EJCL

NEDERLANDSE VERENIGING VOOR RECHTSVERGELIJKING
NETHERLANDS COMPARATIVE LAW ASSOCIATION

Cybercrime Legislation in the Netherlands

B.-J. Koops

1. Introduction: Cybercrime and Cybercrime Legislation in the Netherlands

1.1. 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 at the occasion of the Cybercrime Section of the 2010 International Academy of Comparative Law Congress. 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 how Dutch law regulates cybercrime and cyber-investigation, whether any shortcomings exist in the legislation, and how the legislation relates to the 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 elements from Dutch cybercrime legislation that are as yet unaddressed by the international cybercrime harmonization effort.

1.2. 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 (*opportuniteitsbeginsel*). 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 without authorisation a single bit in a computer already constitutes damage to data (Article 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 (Article 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, the parliamentary history is a leading source, followed by case law[3] (particularly from the Dutch Supreme Court) and by doctrinal literature.

1.3. 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 1993[5] 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, after its chairman Hans Franken, the *Commissie-Franken*.

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 yet requires acceptance, after elections, in second reading by a two-thirds majority of Parliament.
The *Kamerstukken* are Parliamentary Documents. 'II' refers to the Second Chamber, 'I' to the First Chamber. All documents later than 1 January 1995 can be found at, <https://zoek.officielebekendmakingen.nl/>, by searching on the series number, in this case 28331. Documents from before 1995 can be found at <http://www.statengeneraaldigitaal.nl/>.

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 & 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.

The committee made a thorough analysis of both the Criminal Code and the Code of Criminal Procedure, and presented an extensive report and recommendations in 1987.[7] This led to the Computer Crime Bill that was submitted to Parliament on 16 May 1990. The Bill largely followed the committee's recommendations, except for the search and seizure provisions.[8] Various amendments and a heated debate in Parliament led to the definitive version of the Computer Crime Act that came into effect on 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 person has possession of money in a bank account or electricity at the same time. Data, on the other hand, are multiple: when you 'take away' data from someone, you usually copy them and the original owner may still have access to them. Likewise, goods are the subject of property law, but data are the subject of intellectual property law. Therefore, the Dutch legislator decided that computer data were not to be considered as a 'good', so 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 it determined that data indeed are not a 'good'.[10]

In July 1999, a new bill was introduced in Parliament, the Computer Crime II Bill.[11] This 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 for the Netherlands on 1 March 2007.

In terms of other relevant international cybercrime instruments, the Netherlands, being member of the European Union, has implemented the 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

7 Commissie computercriminaliteit 1987.

8 See *infra*, section 2.2.1.

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

10 Hoge Raad (Supreme Court) 3 December 1996, *NJ* 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.

Convention on racist and xenophobic acts (CETS 189); it is 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 signed but not yet ratified the Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201); a Bill is pending to implement this Convention.[16]

2. Analysis of National Cybercrime Legislation

2.1. Substantive Criminal Law

The Computer Crime Act inserted two definitions in the Criminal Code. First, data are defined in Article 80quinquies[17] 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 Article 80sexies DCC as 'a construction (*inrichting*) designed to store, process, and transfer[19] data by electronic means'. An earlier proposed definition was broader, but ultimately the definition was restricted to electronic devices. 'The restriction to 'electronic' was suggested by the wish to exclude merely mechanically functioning information systems from the scope of the definition'.[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.

2.1.1. Offences against the Confidentiality, Integrity, and Availability of Computer Systems

2.1.1.1. Hacking

Hacking is penalized in Article 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 after entry copies data (para. 2),

16 *Kamerstukken II* 2008/09, 31 810, Nos. 1-3.

17 The numbering system in Dutch Codes may seem odd to, for example, common-law countries. The Criminal Code dates from 1886 and has frequently been amended since. To retain some system in the Code, new provisions are 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', 'quarter', 'quinquies' etc. – to the article number after 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 et cetera. 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.

or if she hacks via public telecommunications and uses processing capacity or hacks onwards to a third computer (para. 3).

In 1993, the legislator considered hacking only punishable if someone infringes a security measure or otherwise enters a computer by devious means. As a result, 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, it was debated 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 there was some sort of protection, not merely a sign saying 'do not trespass'. The security requirement was considered relevant as an incentive to induce people and companies to protect their computers, something which in the early 1990s was for many far from self-explanatory.

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 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').

2.1.1.2. Illegal Interception

Illegal interception is criminalised in Article 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 authorisations to the telecom connection, such as employers. Covert monitoring by employers of employees is only an offence if they abuse their power.

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

[22] Originally, the criminalisation was spread across different provisions by the Computer Crime Act, with 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). These were integrated in Art. 139c by the Computer Crime II Act.

2.1.1.3. Data Interference

Data interference is penalised in Article 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 (Article 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 Article 350b DCC, if serious damage is caused, with a maximum penalty of one month's imprisonment.

Worms, computer viruses, and trojans are considered a special case of data interference, being criminalised in Article 350a, para. 3 DCC. The Computer 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 did cover 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]

2.1.1.4. 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 (Article 161sexies DCC). Negligent system interference in similar cases is also criminalised (Article 161septies DCC). Even if no harm is caused, computer sabotage is still punishable when targeted at computers or telecommunication systems for the common good (Articles 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. Article 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 have thus been 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 Article 161sexies DCC to conditional juvenile detention and community service of 80

[23] Hoge Raad (Dutch Supreme Court) 19 January 1999, *NJ* 1999, 25.
[24] *Kamerstukken II* 1998/99, 26 671, No. 3, p. 48.

hours.[25] Another district court, somewhat creatively, interpreted 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]

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

2.1.1.5. Misuse of Devices

Misuse of devices has been penalised through the Computer Crime II Act in Article 139d, paras. 2-3 and 161sexies, para. 2 DCC. Article 139d, para. 2 threatens with punishment of up to one year's imprisonment the misuse of devices or access codes with intent to commit a crime mentioned in Articles 138a (hacking), 138b (e-bombing or DoS attacks), or 139c (illegal interception). In para. 3, the punishment is raised to a maximum of four years if the intent is to commit aggravated hacking (as in Article 138a, para. 2 or 3, see above). Misuse of devices or access codes with intent to commit computer sabotage (as in Article 161sexies, para. 1) is covered by Article 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 for accessing 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 Article 350a DCC is not included in the new provisions on misuse of devices. The legislator argued that the criminalisation of spreading viruses, Article 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 Article 350a, para. 3 DCC, but it certainly falls within the scope of Article 6 CCC as part of the black market of cybercrime tools that Article 6 is supposed to combat.[30] This constitutes one of the rare instances where the Netherlands has insufficiently implemented the Cybercrime Convention.

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.
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 of misuse of devices to implement Article 6 CCC, three provisions already existed that criminalised specific types of misuse of devices:

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

2.1.2. Computer-related Traditional Offences

2.1.2.1. Computer Fraud

Computer-related fraud falls within the scope of the traditional provision on fraud or obtaining property or services through false pretences (*oplichting*), Article 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 regular market (*geldswaarde in het handelsverkeer*), such as computer programs or address databases. However, the falsely obtaining of pin codes or credit card numbers was not covered by this provision, as these data are not tradable on the regular 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 law, which replaced 'data with economic value in the regular market' with simply 'data'.[34]

Other fraud-related offences that also cover computer-related crime are extortion (Article 317 DCC) and blackmail (Article 318 DCC). The provision on extortion used a similar clause as fraud, but here, the clause 'data with economic value in the regular market' was already 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]

31 The term 'data' was included in this provision by Act of 21 April 2004 (*Staatsblad* 2004, 180) to cover, for example, computer programs designated for forging traveller's cheques or shares, implementing the European Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment, *OJ* 2 June 2001, L149/1.

32 Hoge Raad (Supreme Court) 19 November 1991, *NJ* 1992, 124.

33 Koops & Wiemans 2005.

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

35 *Staatsblad* 2004, 180.

36 *Staatsblad* 2009, 245.

A special case of fraud is telecommunications fraud, which is specifically penalised in Article 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.

2.1.2.2. Computer Forgery

Computer-related forgery falls within the scope of the traditional provision on forgery (Article 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 Article 225 DCC: it should be fit 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 was stored with sufficient durability. Since this case, computer forgery can regularly be prosecuted on the basis of Article 225 DCC.

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

2.1.2.3. Data Theft

Although theft – taking away property – does not cover appropriation of data (see *supra*, Introduction), the Dutch 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 (almost[39]) 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.

37 Hoge Raad (Supreme Court) 15 January 1991, *NJ* 1991, 668.

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 the European Framework Decision 2001/413/JHA.

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

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 to 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 in on their accounts with passwords acquired through a phishing website. The juvenile court convicted the offenders for hacking as well as for aggravated theft (Article 311 DCC).[41]

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 in what kinds of circumstances, other courts will follow this line.

2.1.2.4. 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 these 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 at 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.

2.1.2.5. 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 Article 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'.

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.

42 Hoekman & 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 take place at the EU level, see, e.g., Commission Communication, *Towards a general policy on the fight against cyber crime*, COM(2007) 267 final, p. 8.

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. Of course, a key issue is whether it can be proven that the meeting has the purpose of having sex or making (child-porn) images, which will require considerable circumstantial evidence.

In Dutch law, grooming is not yet a crime. To implement the Lanzarote Convention, a new provision, Article 248e DCC, has been proposed.[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 proposed maximum penalty is two years' imprisonment.

2.1.3. Illegal Content

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

2.1.3.1. Child Pornography

In Dutch law, child pornography is penalised in Article 240b DCC, carrying a maximum penalty of four years' imprisonment. This includes the manufacture, distribution, publicly offering, and possession of pictures that show a minor in a sexual act. Doing this on a professional or habitual basis raises the maximum penalty to eight years' imprisonment.[45] To conform with the Cybercrime Convention's preferred standard, the age limit for child pornography was raised in 2002 from 16 to 18 years.[46]

Although prosecutorial priority is given to child-porn manufacture and commercial distribution, many prosecuted cases involve intentional possession of child pornography by individual users. Particularly relevant 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 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

44 *Kamerstukken II* 2008/09, 31 810, Nos. 1-3.

45 This penalty was raised by the omnibus antiterrorism 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 2.1.5), 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 trespass into 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.

child pornography, for example, by searching for or frequently looking at child porn on the Internet.[47]

Currently, watching child pornography without actually possessing it is not criminalised. This is going to change if the Bill to implement the Lanzarote Convention is passed, which will extend Article 240b DCC with '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 accessing a restricted-access website.[48]

In 2002, to implement the Cybercrime Convention, virtual child pornography was included as a punishable offence in Article 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 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'[49] – via 'the image should *at first sight* be indistinguishable from real'[50] 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'.[51]

To date, only one case has been published of criminal virtual child pornography; 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 fitted the rationale of combating a subculture that promotes child abuse.[52] 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 stress put in this decision on the rationale of combating a subculture of child abuse. To date, this is the only conviction for virtual child pornography in the Netherlands, and it remains to be seen whether in future cases courts will adopt this court's using the perspective of a minor to interpret the term 'realistic'.

2.1.3.2. Racism

A Bill is pending for ratification of the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts (CETS 189).[53] The acts covered by the Protocol, however, are already criminal under existing legislation, since the provisions on racism do not refer to media and hence are applicable as well in an online context.[54] These provisions are thus

47 Stevens & Koops 2009, based on a survey of over fifty Dutch cases of hard-disk possession of child pornography.
48 *Kamerstukken II* 2008/09, 31 810, No. 3, p. 4.
49 *Kamerstukken II* 2001/02, 27 745, No. 6, p. 16.
50 *Kamerstukken II* 2001/02, 27 745, No. 6, p. 14 (emphasis added).
51 Aanwijzing kinderpornografie (Art. 240b WvSr) (Guideline child pornography (Art. 240b DCCP), *Staatscourant* (Official Gazette) 2007, No. 162, p. 8.
52 Rechtbank (District Court) 's-Hertogenbosch 4 February 2008, *LJN* BC3225.
53 *Kamerstukken II* 2008/09, 31 838, Nos. 1-4.
54 For a general overview, see De Roos, Schuijt & Wissink 1996.

regularly applied to Internet publications.[55] Article 137c DCC penalises insult of communities, i.e., utterances in public – orally, in writing or with images – that are intentionally insulting to groups of the population on the basis of their race, religion, philosophy of life, sexual orientation, or handicap. Article 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 by profession or custom or in alliance with others, two years. Article 137e DCC criminalises the publication of discriminatory statements as well as dissemination or stocking for dissemination purposes of carriers with discriminatory utterances, if done otherwise than for the purposes of professional reporting. This offence is punishable with a maximum of six months' imprisonment, or, if done by profession of custom or in alliance with others, one year imprisonment. Finally, participating in or supporting discriminatory activities is punishable on the basis of Article 137f DCC with maximally three months' imprisonment, and discriminating people in the performance of a profession or business is punishable with six months' imprisonment (Article 137g DCC).

The only provision from the Protocol that is not as such criminalised yet in the Netherlands, is article 6, concerning denial, gross minimisation, approval or justification of genocide or crimes against humanity. This offence is also included in Article 1 para. 1 sub (c) and (d) of the EU Framework Decision on racism and xenophobia.[56] Often, genocide denial will nevertheless be punishable on the basis of Articles 137c, 137d, or 137e DCC, since these statements will generally be insultory or discriminatory for the groups subjected to the genocide or crimes against humanity.[57] To make genocide denial more visibly punishable, a Bill was proposed to criminalise 'negationism' in a new provision, Article 137da DCC, which would fully cover the acts mentioned in Article 6 of the Protocol.[58] This Bill has largely lain dormant after its submission in June 2006, and despite a reintroduction in July 2009, still awaits discussion in Parliament.

2.1.4. 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 criminal provisions. Article 31 of the Copyright Act criminalises intentional infringement of someone else's copyright, 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 imprisonment (Article 31a Copyright Act), which rises to four years' imprisonment if done as a profession or business (Article 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 maker (Article 34).

For cybercrime purposes, the aforementioned Article 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

55 See, for example, Gerechtshof (Appeal Court) Amsterdam 17 November 2006, *LJN* AZ3011, convicting someone for publishing discriminatory statements about Jews and homosexuals on a website.

56 Framework Decision 2008/913/JHA of 28 November 2008, *OJ* L328/55 of 6 December 2008.

57 See, for example, Rechtbank (District Court) 's-Hertogenbosch 21 December 2004, *LJN* AR7891, finding someone guilty of discrimination (Art. 137c DCC) for publishing on the Internet a website in Dutch with a text titled 'The Holocaust that never was'.

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

(1991). In contrast to the misuse of devices of Article 6 Cybercrime Convention, Article 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 Article 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: Article 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)).

2.1.5. Privacy (or 'Data Protection') Offences

2.1.5.1. Privacy Offences

Several offences in the Criminal Code concern violations of spatial or relational privacy, such as trespass (Article 138 DCC), but these generally do not relate to computer crime, with the exception of unlawful communications interception.[59] Relevant for cybercrime, however, is the criminalisation of stalking in Article 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, not to do, or to tolerate something or of intimidating her; it carries a maximum penalty of three years' imprisonment. Few court cases have been published concerning cyberstalking as such; most stalking cases in practice 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.[60] A lower court considered that posting threatening messages on a fan website of a famous person could not be considered stalking, since the time of posting – two days – was too brief for the behaviour to be considered systematic.[61] Sending loads of email, sms, and Hyves[62] messages during months or years, however, is a clear case of stalking.[63] Various courts have also punished the placing of announcements on dating websites purporting to be from another person, thus causing this person to receive email responses, as stalking.[64] 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.[65]

Somewhat related to cybercrime are the offences of secretly making visual images of people. If someone uses a camera, the presence of which has not been explicitly been made known, to intentionally and unlawfully make pictures of someone, he can be punished with up to six months' imprisonment if it concerns non-public places (Article 139f DCC) or up to two months' imprisonment if it happens in public spaces (Article 441b DCC).

59 See *supra*, section 2.1.1.2.
60 Hoge Raad (Supreme Court) 9 December 2003, *LJN* AL8452.
61 Rechtbank (District Court) Rotterdam 28 April 2009, *LJN* BI2713.
62 Hyves is the most popular social-network site in the Netherlands.
63 Rechtbank (District Court) Breda 30 October 2009, *LJN* BK1696.
64 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.
65 Rechtbank (District Court) Groningen 1 November 2007, *LJN* BB6924.

2.1.5.2. Data Protection Offences

Behaviour that violates informational privacy – or data protection – could in some cases be prosecuted on the basis of data interference (Article 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 Article 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, and
- 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.[66]

2.1.6. 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.[67] The major portion concerns civil liability, as regulated in Article 6:196c of the Civil Code (*Burgerlijk Wetboek*). 'Mere conduit' providers are not liable; caching providers are not liable if they do not change information and if they operate according to generally recognized procedures; and providers of information services are not liable if they have no knowledge of unlawful content and if they remove or make inaccessible the information as soon as they do gain knowledge.

One specific exemption from liability for ISPs has been inserted in the criminal law. Article 54a DCC determines that intermediaries who offer a telecommunications service consisting of transport or storage of data shall not be prosecuted as such[68] if they do all that can reasonably be asked of them to ensure that the data are made inaccessible, in response to an order from the public prosecutor. The prosecutor requires a warrant from the investigating judge for such an order, so that there is an independent check by the courts on whether the information at issue really is illegal or unlawful.

66 Nouwt 2005.

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

68 'As such' means that they will not be prosecuted as a liable intermediary; they may, however, be prosecuted as a content provider if they have made or selected or otherwise contributed to the content themselves. Cf. Gerechtshof (Appeal Court) Leeuwarden 20 April 2009, *LJN* BI1645.

2.2. *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 to incorporate the same definitions in the DCCP as well.[69]

2.2.1. Coercive Investigatory 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. An often-used threshold for allowing investigation powers is that the crime allows pre-trial detention, which generally is the case for crimes carrying a maximum of at least four years' imprisonment (Article 67, para. 1 under a DCCP), but which is also possible for certain specifically mentioned offences (Article 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 in Article 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 whole gamut of investigation powers can be used, including search and seizure. The 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*),[70] which inserted a complex set of provisions in the DCCP after Article 126f DCCP. This set has subsequently been extended several times, and now comprises investigation powers focused on criminal investigation of a concrete crime based on probable cause in Articles 126g through Article 126ni, by and large the same provisions focused on investigating committed or planned organised crime in Articles 126o through 126z, 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 topped off with 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.

2.2.1.1. *Production and Preservation Orders*

The Computer Crime Act created a data production order in Article 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 rather restricted and appeared insufficient, and therefore, a much broader set of provisions entered into force in January

69 Wiemans 2004, p. 240.
70 *Staatsblad* 1999, 245.

2006 with the Data Production Orders Act (*Wet bevoegdheden vorderen gegevens*).[71] These provisions allow the ordering of:

- *identifying data* by any investigating officer in case of a crime (but not a misdemeanour), according to Article 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 Article 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, Article 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 Article 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 people who process the data in a professional capacity; an order of 'other' stored data and of sensitive data, however, can also be directed at people who process data for personal use. Suspects can not, however, be ordered to provide data, in view of the privilege against self-incrimination. If the data are encrypted, the people targeted by the production order – excluding suspects – can be ordered to decrypt them, according to Article 126nh DCCP.

The Computer Crime II Act introduced a power to order the preservation of data, as required by the Cybercrime Convention. Article 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 (once extendible) period of at most 90 days. 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).

2.2.1.2. 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 includes the power to break, where necessary, security measures; a computer, in that respect, is no different from a closet or safe. The general seizure provisions (Articles 95, 96, 96a, and 104 DCCP) can be used to seize data-storage devices. Data as such can not be seized, since they are not considered 'goods',[72]

[71] *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.

[72] See *supra*, section 1.

but they may be copied by law-enforcement officers during a search – comparable to the copying of, for instance, 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 was theoretically impossible. (In practice, though, a search to seize storage devices sufficed.) The Data Production Orders Act therefore introduced in Article 125i DCCP (replacing the old Article 125i DCCP, *supra*, section 2.2.1.1) 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*), Article 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 the restoration, if the making inaccessible was unjustified – must be ordered by a judge in court, Article 354 DCCP.

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. Article 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 regularly stay in those premises.[73] Under the current interpretation, the network search can not go beyond the Dutch borders. No information or experience is available yet about how the Netherlands will interpret the Cybercrime Convention's exception of extraterritorial network search with lawful consent from a lawful authority (Article 32 CCC).

A further ancillary power to the search and seizure procedures was introduced by the Computer Crime Act. This enables the investigating officer to order the undoing of a security measure (Article 125k, para. 1 DCCP) and to order the decryption, or handing over of a decryption key, of encrypted data (Article 125k, para. 2 DCCP). The orders may not be given to suspects, in view of the privilege against self-incrimination (Article 125k, para. 3 DCCP).[74] These orders could initially be given *while* the officer conducted a search or network search, which was felt to be too restrictive, since often computers are 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 has apparently overlooked the fact that Article 125i only concerns a search to secure data, not a regular search on the basis of Articles 96b, 96c, 97, or 110, and in practice, a search will most often be conducted based on one of these other articles. This implies that security-undoing or decryption orders can not 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 Article 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 her laptop or pda is seized;

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

[74] 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 was 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.

this gap already existed under the old Computer Crime Act legislation,[75] but has so far not been addressed by the legislator.

As general safeguards in the procedures for investigating computers and data, obligations exist to delete retrieved data as soon as they are no longer relevant for the investigation, except if they have to be used for a different case or registered in a serious crime register (Article 125n DCCP), and to inform the persons involved when data have been copied or made inaccessible. The persons to be notified are suspects (unless she automatically is 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 (Article 125m DCCP).

2.2.1.3. User and Traffic Data

When the general and comprehensive regime for production orders (*supra*, under 2.2.1.1) was prepared in the mid-2000s, a separate regime was established for telecommunications data, based on the argument that this sector had an long-standing, well-functioning, and in some respects singular practice of providing data to law enforcement, in particular to provide real-time access to future traffic data.

The provision specifically targeted at obtaining user data is Article 126na DCCP. This allows any investigating officer, in case of a crime, to order a communications service provider[76] to produce user data: name, address, number, and type of service. Article 126n, concerning traffic data (*infra*), also comprises the collection of user data.

If the provider does not have these user data available – which will often be the case with pre-paid cards – she may be ordered, on the basis of Article 126na, para. 2 DCCP, to retrieve the phone number of a pre-paid card user by comparing registries; the police then provide her with two or more dates, times, and places from which the sought person is known to have called. To make sure that providers have these data available, a three-month data retention obligation was established (*infra*, under 2.2.3). As an alternative, the police can also, if comparing registries by the telecommunications provider is impossible or too inefficient, use an IMSI catcher, that is, a device that resembles a mobile phone base station and that attracts the traffic of mobile phones in its vicinity. This power is regulated by Article 126nb DCCP, complemented by Article 3.10, para. 4 Telecommunications Act (*Telecommunicatiewet*) to sanction the disturbing of the radio frequency spectrum. An IMSI catcher may only be used to collect someone's unknown telephone number (or IMSI number), but not to collect traffic data or to listen in on communications.

The power to order the production of communications traffic data is regulated by Article 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 communications service providers. This can apply to stored data, but also to incoming future data for a period of up to three months, which have to be provided real-time. Traffic data are listed in an Order in Council as comprising names and numbers of sender (and of the one who pays for her subscription) and recipient,[77] data, time, duration, cell location in the mobile network,[78] numbers of peripheral equipment, and types of services used.[79]

75 Koops 2000, p. 19.

76 See *infra*, note 82 and surrounding text.

77 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, p. 7-8.

2.2.1.4. Interception of Content Data

Interception of communications content is an important investigation power in the Netherlands, which has a very high number of yearly law-enforcement interceptions.[80] Article 126m DCCP enables the public prosecutor, with authorisation from the investigating judge, to order recording of communications that are made by means of a communications service provider's service. Interception is allowed 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 Article 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 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 non-disclosure (lawyers, public notaries, clergy, medical practitioners), however, cannot be intercepted, unless they are themselves a suspect; if in a regular wiretap a conversation with such a person on duty is recorded, it should be deleted (Article 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 is now proposed in which designated phone and fax numbers of attorneys are automatically recognised and excluded from interception.[81]

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 all communications service providers. A communications service provider is defined in Article 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 Article 1 under c of the Cybercrime Convention.[82]

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

78 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.

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

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

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

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

Since 1 July 2004, some forms of cross-border interception are allowed,[83] following the EU Mutual Assistance between Member-States Treaty.[84] Article 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*). Article 13.1 requires providers of public telecommunications networks or services to ensure that their network or service enables interception. This includes Internet providers. The obligation is detailed in an Order in Council and a Decree.[85] The costs for making and keeping their networks or services interceptable are borne by the telecommunications providers themselves; operational costs for concrete intercepts are borne by the state (Article 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.[86]

2.2.1.5. Other

Another major computer-related investigation power is direct interception. Article 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 so it 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 place 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 to authorise it explicitly.

Other than breaking into a premise to place a technical interception device such as a keystroke logger, and the power to conduct an online network search while doing a regular search the police has no power to remotely search or hack into computers.[87]

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

- *undercover operations*: Article 126j DCCP allows law-enforcement officers to systematically gather information undercover. This includes participating in Internet forums, chat groups, etc.;

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

84 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 29 May 2000, *OJ* C197/1 of 12 July 2000.

85 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 several times subsequently.

86 See Koops *et al.* 2005 and *Kamerstukken II* 2005/06, 30 517, Nos. 1 et seq.

87 Koops 2007, p. 118-119; contra: Boek 2000.

- *infiltration and pseudo-purchase*: infiltration (Article 126h DCCP) and pseudo-purchase (Article 126i DCCP) allow investigating officers to infiltrate criminal organisations, on the public prosecutor's order.[88] This includes infiltration in computer child-porn networks, chat groups, etc., and the officers can pretend they want to buy or pay for access to online child pornography (Article 126i was extended by the Computer Crime II Act to include pseudo-purchase of computer data);
- *observation by technical means*: Article 126g DCCP allow the public prosecutor to order systematic observation. A technical device may be used for the observation, as long as this does not record confidential communication (for that, the power of direct eavesdropping, *supra*, should be used). This includes location-tracking devices, but these may not be attached to persons, only to objects;
- *preliminary investigation* (*verkennend onderzoek*): Article 126gg DCCP allows law-enforcement officers to collect information about potential crime in certain sectors of society; data mining may be a primary tool for this.[89] 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 these with other databases for data mining, in contravention to the limitations of the Police Registries Act (Article 126hh DCCP).[90]

2.2.2. 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 (Article 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*) (Article 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 (Article 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 (Article 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 (Article 153 DCCP).[91]

The 'other writings' of Article 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.

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

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

90 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.

91 *Staatsblad* 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, which is expected to be introduced somewhere in 2010.

2.2.3. 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 Article 13.4, para. 2 of the Telecommunications Act (*Telecommunicatiewet*) and the underlying Order in Council,[92] providers of mobile telecommunications are required to store the dates and times, location, and phone numbers of pre-paid card callers, for a period of three months. This obligation was created in order to enable the retrieval of identifying data of pre-paid card users (*supra*, 2.2.1.3).

To implement the European Data Retention Directive,[93] a comprehensive data retention regime for traffic data has been established. The government initially proposed a retention period of 18 months,[94] 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.[95] The Telecommunications Data Retention Act (*Wet bewaarplicht telecommunicatiegegevens*) entered into force on 1 September 2009;[96] the promised amending bill is 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.

2.3. Jurisdiction

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

Article 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 (Article 5, para. 1 under 1 *juncto* 273 DCC), and child pornography (Article 5, para. 1 under 3 *juncto* 240b DCC). Jurisdiction also exists for child pornography committed by foreigners with a fixed residence in the Netherlands, even when they come to reside in the Netherlands after the crime was committed (Article 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 Article 5, para. 1 under 4 DCC. Also, 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 will soon also be subject to Dutch jurisdiction when committed by Dutch citizens abroad.[97]

92 Decree on Special Collection of Telecommunications Number Data (*Besluit bijzondere vergaring nummergegevens telecommunicatie*), *Staatsblad* 2002, 31.
93 Directive 2006/24/EC, *OJ* L105/54 of 13 April 2006.
94 *Kamerstukken II* 2006/07, 31 145, No. 2.
95 *Handelingen I* (Parliamentary Proceedings First Chamber) 7 July 2009, 40-1858.
96 *Staatsblad* 2009, 333.
97 *Staatsblad* 2009, 525, not yet entered into force.

2.4. *Self-regulation and Co-regulation in Relation to Illegal Content*

2.4.1. Notice and Take-down

The provision on ISP liability in the Criminal Code, Article 54a DCC (*supra*, section 2.1.6) 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 Article 54a DCC cannot be considered a legal basis for an NTD procedure.[98] 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 a formal notification by a public prosecutor, in line with Article 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 will remove 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, with unlawful content under civil law, bring her dispute before the courts. In the latter case, if the content provider is unwilling to make 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 concerned.[99]

2.4.2. 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.[100] 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.[101] 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

98 Schellekens, Koops & Teepe 2007.

99 See Art. 6 Code of Conduct, available at <http://www.samentegencybercrime.nl/NTD/Download_the_code_of_conduct?p=content>.

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

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

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 she thinks the website was unjustly blocked.

The co-regulatory effort has recently been stepped up in a new Platform Internet Safety (*Platform Internetveiligheid*).[102] The child-porn hotline, Meldpunt Kinderporno op Internet, a private party, will henceforth be responsible for the blacklist, the first of which is expected to appear in early 2010.[103]

3. 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 made to 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 the 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.[104]

The process of implementing international harmonisation instruments overall occurs quite smoothly, 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 these have to be implemented in national legislation. The provisions of international instruments are rarely challenged in the parliamentary process; where a harmonisation instrument leaves room for the national legislator, for example the retention period from the Data Retention Directive, parties in the Second and First Chambers argue about the implementation, but always within the margins set by the international instrument. Moreover, Parliament seldom forces the government to make reservations when ratifying conventions; significantly, no reservations were made with respect to the Cybercrime Convention, even though the Convention in several provisions allows reservations.

In fact, most international instruments are not often debated as such. They are paid attention to by the (staff of the) Minister 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, in the rest of the parliamentary discussion, the harmonisation background – for

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

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

104 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 & Oskamp 2009).

example, the scope or interpretation of particular terms of the Cybercrime Convention – no longer plays a substantial role.

Whereas the harmonisation effort thus occurs 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 already in April 2000, following a stand-still decision from the European Commission that its provisions on ISP liability diverged from the Electronic Commerce Directive regulation.[105] 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 the 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 these 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 system of Dutch law; 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 abolition of the security requirement for hacking (*supra*, section 2.1.1.1). The Computer Crime Act of 1993 introduced as a threshold for criminal liability that a security measure had been infringed or that access had 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 has triggered the Dutch legislator in 2006 to change the criminalisation of hacking.

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 included private communication providers, the procedural powers were extended in 2006 with powers to intercept private communications, for example, closed company networks. This was a major shift in policy, which, even though it concerned implementation of the Convention's requirements, would

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

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; Article 125la 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 Article 273 DCC, which criminalises the unlawful opening by a provider of communications not addressed to him, speaks of *tele*communications 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 system of Dutch law, inchoate crimes usually carry less punishment than the result crime. The general criminalisation of preparation of crimes, for example, carries half the punishment as the crime under preparation (Article 46 DCC), and criminal attempt carries two-thirds of the maximum punishment (Article 45 DCC). Applying equal punishment to preparation of cybercrimes as the cybercrimes themselves is therefore a significant divergence of the existing system, not necessitated by the international instrument itself but caused, instead, by a conscious choice 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 equally worthy of punishment as the target offence.[106] 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 of hacking. In this respect, the criminalisation of misuse of devices is dogmatically not in line with the system of Dutch law.

4. 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 for harmonising cybercrime legislation, first and foremost the Cybercrime Convention. This is an on-going process; currently, for example a Bill is pending to implement the more recent Lanzarote Convention, criminalising grooming and intentional access to child pornography. This process of harmonising Dutch law with international requirements has generally occurred smoothly and without discussion, albeit rather slowly, causing delay 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 cover also black-market data like passwords and credit-card numbers) for extortion in 2004, but for blackmail and fraud only 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-do-date provisions in substantive and procedural law to combat cybercrime.

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

Only in some – overall minor – respects, can the Dutch legislation be considered unsatisfactory. One issue is incomplete implementation of international harmonisation instruments. The only instance where the Cybercrime Convention has not been fully implemented in Dutch law is criminalising misuse of devices with 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 to criminalise genocide denial or justification, is pending in parliament in a dormant 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 is a wrong signal to computer users on the need to apply computer security – the rationale for the 1993 legislator to pose the security requirement) and for criminalising the inchoate offence of misuse of devices with the same maximum punishment as the target offence, contrary to the system of Dutch law.

A final issue of unsatisfactory legislation concerns incomplete or unsystematic provisions in Dutch law itself, often caused by some oversight of the legislator. A serious error is that the power to order undoing of security measures (Article 125k DCCP) refers only to a 'data or network search' and excludes the regular, physical search, or other investigation powers through which the police can acquire protected computers or encrypted stored data. The provision of criminal liability for ISPs, Article 54a DCC, refers to an order by the public prosecutor to remove illegal content, but a legal basis for such an order in the Code of Criminal Procedure is lacking. 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 what the rationale is, if there be one, for using different terms in the various provisions. Altogether, then, there is room for improvement in Dutch law.

Besides addressing the shortcomings outlined above – some but not all of which the legislator has announced an intention of addressing – 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 whether certain 'virtual goods' – notably 'goods' from virtual worlds that have 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 people 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 a decision by appeal courts and the Supreme Court will follow soon 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 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 it is 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, surveying the standards of virtual child pornography applied

by other countries, and the way in which their courts apply the Cybercrime and Lanzarote Conventions' rationale of combating a subculture of child abuse.

Also for other topics, comparative legal research would 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 updating of cybercrime legislation. In the periphery of cybercrime, and thus beyond the Cybercrime Convention's current scope, some 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 interceptability of telecommunications infrastructures and services, which are the topic of a 1995 Council Resolution[107] 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 will not be the only country struggling with its concept of 'good' in light of 'virtual property' crime, and some international guidance how to qualify virtual property could help countries in dealing with this issue. Three other topics briefly mentioned in my discussion of Dutch law also merit being discussed at the international level in the context of harmonising cybercrime legislation. The first is making 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, and although this may fall under stalking or some other traditional crime, it could be worth while to discuss the added value of a separate criminalisation of cyberstalking to combat this new form of unlawful behaviour. That applies also to the third and final topic, namely identity theft. Like in the Netherlands, discussions are taking place at international levels whether or not to introduce identity theft as a separate criminal offence. Regardless of the outcome of these discussions, it is noteworthy here that they take place in diverging sectoral platforms (drugs and crime, consumer policy, fraud prevention).[108] 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 harmonisation of some upcoming topics at the international level, in conclusion I would like to stress 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 for updating cybercrime legislation, as tomorrow's cybercriminals are bound to invent new ways and means of committing crimes, and so we should stay alert on 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

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

[108] Van der Meulen & Koops 2010 (forthcoming), p. 9.

investigate, prosecute, and convict cybercriminals. Seeing the mere handfuls 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.

References

Boek 2000
Boek, J.L.M., 'Hacken als opsporingsmethode onder the Wet BOB', *Nederlands Juristenblad*, 2000, p. 589-593.

Commissie computercriminaliteit 1987
Commissie computercriminaliteit, *Informatietechniek & strafrecht: rapport van de Commissie Computercriminaliteit*, Den Haag: Staatsuitgeverij/Ministerie van Justitie, 1987.

Dijk van & Keltjens 1995
Van Dijk, C.H. & Keltjens, J.M.J., *Computercriminaliteit*, Zwolle: W.E.J. Tjeenk Willink, 1995.

Groenhuijsen & Wiemans 1989
Groenhuijsen, M.S. & Wiemans, F.P.E., *Van electriciteit naar computer-criminaliteit*, Arnhem: Gouda Quint, 1989.

Hoekman & Dirkzwager 2009
Hoekman, J. & Dirkzwager, C., 'Virtuele diefstal: hoe gegevens toch weer goederen werden', *Computerrecht*, 2009, p. 158-161.

Kaspersen 1990
Kaspersen, H.W.K., *Strafbaarstelling van computermisbruik*, Antwerpen: Kluwer Rechtswetenschappen, 1990.

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

Koops 2000
Koops, B.J., *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer, 2000.

Koops 2007
Koops, B.J. (ed.), *Strafrecht en ICT*, Monografieën Recht en Informatie-technologie, Den Haag: Sdu, 2007.

Koops, Bekkers, Bongers & Fijnvandraat 2005
Koops, B.J., Bekkers, R., Bongers, F. & Fijnvandraat, M., *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, TILT, Tilburg 2005, <http://arno.uvt.nl/show.cgi?fid=46971>.

Koops & Wiemans 2005
Koops, B.J. & Wiemans, P., 'De phish wordt duur betaald', 80 *Nederlands Juristenblad*, 2005, p. 741.

Lodder & Oskamp 2009
Lodder, A.R. & Oskamp, A., *Caught in the Cyber Crime Act (Liber Kaspersen)*, Deventer: Kluwer, 2009.

Meulen van der & Koops 2010
Van der Meulen, N. & Koops, B.J., 'The Challenge of Identity Theft in Multi-level Governance. Towards a co-ordinated action plan for protecting and empowering victims', in: Van Dijk, J. & Letschert, R. (eds.), *Globalisation, Victims and Empowerment*, Berlin: Springer, <http://ssrn.com/abstract= 1447324> 2010 (forthcoming).

Moszkowicz 2009
Moszkowicz, Y., 'Een kritische noot bij de "RuneScape"- en "Habbohotel"-uitspraken: een illusie is geen goed', 7 *Strafblad*, 2009, p. 495-503.

Nouwt 2005
Nouwt, J., 'Tijd voor een nieuw punitief sluitstuk in de WBP?', *Privacy & Informatie*, 2005, p. 253-257.

Roos de, Schuijt & Wissink 1996
De Roos, T., Schuijt, G.A.I. & Wissink, L.W., *Smaad, laster, discriminatie en porno op het Internet*, Alphen a/d Rijn: Samsom, 1996.

Schellekens 1999
Schellekens, M.H.M., *Strafbare feiten op de elektronische snelweg*, Deventer: Kluwer, 1999.

Schellekens, Koops & Teepe 2007
Schellekens, M.H.M., Koops, B.J. & Teepe, W., *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg: TILT/Cycris, 2007.

Siemerink 2000
Siemerink, L., *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het Internet*, Deventer: Kluwer, 2000.

Sietsma 2006
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*, Den Haag: Sdu Uitgevers, 2006.

Stevens & Koops 2009
Stevens, L. & Koops, B.J., 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', 39 *Delikt & Delinkwent*, 2009, p. 669-696.

Stol, Kaspersen, Kerstens, Leukfeldt & Lodder 2008
Stol, W.P., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R., *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland*, Den Haag: WODC, 2008.

Vries de, Tigchelaar, Van der Linden & Hol 2007
De Vries, U.R.M.T., Tigchelaar, H., Van der Linden, M. & Hol, A.M., *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Utrecht: WODC, 2007.

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

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

Cite as: B.-J. Koops, *Cybercrime Legislation in the Netherlands*, vol. 14.3 ELECTRONIC JOURNAL OF COMPARATIVE LAW, (December 2010), <http://www.ejcl.org/143/art143-10.pdf>.