and *Kamerstukken II* 2005/06, 30 517, Nos. 1-3.

⁸⁸ Koops 2007, pp. 118-119; contra: Boek 2000.

⁸⁹ See Siemerink 2000 for a discussion of online infiltration and pseudo-purchase.

- *Observation by technical means*: Art. 126g DCCP allows the public prosecutor to order systematic observation. A technical device may be used for the observation, as long as it does not record confidential communication (for this, the power of direct eavesdropping, *supra*, should be used). It includes location-tracking devices, but they may not be attached to persons, only to objects.
- *Preliminary investigation (verkennend onderzoek)*: Art. 126gg DCCP allows law-enforcement officers to collect information about potential crime in certain sectors of society; data mining is a primary tool to this end.⁹⁰ If the preliminary investigation focuses on a terrorist crime, the prosecutor can, with authorisation from the investigating judge, order the production of databases, and combine them with other databases for data mining, in contravention of the limitations of the Police Registries Act (art. 126hh DCCP).⁹¹

2. Law of evidence

The yardstick for conviction is that the trial judge has obtained the inner conviction that the defendant is guilty of the offence, based on the statutory means of evidence (art. 338 DCCP). The statutory means of evidence are the judge's own observation, statements in court from the defendant, witnesses, and experts, and written documents (*schriftelijke bescheiden*) (art. 339 DCCP). Written documents include various official documents that have evidential value on their own and all "other writings" that count only in relation to the contents of other means of evidence (art. 344, para. 1 DCCP). An official report by an investigating officer has special evidential value, since it can constitute proof that the defendant committed the charged facts (art. 344, para. 2 DCCP). Reports by investigating officers can currently be drafted only in signed paper form, but electronic reports will be made possible in the near future (art. 153 DCCP).⁹²

The "other writings" of art. 344, para. 1 DCCP are independent of a medium and can include electronic documents, as long as they can be read aloud. Forensic digital evidence can thus be used in court in various ways: as official documents written by experts, as expert statements made in court, as official reports by investigating officers describing their observations, or as observations by the judge when the evidence is demonstrated on a computer in court.

⁹⁰ See Sietsma 2006 for a discussion of data mining as an investigation power.

⁹¹ The Police Registries Act (*Wet politieregisters*) was replaced by the Police Data Act (*Wet politiegegevens*) in 2008; the legislator forgot at the time to update the reference in art. 126hh DCCP, which will be repaired by an Omnibus Act, *Staatsblad* 2009, 525, not yet in force.

⁹² *Stb.* 2005, 470, adding a clause to art. 153, para. 2 that an electronic report has the same status as a signed written report, if it conforms to the requirements stipulated by Order in Council. This provision has not yet entered into force, pending the Order in Council.

3. Obligatory retention of traffic data and location data

In 2002, the Netherlands introduced a limited obligation for public telecommunications providers to retain data. Based on art. 13.4, para. 2 of the Telecommunications Act (*Telecommunicatiewet*) and the underlying Order in Council,⁹³ providers of mobile telecommunications are required to store the dates and times, locations, and phone numbers of prepaid card callers for a period of three months. This obligation was created in order to enable the retrieval of identifying data of prepaid card users (*supra*, B(1)(c)).

To implement the European Data Retention Directive,⁹⁴ a comprehensive data retention regime for traffic data has been established. The government initially proposed a retention period of 18 months,⁹⁵ which was reduced by the Second Chamber to 12 months. The First Chamber was critical of the bill but accepted it after the Minister promised to submit an amending bill that would further reduce the retention period for Internet service providers to six months.⁹⁶ The Telecommunications Data Retention Act (*Wet bewaarplicht telecommunicatiegegevens*) entered into force on 1 September 2009;⁹⁷ the promised amending bill has yet to be submitted to the Second Chamber. The data to be retained by telecommunication providers are listed in the Appendix to the Data Retention Act.

C. Jurisdiction

Substantive jurisdiction is set out first and foremost in art. 2 DCC, which provides that the Code “is applicable to anyone guilty of any offence in the Netherlands.” Art. 4 DCC provides jurisdiction grounds for many specific offences committed outside of the Netherlands. This includes forgery, extending to computer forgery, committed abroad by Dutch government employees (art. 4(11) *juncto* 225 DCC) and computer sabotage or data interference committed against a Dutch national if the act is related to terrorism (art. 4(13-14) *juncto* 161sexies and 350a DCC).

Art. 5 DCC establishes jurisdiction for certain crimes committed outside of the Netherlands by Dutch nationals. This includes publishing corporate secrets acquired by accessing a computer (art. 5, para. 1 under 1 *juncto* 273 DCC) and child pornography (art. 5, para. 1 under 3 *juncto* 240b DCC). Jurisdiction also exists for child pornography committed by foreigners with a fixed residence in the

⁹³ Decree on Special Collection of Telecommunications Number Data (*Besluit bijzondere vergaring nummergegevens telecommunicatie*), *Staatsblad* 2002, 31.

⁹⁴ Directive 2006/24/EC, *OJ L*105/54, 13.4.2006.

⁹⁵ *Kamerstukken II* 2006/07, 31 145, No. 2.

⁹⁶ *Handelingen I* [Parliamentary Proceedings First Chamber] 7 July 2009, 40-1858.

⁹⁷ *Staatsblad* 2009, 333.

Netherlands, even when they come to reside in the Netherlands after the crime has been committed (art. 5a DCC).

The Computer Crime II Act has established jurisdiction over almost all cybercrimes from articles 2 through 10 of the Cybercrime Convention, when committed by Dutch nationals abroad, in a new section in art. 5, para. 1 under 4 DCC. In addition, racist, discriminatory, libellous, slanderous, and threatening crimes from articles 3 through 6 of the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts when committed by Dutch citizens abroad will soon also be subject to Dutch jurisdiction.⁹⁸

D. Self-regulation and co-regulation in relation to illegal content

1 Notice and take-down

The provision on ISP liability in the Criminal Code, art. 54a DCC (*supra*, section A(6)) has the semblance of a notice-and-take-down (NTD) procedure in that it suggests that the public prosecutor can order an ISP to remove content deemed illegal. However, there is no mirroring provision in the Code of Criminal Procedure that establishes a power for the prosecutor to order removal of content, and, in light of the procedural legality principle, a substantive law provision on ISP liability cannot be considered a basis for a law-enforcement power. In addition, other arguments, such as a lack of legal protection for the stakeholders, indicate that art. 54a DCC cannot be considered a legal basis for an NTD procedure.⁹⁹ Legislation is now being prepared to provide an NTD procedure for illegal content in a law-enforcement context.

In the meantime, co-regulation has created an NTD procedure for unlawful content. Stimulated by the NICC, the Netherlands Infrastructure Cybercrime, an NTD code of conduct was drafted by government and industry, which was accepted in October 2008. The code of conduct can be adopted by ISPs or other intermediaries on the Internet. It provides guidelines for dealing with notifications of unlawful or illegal content. In case of formal notification by a public prosecutor, in line with art. 54a DCC, the intermediary simply takes down the content. In other cases, the intermediary evaluates on the basis of the notification whether the content is unequivocally unlawful (*onmiskenbaar onrechtmatig*) – the standard applied in tort cases on liability for unlawful content. If so, then the intermediary removes the content, if not, the intermediary informs the notifier accordingly. If the intermediary cannot readily judge the unequivocal unlawfulness of the material, he will inform the content provider with the request to remove the material or to contact the notifier. If the notifier and content provider do not come to an agreement, the notifier can report the content to the police or, in case of unlawful

⁹⁸ *Staatsblad* 2009, 525, has not yet entered into force.

⁹⁹ Schellekens, Koops and Teepe 2007.

content under civil law, bring his/her dispute before the courts. In the latter case, if the content provider is unwilling to make himself/herself known to the notifier, the intermediary can decide to provide the notifier with the content provider's name and contact details or to remove the content in question.¹⁰⁰

2 Filtering and blocking websites

In the Netherlands, initiatives to filter and block websites with illegal content have, so far, been restricted to websites containing child pornography.¹⁰¹ In 2007, in a co-regulatory effort, several ISPs and the Netherlands Police Agency (KLPD) signed an agreement to the effect that the ISPs would block child-porn websites based on a blacklist created by the KLPD.¹⁰² The KLPD drafts the blacklist using, inter alia, the national child-pornography database, but also blacklists from other countries with a similar system, such as Norway. In principle, only foreign websites are blocked in this way; for Dutch-hosted websites, a notice-and-takedown order is preferred; in practice, however, some websites hosted in the Netherlands are blacklisted as well. The blocking occurs on the level of domain names; users trying to access a blacklisted webpage get to see a "Stop" page, which includes a police email address where the user can complain if he/she thinks the website was unjustly blocked.

The co-regulatory effort has recently been stepped up in a new Platform Internet Safety (Platform Internetveiligheid).¹⁰³ The child-porn hotline, Meldpunt Kinderporno op Internet, a private party, will henceforth be responsible for the blacklist.¹⁰⁴

III. The Process of Harmonisation

Having extensively surveyed Dutch cybercrime legislation, we can observe that the Netherlands has, in general, very faithfully implemented international legal instruments in the area of cybercrime. All the relevant EC Directives and EU Framework Decisions have been implemented, and national legislation has been, or is being, updated to meet the standards of the international treaties and conventions to which the Netherlands is a party. The only pertinent objection that could be

¹⁰⁰ See art. 6 Code of Conduct, available at http://www.samentegencybercrime.nl/NTD/Download_the_code_of_conduct?p=content.

¹⁰¹ See, extensively, Stol *et al.* 2008, in particular pp. 88-102, on which this paragraph is based.

¹⁰² The legality of these agreements can be disputed, since the KLPD has no formal power to block Internet traffic; making agreements with private parties to do so is at odds with the rule of law and the public-law checks and balances to which the KLPD is subject. *Ibid.*, p. 98.

¹⁰³ See <http://www.ecp.nl/platform-internetveiligheid>.

¹⁰⁴ Speech by the Minister of Justice, 8 December 2009, available at http://www.ecp.nl/sites/default/files/Toespraak_mvj_8december2009.pdf.

made regarding Dutch implementation of international instruments is that the legislator is frequently slow: for example, the Electronic Commerce Directive was transposed more than two years late, the transposition of the Data Retention Directive was two years late for telephone data, and it took almost five years to adapt Dutch law to the Cybercrime Convention.

On the positive side, however, it should also be observed that the Netherlands has been a frontrunner in cybercrime legislation in some respects, particularly with its provisions on procedural law dating from the Computer Crime Act of 1993. Several powers introduced then, such as the network search and the power to order undoing of security measures, may well have inspired the drafters of the Cybercrime Convention, not least because the Dutch chairman of the convention's drafting committee PC-CY, Rik Kaspersen, had been closely involved in the legislative process of the Computer Crime Act.¹⁰⁵

The process of implementing international harmonisation instruments occurs quite smoothly overall, almost as a matter of course. The Dutch legislator hardly ever questions provisions from EU or Council of Europe instruments but takes it for granted that they have to be implemented in national legislation. The provisions of international instruments are rarely challenged in the parliamentary process; if a harmonisation instrument leaves room for the national legislator, for example the retention period of the Data Retention Directive, parties in the Second and First Chambers may argue about the implementation, but always within the margins set by the international instrument. Moreover, Parliament rarely forces the government to make reservations when ratifying conventions; significantly, no reservations were made with respect to the Cybercrime Convention, even though the convention allows reservations in several provisions.

In fact, most international instruments are not often debated as such. The (staff of the) Minister pays attention to them when drafting bills, who indicates in Explanatory Memorandums why and how certain provisions are needed in light of a particular international harmonisation instrument, sometimes illustrated with transposition tables showing which Convention or Directive article is transposed in which national provision. However, the harmonisation background – for example, the scope or interpretation of particular terms of the Cybercrime Convention – no longer plays a substantial role in the rest of the parliamentary discussion.

Although the harmonisation effort proceeds quite smoothly, it does tend to slow down the legislative process. In particular, the Computer Crime II Act has suffered long delays because of international harmonisation instruments. The original bill, submitted in July 1999, had to be amended in April 2000 already, following a

¹⁰⁵ With good reason, the editors entitled the *Liber Amicorum* presented to Kaspersen on the occasion of receiving his emeritus status: *Caught in the Cyber Crime Act* (Lodder and Oskamp 2009).

standstill decision from the European Commission that its provisions on ISP liability diverged from the Electronic Commerce Directive regulation.¹⁰⁶ Subsequently, after the parliamentary preparatory committee had submitted an extensive set of questions to the Minister in September 2000, the Minister decided to postpone debate on the bill pending the Cybercrime Convention's coming into being. The convention prompted a thorough review of existing and proposed cybercrime legislation to see which gaps existed, and the consequent extensive amendment proposal to the Computer Crime II Bill had to follow the same basic procedure as the original bill, i.e., be circulated for comments to stakeholders and submitted to the Council of State for advice. The amendment was submitted in March 2005, and the parliamentary committee's questions from 2000 were finally answered in May 2005. The rest of the process went quite speedily, but, all in all, it had taken over seven years to update cybercrime legislation. This delay was warranted for the issues affected by the Cybercrime Convention, but the Computer Crime II Bill also contained numerous amendments unrelated to the convention, and they would have merited more expeditious treatment by the legislator.

A final observation to make about the impact of harmonisation instruments on national legislation is that, in general, the provisions from conventions and EU instruments fit well within the Dutch legal system; with a few exceptions, they have not led to significant changes in the scope or nature of criminalisation or criminal investigation in the area of cybercrime.

The exceptions, however, are not insignificant. A major systematic change has been the abolishment of the security requirement for hacking (*supra*, section II(A)(1)(a)). The Computer Crime Act of 1993 introduced as a threshold for criminal liability that a security measure be infringed or that access have taken place through devious means, such as technical intervention or a false key. The legislator argued that both the Cybercrime Convention and the Framework Decision on attacks against information systems do allow for a security measure as a condition for liability, but not for other conditions such as a false key. As a result, to meet the requirements of the international instruments, the legislator abolished the security requirement altogether. This reading by the Dutch legislator of the Convention and Framework Decision can be questioned; in my opinion, the "devious means" mentioned on a par with infringing a security measure in the former Dutch provision also imply that a certain security measure is in place (or why else should an intruder employ devious means to enter the computer?). In light of the rationale of the security requirement as articulated by the national legislator in 1993 – incentivising computer users to secure their computers – it is to be lamented that the, perhaps flawed, interpretation of international instruments triggered the Dutch legislator to change the criminalisation of hacking in 2006.

¹⁰⁶ *Kamerstukken II* 1999/2000, 26 671, No. 5.

Another exception is the interception of communications via communications service providers. Dutch law only allowed wiretapping of public telecommunications, and, since the Cybercrime Convention's definition of service provider also includes private communication providers, the procedural powers were extended by powers to intercept private communications, for example closed company networks, in 2006. This was a major shift in policy, which, even though it concerned implementation of the convention's requirements, would have merited more discussion in Parliament and in the media than it did; as it happened, the broadening of investigation powers was hardly debated. Moreover, the change in policy led to a change in concepts: "providers of public telecommunications" was replaced by "providers of communications services" in the provisions on interception and traffic data. However, this was not done systematically; art. 1251a DCCP, for example, which regulates searching a telecommunication provider's computers, still refers to "providers of public telecommunication networks or services," implying that it does not apply to a search of a private communications provider. And art. 273 DCC, which criminalises the unlawful opening by a provider of communications not addressed to him, refers to *telecommunications* providers rather than communications providers. Altogether, the implementation of the Cybercrime Convention's term "service provider" has not contributed to improving the system of the Dutch cybercrime legislation.

A final exception is the Cybercrime Convention's provision on misuse of devices, which has been implemented with the same maximum punishment as the target offences. In the Dutch legal system, inchoate crimes usually carry less punishment than result crimes. The general criminalisation of preparation of crimes, for example, carries half the punishment for the crime under preparation (art. 46 DCC), and criminal attempt carries two-thirds of the maximum punishment (art. 45 DCC). Applying equal punishment to the preparation of cybercrimes as the cybercrimes themselves is therefore a significant divergence from the existing system that is not necessitated by the international instrument itself but caused, instead, by a conscious choice on the part of the national legislator. The legislator argued that the criminalisation of misuse of devices requires the strongest form of intent (*oogmerk*) to commit a specifically mentioned target offence, in contrast to the general criminalisation of preparation which only requires "normal" intent (*opzet*), so that the preparation can be considered as worthy of punishment as the target offence.¹⁰⁷ This is not a convincing argument, given that a criminal attempt at hacking still comes closer to committing hacking than possessing a hacking tool with the purpose (*oogmerk*) of committing hacking – but the attempt is punishable with only two-thirds of the punishment for hacking. In this respect, the criminalisation of misuse of devices is dogmatically not in line with the Dutch legal system.

¹⁰⁷ *Kamerstukken I 2005/06*, 26 671, No. D, p. 14.

IV. Conclusion

The Netherlands introduced computer-crime legislation in the early 1990s and has updated its legislation several times since. Most of the major changes were the result of implementing international legal instruments to harmonise cybercrime legislation, first and foremost the Cybercrime Convention. This is an ongoing process; recently, for example, an act was passed to implement the Lanzarote Convention in order to criminalise grooming and intentional access to child pornography. This process of harmonising Dutch law with international requirements has generally taken place smoothly and without discussion, albeit rather slowly, causing delays in updating national law, for example, in the criminalisation of email bombs and DoS attacks. Sometimes, the updating has also occurred in an unsystematic, piecemeal fashion; for example, the element “data with financial value in the regular market” was changed into simply “data” (to additionally cover black-market data like passwords and credit card numbers) for extortion in 2004, but for blackmail and fraud in 2009. Overall, however, Dutch cybercrime legislation is in good shape, particularly after the Computer Crime II Act of 2006, with a wide and comprehensive range of largely up-to-date provisions in substantive and procedural law in place to combat cybercrime.

Only in some – overall minor – respects, can the Dutch legislation be considered unsatisfactory. One issue is the incomplete implementation of international harmonisation instruments. The only instance where the Cybercrime Convention has not been fully implemented in Dutch law is the criminalisation of misuse of devices with the intent of committing data interference; this is an omission that the legislator should redress. The one gap in the implementation of the Additional Protocol on racist and xenophobic acts and the EU Framework Decision on racism and xenophobia, namely the criminalisation of genocide denial or justification, is pending in Parliament in a bill on “negationism”; in most cases, however, genocide denial will already fall within the scope of criminal discrimination.

Another issue is that the legislator has implemented some international provisions in a way that can be criticised. This holds for the abolishment of the security requirement in the criminalisation of hacking (which sends a wrong signal to computer users regarding the need to apply computer security – the rationale for the 1993 legislator to pose the security requirement in the first place) and the criminalisation of the inchoate offence of misuse of devices with the same maximum punishment as that for the target offence, contrary to the Dutch legal system.

A final issue of unsatisfactory legislation concerns incomplete or unsystematic provisions in Dutch law itself, often caused by some oversight by the legislator. A serious error is that the power to order the undoing of security measures (art. 125k DCCP) refers only to a “data or network search” and excludes the regular, physical search or other investigation powers by which the police can acquire protected

computers or encrypted stored data. The provision of criminal liability for ISPs (art. 54a DCC) refers to an order by the public prosecutor to remove illegal content, but a legal basis for such an order is lacking in the Code of Criminal Procedure. The change from “public telecommunications providers” to “communications service providers,” triggered by the Cybercrime Convention’s use of this term, has not been implemented systematically throughout the Code of Criminal Procedure and the Criminal Code, creating confusion as to what the rationale is, if there be one, for using different terms in the various provisions. Altogether, there is room for improvement in Dutch law.

Besides addressing the shortcomings outlined above – some but not all of which the legislator has announced that it intends to address – improvement can also be made by further clarification. Two topical issues are just starting to be addressed by the courts. The most important one regards the issue of whether certain “virtual goods” – notably “goods” from virtual worlds that have a real-world economic value and that are unique rather than multiple – can be considered a “good” in the sense of property crimes like theft or embezzlement. Two lower courts have convicted persons for stealing such virtual “goods,” deviating from the long-standing doctrine that computer data are not “goods.” These decisions have been acclaimed but also criticised in the literature, and it is to be hoped that a fundamental dogmatic discussion and decisions by appeal courts and the Supreme Court will follow soon in order to shed more light on this issue.

The second topic concerns the level of “realism” required for virtual child pornography to be criminal. Dutch law applies a vaguer standard – an image “seeming” to involve a minor – than the term “realistic image” used in the Cybercrime Convention, and the parliamentary documents provide various explanations of this standard, raising questions as to how this element should be interpreted. A lower court has determined that a cartoon movie that is apparently targeted at seducing small children to have sex with adults can be considered virtual child pornography because it is realistic to the average child and part of a subculture stimulating sexual child abuse. It remains to be seen how other – and higher – courts will interpret cartoons or other images that are not overtly realistic. For Dutch courts, comparative legal analysis would be helpful, i.e., surveying the standards of virtual child pornography applied by other countries and the way in which their courts apply the Cybercrime and Lanzarote Conventions’ rationales of combating a subculture of child abuse.

For other topics, comparative legal research would also be welcome. Looking at the overview of Dutch law, I see several topics that merit investigation at an international level, to stimulate further harmonisation as well as to update cybercrime legislation. In the periphery of cybercrime, and thus beyond the Cybercrime Convention’s current scope, an effort at harmonisation may be required for issues that are crucial for cross-border ICT services. I am thinking, in particular, of data-protection offences, which are far from harmonised in practice

by the European Data Protection Directive, and of requirements for the interceptability of telecommunications infrastructures and services, which were the topic of a 1995 Council Resolution¹⁰⁸ that needs to be reconsidered in light of the many developments in ICT of the past decade.

Other topical issues may call for new initiatives at an international level. The Netherlands is surely not the only country struggling with its concept of “good” in light of “virtual property” crime, and some international guidance on how to qualify virtual property could help countries deal with this issue. Three other topics briefly mentioned in my analysis of Dutch law also merit discussion at the international level in the context of harmonising cybercrime legislation. The first is recording visual images of people without their consent or knowledge, something that increasingly happens with miniature cameras, mobile-phone cameras, and webcams. Although it is not classic cybercrime, it is close enough to unlawful interception to be considered a topic for potential inclusion in the international cybercrime catalogue. The second is cyberstalking: systematically harassing someone via electronic means. The online variants of stalking someone from a distance – sms and email – will, in most countries, be considered functional equivalents of stalking through phone and mail. However, the element of creating a profile page with pictures and data of someone else on a social-network site, without that person’s consent, seems to add a notch to the possibilities of stalking someone online. Although this may fall under stalking or some other traditional crime, it could be worthwhile to discuss the added value of a separate criminalisation of cyberstalking to combat this new form of unlawful behaviour. This also applies to the third and final topic, namely identity theft. Beyond the Netherlands, discussions are taking place at international levels regarding whether or not to introduce identity theft as a separate criminal offence. Regardless of the outcome of these discussions, it is worth noting here that they are taking place in diverging sectoral platforms (drugs and crime, consumer policy, fraud prevention).¹⁰⁹ It would be wise to incorporate and concentrate these discussions in the context of harmonising cybercrime, given the close links between identity theft and phishing, computer forgery, and computer fraud.

While there is, as I have indicated, room for improvement and clarification of Dutch cybercrime legislation, and a need for debate on the harmonisation of some upcoming topics at the international level, I would like to stress in conclusion that, overall, cybercrime legislation is in good shape and largely up-to-date to meet the challenges of today’s cybercriminals. Of course, there is a continuing need to update cybercrime legislation, as tomorrow’s cybercriminals are bound to invent new ways and means of committing crimes, and therefore we should stay alert on

¹⁰⁸ Council Resolution 96/C329/01 of 17 January 1995 on the lawful interception of telecommunications, *OJ* 4 November 1996.

¹⁰⁹ Van der Meulen and Koops (forthcoming), p. 9.

updating and further harmonising cybercrime legislation where possible. But, at the end of the day, legislation is hardly the issue in the fight against cybercrime. Good legislative frameworks are in place. Now it comes down to using them and to actually investigating, prosecuting, and convicting cybercriminals. From the mere handful of cases about hardcore cybercrimes that have appeared on the official Dutch case-law website, www.rechtspraak.nl, in the past decade, one can only conclude that there is yet a world to win in making cybercrime legislation actually work in practice.

Literature

- Boek, J.L.M., 'Hacken als opsporingsmethode onder the Wet BOB', *Nederlands Juristenblad* 589-593 (2000).
- Commissie computercriminaliteit, *Informatietechniek & strafrecht: rapport van de Commissie Computercriminaliteit*, Staatsuitgeverij/Ministerie van Justitie, Den Haag 1987.
- De Roos, T., G.A.I. Schuijt and L.W. Wissink, *Smaad, laster, discriminatie en porno op het Internet*, Samsom, Alphen a/d Rijn 1996.
- De Vries, U.R.M.T., H. Tigchelaar, M. Van der Linden and A.M. Hol, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, WODC, Utrecht 2007.
- Groenhuijsen, M.S. and F.P.E. Wiemans, *Van electriciteit naar computercriminaliteit*, Gouda Quint, Arnhem 1989.
- Hoekman, J. and C. Dirkzwager, 'Virtuele diefstal: hoe gegevens toch weer goederen werden', *Computerrecht* 158-161 (2009).
- Kaspersen, H.W.K., *Strafbaarstelling van computermisbruik*, Antwerpen: Kluwer Rechtswetenschappen 1990.
- Kaspersen, H.W.K., 'De Wet Computercriminaliteit is er, nu de boeven nog', *Computerrecht* 134-145 (1993).
- Koops, B.J. *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Kluwer, Deventer 2000.
- Koops, B.J., R. Bekkers, F. Bongers and M. Fijnvandraat, *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, TILT, Tilburg 2005, <http://arno.uvt.nl/show.cgi?fid=46971>.
- Koops, B.J. and P. Wiemans, 'De phish wordt duur betaald', 80 *Nederlands Juristenblad* 741 (2005).
- Koops, B.J. (ed.), *Strafrecht en ICT*, Monografieën Recht en Informatietechnologie, Sdu, Den Haag 2007.
- Lodder, A.R. and A. Oskamp, *Caught in the Cyber Crime Act (Liber Kaspersen)*, Kluwer, Deventer 2009.
- Moszkowicz, Y., 'Een kritische noot bij de 'RuneScape'- en 'Habbohotel'-uitspraken: een illusie is geen goed', 7 *Strafblad* 495-503 (2009).
- Nouwt, J., 'Tijd voor een nieuw punitief sluitstuk in de WBP?' *Privacy & Informatie* 253-257 (2005).
- Schellekens, M.H.M., *Strafbare feiten op de elektronische snelweg*, Kluwer, Deventer 1999.
- Schellekens, M.H.M., B.J. Koops and W. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, TILT/Cycris, Tilburg 2007.

- Siemerink, L., *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het Internet*, Kluwer, Deventer 2000.
- Sietsma, R., *Gegevensverwerking in het kader van de opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy*, Sdu Uitgevers, Den Haag 2006.
- Stevens, L. and B.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', 39 *Delikt & Delinkwent* 669-696 (2009).
- Stol, W.P., H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt and A.R. Lodder, *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland*, WODC, Den Haag 2008.
- Van der Meulen, N. and B.J. Koops, 'The Challenge of Identity Theft in Multi-level Governance. Towards a co-ordinated action plan for protecting and empowering victims', in: J. Van Dijk and R. Letschert (eds), *Globalisation, Victims and Empowerment*, Springer, <http://ssrn.com/abstract=1447324> (forthcoming).
- Van Dijk, C.H. and J.M.J. Keltjens, *Computercriminaliteit*, W.E.J. Tjeenk Willink, Zwolle 1995.
- Wiemans, F.P.E., *Computercriminaliteit. Commentaren op het wetsvoorstel computercriminaliteit*, Cipher Management, Maastricht 1991.
- Wiemans, F.P.E., *Onderzoek van gegevens in geautomatiseerde werken*, Wolf Legal Publishers, Nijmegen 2004.