Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

THE NETHERLANDS*

B.F. KEULEN & H.D. WOLSWIJK*

1 Introduction

Criminal law provisions related to cybercrime offences are not contained in a separate code, or a separate title within a code. Several separate bills have introduced provisions related to cybercrime offences into several separate titles of the Dutch Penal Code (DPC). Especially important were the Computer Crime Act of 1993,[1] and the Computer Crime II Act of 2006.[2] The new provisions related to cybercrime offences were inserted next to existing provisions which they more or less resembled. Intentionally and without right destroying a good belonging to someone else, for instance, is a crime according to Art. 350 DPC. The Computer Crime Act introduced a new Art. 350a par. 1 DPC which made intentionally and without right destroying computer data a crime.

This new provision regarding the destroying of computer data was considered necessary because computer data, according to the legislator, were not a 'good'. This opinion of the legislator was influenced by case law of the Dutch Supreme Court which concerned the interpretation of the concept 'good'. That is only one example in which decisions of the Dutch Supreme Court influenced the legislation on cybercrime. At the moment a new Act on Computer Crime is in a preparatory phase.[3] A part of the changes this Act wants to bring is also related to case law of the Dutch Supreme Court and other courts. One can say that criminal law provisions related to cybercrime offences are frequently adapted as a result of a continuous dialogue with case law of the courts.

In this country report, we will focus on provisions regarding specific cybercrime offences in the Netherlands.[4] But before we do that, we will make some remarks about mens rea in the context of cybercrime offences.

---

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

* Prof. dr. B.F. Keulen & Dr. H.D. Wolswijk.

1 Staatsblad (Dutch Bulletin of Acts and Decrees) 1993, 33.

2 Staatsblad 2006, 300.

3 Concept-wetsvoorstel (concept bill) versterking bestrijding computercriminaliteit (www.rijksoverheid.nl). On this concept, see Koops 2010b.

4 See for another recent country report on more or less the same subject Koops 2010a.

2 Mens Rea and Cybercrime

Dutch substantive criminal law makes a distinction between misdemeanors and crimes. With regard to crimes, usually intent is required. Dutch criminal law recognizes several gradations of intent, comprising not only 'wilful intent' (*dolus directus*) and 'awareness of a high degree of probability' (*dolus indirectus*), but also 'conditional intent' (*dolus eventualis*, 'bedingter Vorsatz'), which is considered the 'lower limit' of intent.[5] According to the case law of the Dutch Supreme Court, conditional intent means that the perpetrator is aware of the considerable possibility that a certain result will occur, yet nevertheless accepts that possibility. Art. 350a DPC, for instance, requires that the perpetrator consciously accepts the chance that computer data are destroyed as a result of his actions. A specific intent is usually not required.

The Dutch Penal Code also contains some criminal offences which require negligence. Negligence requires culpa lata, in the Netherlands, i.e. a gross deviation of the conduct that can be expected from the person involved.[6] Doctrinally, a distinction is made between conscious negligence and unconscious negligence. With conscious negligence, the perpetrator is aware of the considerable possibility that a certain result will take place (like conditional intent), but instead of accepting this possibility, wrongfully trusts that the result will not occur (unlike conditional intent).[7] Not every intentional offence has a negligent equivalent. The main reason for introducing negligent offences lies in the seriousness of the legal interest (f.e. death through criminal negligence, Art. 307 DPC). This reasoning has led to criminalizing several negligent cybercrimes.

According to Art. 350b DPC, for instance, negligence resulting in severe damage to computer data constitutes a crime. That is a remarkable provision; there is not an equivalent of this provision with regard to 'goods'. There is only a specific provision according to which negligence resulting in the destruction of railroads, gas pipelines and some other goods that are used in the public interest constitutes a criminal offence (Art. 351bis DPC). Private computer data are, it seems, to some extent placed on equal footing with public works.

Other crimes which require negligence are limited to computers which are used in the public interest. According to Art. 351bis DPC, for instance, negligence resulting in damage to a computer which is used in the public interest can lead to a maximum penalty of one month imprisonment. And according to Art. 161septies DPC, negligence resulting in damage to a computer which causes a disturbance of the operation of the computer constitutes a crime if this leads to an impediment of the storage, processing or transfer of data which are of public interest.

---

[5] De Hullu 2012, p. 226-232.
[6] De Hullu 2012, p. 252.
[7] De Hullu 2012, p. 228.

3 Offences against the Integrity and Functionality of Computer Systems

3.1 Illegal access and interception of transmission

Intentionally and without right entering a computer or a part thereof is a criminal offence according to Art. 138ab DPC. This provision is placed next to articles which concern trespassing (Art. 138 and 138a DPC). It carries the same maximum penalty: one year imprisonment. If the hacker after this entry without right copies data stored in the computer to which he has gained access unlawfully, and records these data for his own use or that of another, the maximum term of imprisonment is four years (Art. 138ab par. 2 DPC). The same maximum penalty applies if the hacker enters the computer by using public telecommunications, and subsequently uses processing capacity of the computer to obtain an unlawful gain for himself, or gains access to the computer of a third person through the computer into which he has intruded (art. 138ab par. 3 DPC).

Breaking a security measure is not an element of this criminal offence. That was different at first. In 1993, the legislator was of the opinion that hacking only constituted a criminal offence if a security measure had been infringed, or the entry had been acquired by using technical means, with the help of false signals or a false key, or by assuming a false capacity. But in 2006 the legislator abolished this requirement, for reasons related to the Cybercrime Convention and the Framework Decision on attacks against information systems. According to the legislator these legal instruments did allow the State Parties to pose the requirement of infringing security measures, but did not allow them to pose other requirements such as using a false identity.[8] Art. 138ab DPC now only mentions some examples of ways to enter a computer, for instance infringing a security measure or using a false key.[9] Koops calls this an odd construction because infringing a security measure does not in itself constitute trespass.[10] We also think it is an odd construction, but for a different reason. Other provisions of the DPC do not contain examples of behavior that constitute a criminal offence. It is not spelled out that murder can take place by poisoning, stabbing or shooting a person. It is a bit strange that the provision which deals with entering a computer without right uses a legal technique which reminds of old times.

To us it seems right not to make breaking a security measure an element of the criminal offence. Hacking is the essence of this criminal offence, not breaking a security measure. The Dutch Supreme Court judgment of 22 February 2011, LJN: BN9287 shows the sort of questions that have to be decided when breaking a security

[8] Kamerstukken II (Parliamentary Documents; II refers to the Second Chamber of Parliament; I refers to the First Chamber) 2004/05, 26 671, no. 7, p. 31-32.
[9] According to case law, using a stolen password is considered using a 'false key'; see Court of Appeal 's-Gravenhage 8 juni 2004, LJN: AP7974.
[10] Koops 2010a, p. 600.

measure is an essential element of the criminal offence. In this case, the victim had used Windows XP. The Court of Appeal considered that every version of Windows XP, bought by a private person, contained some security measures. The Dutch Supreme Court upheld the conviction, adding that breaking a security measure can also exist in against the will of the rightful claimant entering a computer by a way which is not shut off by these security measures. This decision corresponds with the idea that it is not the task of criminal courts to judge the quality of security measures, but to determine the guilt of the accused.

3.2 Data and System Interference

As we saw before, *data* interference is a criminal offence according to Art. 350a DPC. It carries a maximum penalty of two years imprisonment. Art. 350a DPC not only sees to intentionally and without right altering and erasing computer data and making these data unusable or inaccessible; it is also a criminal offence to add data intentionally and without right. The Convention on Cybercrime does not oblige the State Parties to establish adding data as a criminal offence. To us, penalizing adding data seems a good idea: adding data also interferes with the integrity of documents.

In some cases the maximum penalty is higher than two years imprisonment. If the interference is committed after unlawful entering the computer (hacking) through a public telecommunications network and causes severe damage to the data, the maximum penalty is four years imprisonment (Art. 350a par. 2 DPC).[11] The legislator deemed the increased maximum penalty not appropriate in case the perpetrator invaded the information system through an *internal* network. The greater vulnerablity of the administrator of the information in case of a public communications network, plus the fact that the perpetrator may operate secretly (and causing severe damage), justify the increased maximum penalty.[12] And, as we saw before, negligent data interference also constitutes a criminal offence, but only when the interference resulted in severe damage to computer data (Art. 350b DPC).These are exceptional provisions in the DPC, other provisions do not distinguish between damage and severe damage.

A maximum penalty of two years imprisonment also applies if worms and other computer viruses are made available or disseminated (Art. 350a par. 3 DPC). Earlier, only data intended to cause damage 'by replicating' in a computer were mentioned. This provision was used in the case against the boy who had caused a lot of damage, worldwide, by putting on the internet the so called Kournikova-virus.[13] This virus indeed caused

[11] The Dutch Supreme Court has decided that 'serious damage' includes an information system not being available for several hours; see DSC (Dutch Supreme Court, Hoge Raad) 19 January 1999, NJ (Nederlandse Jurisprudentie, the Dutch Law Reports) 1999, 25.
[12] Kamerstukken II 1991/92, 21 551, nr. 27.
[13] DSC 28 September 2004, NJ 2004/642.

damage by replicating itself. But Art. 350a par. 3 DPC seemed to exclude viruses that caused damage in another way. The Computer Crime II Act changed this, and Art. 350a par. 3 DPC now covers all data designated to cause damage in a computer. And the Explanatory Memorandum made clear that trojans and logic bombs are also covered by this provision, although they do not necessarily cause damage in a computer.[14] Art. 350a par. 4 DPC provides for a ground exluding liability: a person who carries out the act specified in par. 3 with the object of limiting the damage resulting from such data is not criminally liable.

Further, there are two provisions relating to computers which are used in the public interest. According to art. 351 DPC, it is a crime to intentionally and unlawfully destroy, damage, render unusable or defective any railroad work, power station, *automated work or telecommunications systems*, works serving as water barriers (etc.) *in sofar as these works and systems are intended for the use of the general public*. This offence of sabotage can lead to a maximum penalty of three years imprisonment. And, as we saw before, negligence resulting in damage to a computer which is used in the public interest can lead to a maximum penalty of one month imprisonment (Art. 351bis DPC).

The most important provision relating to system interference can be found in Art. 138b DPC. Intentionally and without right hindering the access to or use of a computer by offering or sending data to it, is a criminal offence which can be punished with a maximum penalty of one year imprisonment. This provision was introduced in the DPC by the Computer Crime II Act, in 2006, and can be used in case of e-bombs or denial-of-service (DOS) attacks. Earlier, in 1993, the Computer Crime Act had already introduced Art. 161sexies DPC. According to this provision, intentionally destroying, damaging or rendering unusable any automated work can be punished with a maximum penalty of a year imprisonment if it leads to an impediment without right of the storage, processing or transfer of data which are of public interest. The maximum penalty is six years imprisonment if it causes general danger to goods or services. There is also a culpable offence relating to these data, as we saw before (Art. 161septies DPC).

Art. 161sexies DPC has been used in a case in which a person had spread viruses which hindered electronic banking.[15] The indictment accused him of having developed viruses and/or Trojans (for example Wayphisher) and ordering his botnet to download and install these viruses and Trojans on computers, causing general danger to goods or services, because users of these computers could no longer safely use banking services: they were redirected to other internet addresses, data used to log in could be intercepted, and the defendant and his codefendant got at their disposal data relating to banking services of one or more of the users of these

[14] Kamerstukken II 1998/99, 26 671, no. 3, p. 48.
[15] DSC 22 February 2011, LJN: BN9287.

computers. The indictment further accused him of developing viruses (for example Toxbot) and installing them on computers, making these computers crash, causing general danger to goods or services because the keystrokes on these computers were fixed, giving the defendant and his codefendant access to banking data of the users of these computers. The Court of Appeal acquitted the defendant, because it was of the opinion that there was no general danger (*gemeen gevaar*) to goods or services. General danger implies danger to automated works which are used in the public interest, according to the Court of Appeal. In this case, there was no disturbance in the functioning of the automated works of banks and credit card companies, only a disturbance in the functioning of the computers of their clients. But the Dutch Supreme Court quashed this acquittal. It was of the opinion that the legislator with Art. 161sexies DPC wanted to protect the rendering of services in as far as it can be endangered by, amongst other things, intentionally causing a disturbance in the functioning of an automated work. A computer and a network of computers are an automated work, and so are computers linked through internet by harmful software, according to the Supreme Court. And general danger (*gemeen gevaar*) has to be interpreted as danger to the undisturbed supply of services to an indeterminate but considerate number of customers.

Advocate General Knigge had advised the Supreme Court to uphold the acquittal. He referred to arson, where causing general danger to goods is also an element to the offence. He points out that it is not the danger to the object that is set on fire, but the danger to other objects that is relevant where it comes to the general danger requirement. The Supreme Court more or less departs from this line of thinking. Art. 161sexies DPC requires that general danger is caused by a disturbance of the operation of an automated work; according to the Supreme Court a disturbance in the operation of a lot of separate computers which endangers the supply of services can also lead to a conviction based on this provision. The result is appealing: this is a criminal offence which justifies a maximum prison sentence of six years. But the question remains whether this approach is compatible with the concept of general danger.[16] Perhaps this type of cybercrime requires another approach then arson.

Spamming is dealt with in Art. 11.7 Telecommunications Act. Sending electronic messages for commercial or charitable purposes is only allowed if the addressee has given permission or, in case of persons who have been contacted before, they have been given an opportunity to resist the use of their electronic contact data.

[16] See also Oerlemans & Koops 2011, p. 1181.

Spamming is an economic offence that carries a maximum penalty of two years imprisonment (Artt. 2 and 6 Economic Offences Act).[17]

3.3 Data Forgery

Art. 225 DPC provides for a general criminalization of forgery, with a maximum penalty of 6 years: falsely preparing or falsifying a writing that is to serve as evidence of any fact, with the object of using it as genuine and unfalsified or of having it used as such by others. According to case law, a 'writing' requires two things: it should be readable (if necessary with a device) and it should be durable to a certain degree. Under this 'definition', a computer file will be considered a 'writing' in most cases. And therefore, forgery of computer data falls within the scope of this traditional provision of forgery, as was decided by the Dutch Supreme Court in 1991.[18] In this case a civil servant working for the municipality of Rotterdam changed a computer file by inserting fraudulent payment orders, which were actually payed. This computer file (DGeldV) was a temporary file which was emptied every day. The Supreme Court deduced from this that the file consisted of data which could be made readable and which were fixed on a magnetic disc with sufficient permanence. It further stated that this file was intended to be used as proof of certain facts since it was essential for the processing of payment orders, and in this process the correctness of the file was relied on.

A specific criminal provision can be found in Art. 232 DPC: a person who intentionally falsely prepares or falsifies chip cards designed for payments or other automated service provisioning, with the object of obtaining gain for himself or another person, is liable to a maximum term of imprisonment of six years (par. 1). The use, provision, possession, receiving, obtaining, transport, sale or transfer of a forged card carries the same maximum penalty (par. 2). The Dutch Supreme Court decided that a card used to tank gasoline is also a card as mentioned in this Article.[19]

3.4 Misuse of devices

According to Art. 139d par. 2 DPC the manufacturing, selling, acquiring, importing, distributing and otherwise making available of a technical device that is primarily designed for committing hacking (Art. 138ab DPC), e-bombing or a DOS-attack (Art. 138b DPC) or illegal interception (Art. 139c DPC), with the intention to commit such a crime, can be punished with a maximum sentence of one year imprisonment. The same maximum

[17] And (in practice much more important) it is also an administrative offence that can be fined by the Opta, a Government agency which operates at a detached level from the Ministry of Economic Affairs. See e.g. Court of Rotterdam 26 May 2011, LJN: BQ6210: fines of 150.000 and 100.000 euros.

[18] DSC 15 January 1991, NJ 1991/668.

[19] DSC 20 January 2004, NJ 2004/215.

penalty applies to selling, acquiring and distributing a computer password or other code which gives access to an automated work with the intention to commit one of these crimes. The maximum penalty increases to four years if the perpetrator has the intention to record data in the hacked computer, or to use the processing capacity of the hacked computer (Art. 139d par. 3 DPC). Misuse of devices related to computer sabotage (as defined in Art. 161sexies par. 1 DPC) is made a criminal offence in Art. 161sexies par. 2 DPC. It can also consist in the manufacturing (etc.) of technical devices and in selling (etc.) a computer password or access code.

Some other legal provisions can also play a role in case of misuse of devices. Manufacturing, receiving, acquiring, selling, handing over and having available objects and data which the perpetrator knows to be designated for committing forgery in a chip card designed for payments or other automated service provisioning can be punished with a maximum prison sentence of four years (Art. 234 DPC). Art. 32a of the Copyright Act makes the openly offering for distribution, possession with a view to distribution, import, transport and export as well as the having available for the pursuit of profit of devices which are exclusively designed to circumvent software-protection a criminal offence. It carries a maximum penalty of six months imprisonment. A third legal provision, which can be found in Article 326c DPC, has led to some case law of the Dutch Supreme Court.

Art. 326c par. 1 DPC contains a specific provision for illegitimate use of telecommunications services (for example using technical equipment to gain access to telecommunication services accessible to the public such as telephone lines or paid tv). According to this paragraph it is a criminal offence to use a service which by telecommunications is offered to the public by a technical interference or by using false signals, with the intent to avoid paying in full. This criminal offence carries a maximum prison sentence of four years. Relevant with regard to misuse of devices is Art. 326c par. 2 DPC. According to this paragraph the openly offering of an object or data obviously designated to commit the criminal offence described in the first paragraph can be punished with a maximum penalty of two years imprisonment. And the same maximum penalty applies in case of possession with a view to distribution or import of such an object or data, and in case of manufacturing or saving such an object or data for the pursuit of profit. In 2003, the Dutch Supreme Court had to decide a case in which the defendant was accused of possessing objects with which telephone cards could be upgraded, by manipulating the chip on these cards.[20] Afterwards, they would contain the false signal that the card carries credits received with the permission of KPN (a leading telecommunications and ICT service provider in the Netherlands). The Court of Appeal had convicted the defendant, who stated that this decision was wrong

[20] DSC 15 April 2003, NJ 2003/333.

because the elements of Art. 326c DPC are only fulfilled if the object can be used *directly* in order to obtain a service mentioned in the first paragraph of Art. 326c DPC. The Supreme Court rejected this interpretation. The legislator made it clear, according to the Supreme Court, that the provision of Art. 326c par. 2 DPC is considered necessary to effectively protect the economic interest of the supplier of telecommunications services. It aims to counter as much as possible the illegal use, without payment, of diverging forms of these services. Therefore behavior that can lead to such illegal use (by other persons), is also covered by this provision. And in 2005 and 2008, the Dutch Supreme Court had to decide two cases which concerned a computer magazine (*Computeridee*) which was offered to the public containing an article in which the author explained how the reader could receive and decode Canal+ without paying. In both cases the Court of Appeal had acquitted the defendant. In the first case he was acquitted because the legal term 'object' (*voorwerp*) according to the Court of Appeal only related to computer programs and devices (not to an article in a magazine) and that the content of the article were not data (*gegevens*) as required by Art. 326c DPC.[21] The Supreme Court overturned this decision: such a narrow interpretation of data (*gegevens*) was not in line with the intention of the legislator. In the second case the defendant was acquitted because there was no sound available, the program could only be watched on a computer, and the laborious decoding ritual had to be executed every time.[22] The Dutch Supreme Court also overturned this acquittal. Art. 326c DPC protects the economic interests of the person offering the service. Therefore using a service which by telecommunications is offered to the public has to be interpreted in such a way that it includes use of a part of the service with a certain independent meaning.

Koops calls it an omission of the Dutch legislator not to have made misuse of devices with the intent to commit data interference, such as spreading computer viruses, a criminal offence.[23] He rightly points out that this type of misuse of devices is covered by Art. 6 of the Cybercrime Convention. The legislator seemed to be of the opinion that the general provisions relating to the preparation of criminal offences combined with a specific provision in Art. 350a DPC already implemented Art. 6 of the Cybercrime Convention.[24] Since the general provision on preparation of criminal offences is only applicable when the prepared crime carries a maximum prison sentence of at least eight years (Art. 46 DPC), it is however not applicable in the context of data interference. And Art. 350a par. 3 DPC only sees to making available data which are intended to do damage in an automated work, like viruses. Preparation of spreading viruses, such as making or possessing a virus

[21] DSC 29 March 2005, NJ 2007/508.
[22] DSC 8 July 2008, NJ 2008/426.
[23] Koops 2010a, p. 603.
[24] Kamerstukken II 2004/05, 26 671, no. 7, p. 36.

toolkit, is not covered by this provision or any other provision of the Dutch Penal Code, but falls within the scope of Art. 6 of the Cybercrime Convention, as Koops rightly points out.

The obligations which follow from the Cybercrime Convention alone are already a convincing argument for the position Koops takes. But there is a national argument as well. In light of the broad interpretation the Dutch Supreme Court has given to Art. 326c DPC, an interpretation that has in our opinion led to just and convincing results, there is every reason to see where other provisions penalizing misuse of devices, perhaps even a general provision, can be in place.

4 Privacy and Computer Offences

4.1 Violation of Secrecy of Private Data

Eavesdropping, by a technical device, of oral conversation that takes place in a home, an enclosed room or premises, is a criminal offence according to Art. 139a par. 1 DPC, except if the eavesdropping takes place on instruction of one of the participants to the conversation. Recording such oral conversation by someone who does not participate in the conversation and does not act on instruction of one of the participants is also a criminal offence. The maximum penalty is six months imprisonment. The second paragraph of Art. 139a DPC contains a few exceptions to these prohibitions. They are not applicable to the recording (1) of data that are processed or transferred through telecommunication or through an automated work; (2) with the help of a technical device that is present, and not concealed, upon the authority of the occupant of the home, enclosed room or premises, except in cases of clear abuse; (3) to implement the 2002 Act on the Intelligence and Security Services.

Secretly eavesdropping and recording oral conversation that takes place outside a home, enclosed room or premises is (under the same limitations) a criminal offence according to Art. 139b DPC, and carries a maximum penalty of three months imprisonment (the same exceptions apply as for art. 139a DPC).

Intentionally and without right recording data which are processed or transferred by telecommunications or a computer is a criminal offence according to Art. 139c DPC. This provision does not apply to intercepting or recording (1) data received by a radio receiver, unless a special effort was made or a prohibited receiver was used to make such reception possible; (2) by the user of a telephone connection, unless in case of abuse; (3) for the purpose of ensuring that the telecommunications infrastructure used to service the general public is working properly, for the purpose of criminal investigation, or to implement the 2002 Act on the Intelligence and Security Services.

Installing a technical device on a specific place with the intention to overhear or record an oral conversation, telecommunication or other transfer of data by an automated work is a criminal offence according to Art. 139d

par. 1 DPC. It carries a maximum term of imprisonment of one year. And according to Art. 139e DPC it is a criminal offence to possess an object on which, as the perpetrator knows or should know, data have been fixed which have been obtained by without right eavesdropping or recording an oral conversation, telecommunication or other transfer of data by an automated work. It carries a maximum prison sentence of six months. The same maximum penalty applies if these data are shared with a third person, and if the object on which these data have been fixed is made available to a third person.

The new Act on Computer Crime, which is in a preparatory phase, contains a few proposals to change these Articles (see also par. 4.3, on Illegal Processing of Personal and Private Data). Art. 139a par. 1 DPC should, according to this concept, make intentionally and without right eavesdropping and recording an oral conversation which takes place in a home, enclosed room or premises with a technical device a criminal offence. A similar change is proposed for Art. 139b DPC. According to the concept of the Explanatory Memorandum, this wording implies that even a person who secretly records a conversation to which he is a participant commits a criminal offence (par. 1). The recording is not without right if (all) participants to the conversation have agreed to the recording, and in case the recording is necessary to expose abuses (par. 4).

A second proposal concerns Art. 139c and Art. 139e DPC. Art. 139c should, according to the concept, cover intentionally and without right, with a technical device, recording transfer of data by telecommunications or an automated work which is not public, and copying data which are stored in an automated work. According to the proposed Art. 139e DPC it will be a criminal offence to possess data which are not public if they, as the perpetrator knows or should know, have been obtained by without right eavesdropping, recording or copying a conversation, transfer of data or processing of data by telecommunications or an automated work. The concept of the Explanatory Memorandum clarifies that these changes intend to make it a criminal offence to copy data to which the perpetrator has legitimate access because of (for instance) his job as a civil servant, but which he is not allowed to copy. It refers to a case in which nude pictures of a well known female presenter were published on the internet. We consider these proposed changes to be improvements.

4.2 Violation of Professional Confidentiality

As we saw in the introduction, in the Netherlands new provisions related to cybercrime offences were inserted next to existing provisions which they more or less resembled. That is also true for the provisions relating to violations of professional confidentiality. According to Art. 272 DPC it is a criminal offence to violate a secret of which the perpetrator knows or should know that he is by reason of his office, profession, legal obligation or earlier office or profession bound to keep it a secret. This criminal offence carries a maximum penalty of one year imprisonment. Art. 273 DPC makes it a criminal offence to intentionally make public information which the perpetrator is bound to keep secret regarding an enterprise in which he is or has been employed.

Since 1993, Art. 273 par. 1, 2° DPC also contains a provision related to cybercrime. Intentionally making public or using in pursuit of profit data which have been obtained by a criminal offence from an automated work of an enterprise which are related to this enterprise, is a criminal offence if these data were not common knowledge at the time of their publication or use, if this publication or use can result in a disadvantage. Liability is excluded (par. 2) in case the perpetrator has assumed in good faith that disclosure of the data was in the public interest. Furthermore, prosecution will take place only upon complaint by the organization's management (par. 3). In 2006, some other provisions have been added, of which Art. 273d DPC is relevant to cybercrime offences. According to this provision a person employed by a public telecommunications network or a public telecommunications service commits a criminal offence if he intentionally and without right takes cognizance of data which are stored, processed or transferred by such a network or service, and which are not intended for him. This person also commits a criminal offence if he copies or records such data or possesses an object which, as he knows or should know, contains data which have been acquired by without right copying or recording such data. The applicable maximum penalty is one year and six months imprisonment. This maximum penalty also applies if this person intentionally and without right shares the content of these data with a third person, or intentionally and without right makes available to a third person an object from which the content of these data can be extracted. According to the second paragraph, these provisions are also applicable to persons who are employed by a provider of a non-public telecommunications network or a non-public telecommunications service.

4.3 Illegal Processing of Personal and Private Data

The term 'goods' is a key element in several criminal law provisions, in particular property offences: removing goods (theft, Article 310), appropriating goods which the perpetrator lawfully has in his or her possession (embezzlement, Article 321), inducing the victim by deception to surrender goods (deception, Article 326), forcing someone to surrender goods (extortion, Article 317) and handling goods derived from a crime (Article 416). The legislator made a fundamental – and controversial[25] - choice in considering data not as 'goods' under the criminal law.[26] Although a good need not be tangible – already in 1921 the Supreme Court decided that 'electrical energy' is a 'good' that can be the object of theft[27] -, data lack the feature of uniqueness, they are 'multiple': a person who has control over data does not necessarily lose control if another person gains

[25] The question whether data can be considered goods has been much debated in Dutch literature. See, for example: Dijkstra & Keijzer 1986; Commissie Computercriminaliteit 1987; Vellinga-Schootstra 1988; Groenhuijsen & Wiemans 1989; Van Kasperen 1990.
[26] See also the Country Report, Section I, by Stamhuis (Chapter 2).
[27] DSC 23 May 1921, NJ 1921, p. 564.

control of them, for example if data are copied.[28] Considering data as goods would have the consequence that data receive full protection via the abovementioned property offences. According to the legislator, this would amount to an undesired situation, in particular in view of the interest of the 'free flow of information' (Article 10 ECHR).[29] The criminal provisions concerning 'goods' have not been thought through as far as their relationship with the principle of 'free flow of information' is concerned. On this principal ground, the legislator deemed it wrong to criminalize, in general, the unlawful gathering of data. Data as such are not protected by criminal law (apart from damaging data); the way data are appropriated may lead to liability, for example by hacking into a computer or by interception of transmission of data. So, not the data themselves, but the medium through which data are processed (systems and networks) is protected from unlawful abuse.[30]

Since data are not considered goods, data are (in principle) not subjects to property offences. Still, the legislator made some exceptions to this basic rule. We have already seen that Art. 273 par. 1, 2° DPC criminalizes intentionally making public or using in pursuit of profit data which have been obtained by a criminal offence from an automated work of an enterprise which are related to this enterprise, provided these data were not common knowledge at the time of their publication or use, if this publication or use can result in a disadvantage. This is really a specific form of handling goods derived from a crime (Art. 416 DPC) applied to data. But there is a difference.[31] With the offence of handling goods derived from a crime, the perpetrator (the person handling the stolen goods), may not be the perpetrator of the 'first' crime (the crime of which the goods are 'derived'), since this offence is about promoting *other* persons crimes. With the offence of Art. 273 par. 1, 2° DPC, abuse of company secrets, it is irrelevant whether or not the abuser is also the person who initially obtained the secrets illegally.

Other examples concern the adjustment of classic property offences like the ones mentioned above. Art. 317 DPC contains the criminal offence of extortion. Before the Computer Crime Act came into force in 1993, extortion was defined as by use of violence or threat of violence forcing someone to surrender a good that belongs to this or a third person, accepting a debt or annihilating a claim, with the intent to favor oneself or another person without right. The Computer Crime Act added a clause in this provision: extortion also included by use of violence or threat of violence forcing someone to make available data with economic value. A payment card's pincode, however, has no economic value. Forcing someone, by use of violence or threat of

[28] The view that data are not goods was also held by the Supreme Court, after the Computer Crime Act entered into force (DSC 3 December 1996, NJ 1997/ 574). See on this issue also par. 6.
[29] Kamerstukken II 1989/90, 21 551, no. 3, p. 4.
[30] Kamerstukken II 1990/91, 21 551, no. 6, p. 8.
[31] See also the Country Report, Section I, by Stamhuis (Chapter 2).

violence, to mention a pincode, therefore was no extortion according to the Dutch Supreme Court.[32] That lead to a second change of this provision.[33] It now refers to the by use of violence or threat of violence making available of data, in general, and is no longer limited to data with economic value.

Another provision in the Dutch Penal Code is also relevant where it comes to the illegal processing of personal data. Before 1993, Art. 326 DPC made it a criminal offence to impel another person, by accepting a false name or quality, by tricky maneuvers or by a contexture of lies, to surrender a good that belonged to this or another person, rendering a service, accepting a debt or annihilating a claim, with the intent to favor oneself or another person without right. The Computer Crime Act also added a clause to this provision. The act the victim was impelled to do could also consist in making available data with economic value. But here as well, this was changed: phishing often has to do with data which as such have no economic value. Since a few years, this provision refers to the making available of data in general.[34]

Interestingly, the new Act on Computer Crime, which is in a preparatory phase, goes further on the path of criminalizing the unlawful gathering or taking over of data. According to the concept of the Explanatory Memorandum, the legislative proposal intends to protect citizens against the abuse of computer data in more cases. The background for the strengthening of the protecton is that technical developments make it increasingly simple to take confidential information from a computer and put these on the internet, which makes these data accessible to large groups. This causes damage to the privacy of citizens involved and expansion of criminal law protection is therefore deemed necessary. In fact, with this new Act, the legislator departs from the abovementioned principle not to criminalize, in general, the unlawful gathering of data (which would be the case if data were considered goods and received full protection via the property offences). In this respect the new Act entails two relevant provisions which already came up in par. 4.1 (see above), changing the Articles 139c and 139e DPC. Art. 139c should cover intentionally and without right copying data which are stored in an automated work. With this provision, it will become punishable for someone to take non-public data without authorisation from a computer while having legitimate access to said computer. For example, it will be punishable for an employee of a company to deliberately copy personal details of a famous Dutch citizen with the objective of selling these to a third party (taking the information is already punishable under current law for an employee working at a provider of a telecommunications network). In fact, as the concept of the Explanatory Memorandum itself states, this new provision comes down to criminalizing embezzlement of data (cf Art. 321 DPC: appropriating goods which the perpetrator lawfully has in his or her possession). The

[32] DSC 13 June 1995, NJ 1995/635.
[33] Wet van 21 april 2004, Staatsblad 180.
[34] Wet van 12 juni 2009, Staatsblad 245.

other proposed provision concerns Art. 139e DPC: it will be a criminal offence to possess data which are not public if they, as the perpetrator knows or should know, have been obtained by without right eavesdropping, recording or copying a conversation, transfer of data or processing of data by telecommunications or an automated work. In this way, having stolen computer data at one's disposal, placing the data at someone's disposal, or making these data public, is made punishable. In practice, data from hacked computers, such as passwords and access codes belonging to users, are often used. Criminals who forward digitally stolen information to third parties are currently not punishable because such information is not a 'good' (unless the person who forwards the information is also the hacker, which already leads to liability under Art. 138ab par. 2 DPC). As the concept of the Explanatory memorandum says, this new provision is really a criminalization of 'handling data derived from a crime', which is the counterpart of handling goods derived from a crime (Art. 416).

The result of this development would be that data are treated more and more in the same way as 'goods'.

4.4 Identity Theft

Dutch law does not contain a specific provision proscribing the (unlawful) appropriation of another person's (personal) information. The legislator has held off on the criminalization as a separate offence, primarily because of lack of practical need.[35]

The way the personal information is collected may, of course, constitute an offence.[36] Using the provision of theft itself is not an option, since theft (Art. 310 DPC) entails the removal of 'goods' and data are not considered as goods, at least not in this context. As remarked before, the Dutch Supreme Court has held that an (intangible) object may be considered a good provided it is an object that by its nature can be removed from the de facto control of another person. In the context of identity theft, this is per definition not the case since the victim does not lose the personal information. 'Fishing' will normally constitute the crime of deception (Art. 326 DPC): with the object of obtaining unlawful gain, inducing a person to make data available, for example by assuming a false name or false capacity. Apart from deception (and extortion, Art. 317 DPC), other offences may be committed, depending on the way the personal information is collected, like hacking or illegal interception.

Using (unlawfully) collected personal information will in many cases fall under a criminal provision, such as (again) deception, fraud (with travel documents and payment cards) or theft. The collecting of the information may, under circumstances, constitute a criminal attempt to commit these offences.

---

[35] For an overview of the discussion, see Van der Meulen 2011, p. 47.

[36] See also the Country Report, Section I, by Stamhuis (Chapter 2).

5 Content related offences

5.1 Child Pornography and Grooming

Child pornography is dealt with in Art. 240b DPC. This Article has been changed several times, in the last two decades. In 1996, the maximum penalty was increased substantially, from three months imprisonment to four years.[37] And a maximum penalty of six years was from this day on applicable in case the defendant committed his acts on a professional or habitual basis. A second paragraph however excluded criminal liability in case the picture was used for a scientific, educative or therapeutic goal. In 2002 the wind had changed direction and this second paragraph was abolished. [38] The legislator further decided that pictures taken from minors of 17 or 18 years old should be covered by this provision. And virtual child pornography was also included in Art. 240b DPC. In 2009, the maximum penalty on committing acts related to child pornography on a professional or habitual basis was increased to eight years imprisonment.[39] And, finally, in 2010 the treaty of Lanzarote was implemented.[40] By this Act gaining access to pictures of a sexual act (seemingly) involving a minor by using a computer system or a communication service was made a criminal offence.

As a result of all these changes, Art. 240b DPC now covers all pictures of a sexual act in which a person who apparently is under the age of eighteen is involved or seems to be involved. Distributing, offering, openly exposing, producing, import, transit, export, obtaining and possession of child pornography carries a maximum sentence of four years, and so does gaining access to these pictures by using a computer system or a communication service. Committing one or more of these acts on a professional or habitual basis carries a maximum sentence of eight years imprisonment.

There has been some discussion about what a picture of a sexual act actually means. In 1990 the Dutch Supreme Court decided that this term includes a picture of a minor in such a position that it obviously means to lead to sexual arousal.[41] This decision lead to a discussion in parliament. Some members of parliament said that the reprehensible character of child pornography was to be found in the abuse made of children, not in the fact that pictures lead to sexual arousal by an observer. [42] Pictures which only showed a nude minor should not be regarded as child pornography. Minister of Justice Sorgdrager more or less agreed with these members

[37] Wet van 13 november 1995, Staatsblad 1995. 575.
[38] Wet van 13 juli 2002, partiële wijziging zedelijkheidswetgeving, Staatsblad 388.
[39] Wet van 12 juni 2009, Staatsblad 245.
[40] Wet van 26 november 2009, Staatsblad 544.
[41] DSC 6 March 1990, NJ 1990/667.
[42] Kamerstukken II 1994/95, 23 682, no. 4, p. 4-7.

of parliament.[43] Advocate General Knigge, in an advisory opinion to the Dutch Supreme Court, however questioned whether this discussion should lead to another interpretation of the term sexual act. [44] He referred to an argument that in 2001 has been used by Minister of Justice Korthals to defend including virtual child pornography in Art. 240b DPC.[45] Banning virtual child pornography was considered necessary because it fosters a subculture with a market for child pornography. Relevant is also that the Minister of Justice at this point in time holds the opinion that making pornographic pictures by minors which are 16 or 17 years old, for own use, is a criminal offence, although prosecution is not considered necessary.[46] The Dutch Supreme Court thereupon decided in line with the decision it took in 1990. Decisive is whether the picture concerns either explicit sexual behavior, or minors in such a pose or environment that the picture has an unmistakable sexual meaning.

A decision the Dutch Supreme Court took in 2006 sheds some light on the question when a person can be said to be in possession of pornographic pictures.[47] In this case the Court of Appeal had convicted the defendant for possessing on the hard disc of his personal computer images which were classified as child pornography. The Dutch Supreme Court quashed this conviction. Taking into account that the acts mentioned in Art. 240b DPC constitute a crime, intent is required, according to the Supreme Court. And in this case, intent could not be inferred from the evidence selected by the Court of Appeal. The advisory opinion of Advocate General Knigge gives some extra information. He refers to a statement made by a policeman who had conducted the search in the computer. According to this policeman the pictures were found in the map Received, and the computer showed that the defendant had chatted with a lot of people. Knigge also refers to a statement of the defendant, who told the Court of Appeal that the pictures mentioned in the indictment were sent to him, that he had a look at them and then clicked them away because he was not interested in pictures like these. And he points out that the Court of Appeal has not responded to this statement, which is incompatible with a conviction for possession with intent.

The legislation implementing the treaty of Lanzarote also made grooming a criminal offence. This is described as proposing to meet, by an automated work or using a communication service, to a person who, as the perpetrator knows or should know, has not yet reached the age of sixteen, with the intent to commit sexual acts with that minor or to manufacture a picture of a sexual act in which this minor is involved, in case the

---

43 Kamerstukken II 1994/95, 23 682, no. 5, p. 7-11.
44 DSC 7 December 2010, NJ 2011/81.
45 Kamerstukken II 2001/02, 27 745, no. 6, p. 9.
46 Kamerstukken II 2001/02, 27 745, no. 6, p. 17.
47 DSC 28 February 2006, LJN: AU9104; see also DSC 26 October 2010, LJN: BO1713..

perpetrator commits an act to accomplish such a meeting (Art. 248e DPC). The maximum penalty is two years imprisonment.

5.2 Other Content related offences

Apart from child pornography, Dutch law does not contain other content-related offences that depend on the use of information and communication technology. Content related offences are formulated 'technologically neutral'. Many of these crimes use the term 'in writing' or 'written'. Discrimination concerns 'publicly, either orally or in writing or by image', intentionally making a defamatory statement about a group of persons (Art. 137c DPC). Slander (Art. 261 par. 1 DPC) done by means of 'written material or images, which are either disseminated, publicly displayed or posted, or by means of written material the contents of which are publicly uttered', constitutes libelous defamation (Art. 261 par. 2 DPC). With threat of a serious crime (Art. 285 par. 1 DPC), an increased maximum penalty is applicable where such threat is made 'in writing' stating a specific condition (par. 2). This element of 'in writing' (or 'written') does not lead to problems when applied to statements by electronic means. For example, an email containing a threat of a serious crime, constitutes a threat made in writing.[48]

The same goes for 'publicly', another much used element in content related offences (discrimination concerns publicly making a defamatory statement), and for 'dissemination' (for example dissemination of an object containing a defamatory statement, Art. 137e DPC). Putting a defamatory text on the internet constitutes 'publicly' making a defamatory statement (provided the public has access to the internet page).[49] It also constitutes 'dissemination' of the text. According to its traditional interpretation, 'dissemination' means putting a plurality of copies into circulation, but it is generally assumed that this interpretation has become obsolete in the internet era.[50]

[48] DSC 19 June 2007, LJN: BA3598.
[49] Court of Appeal Amsterdam 23 November 2009, LJN: BK4139.
[50] Janssens & Nieuwenhuis 2011, p. 90.

As regards cyber-stalking, this is not a separate offence. Art. 285b DPC criminalizes stalking in a technologically neutral way: the unlawful systematic invading of another person's privacy, with the objective of compelling that person to act, to refrain from acting or to submit to anything, or of intimidating him. Invading another person's privacy may be done by electronic means (telephone calls, posting messages on a website, sending email etc.[51]

6 Criminal Offences and the Virtual World

Apart from child pornography (see above), Dutch criminal law does not penalize the commission of crimes committed in the virtual world when no real persons are involved. The crime of (physical) abuse (Art. 300 DPC) requires inflicting bodily harm on another person, i.e. a real person. The same goes for rape (Art. 242 DPC): sexual penetration of the body is penetration of the body of a real person. And arson (art. 157 DPC) presupposes the setting of a real object in real fire.[52]

The situation only seems different with regard to property offences. In this context, the so called RuneScape case is important.[53] In this case the Dutch Supreme Court addressed the question of whether a virtual object is a good that can be stolen. The defendant, co-defendant and victim in this case were all keen players of the worldwide online computer game RuneScape. Classified as a 'massive multiplayer online role playing game', it is played in a virtual world. Players use personal accounts to create avatars, through which they fulfil quests, fight other players and do other things to gain points and earn virtual items. Each item has its own (virtual) value, expressed in 'coins', which players can use to hone their skills. The defendant and the co-defendant in this case took the then 13-year-old victim to the home of the co-defendant where they assaulted and threatened the victim with knives to coerce him to log into his account for the RuneScape game and then 'drop' (virtual) objects in the game environment. The defendant was then able to transfer a mask and an amulet belonging to the victim to his own account. The defendant and co-defendant were charged with the theft accompanied by violence (robbery) of these virtual items. Theft requires the 'removal' of 'goods' belonging to another person. The District Court of Leeuwarden and subsequently the Court of Appeal of Leeuwarden considered this to be theft: the perpetrators had taken away data that were unique and had economic value. And the Supreme Court agreed: it held that virtual objects like the virtual amulet and the virtual mask in the online game RuneScape were goods which can be the object of theft. The assertion that virtual objects are not goods because they consist of 'bits and bytes' was untenable. That these objects are virtual, does not mean that they cannot be considered a 'good' that can be stolen. The Dutch Supreme Court attaches weight to the

[51] Koops 2010a, p. 611.
[52] See also Viersma & Keupink 2006.
[53] DSC 31 January 2012, NJ 2012/536. This case is also discussed by Stamhuis in Country Report, Section I. See also Wolswijk 2012.

fact that to the victim as well as to both perpetrators the possessions acquired in this game constitute real value, that can be taken away from them. And it mentions that these values have arisen in the course of the game, and are or can be acquired by efforts and time investments. Finally it mentions that the victim had the actual and exclusive control over these objects, and that he had lost this control by the acts of both perpetrators.[54]

This case is not about a crime committed in the virtual world when no real persons are involved. As with abuse and rape, theft requires the involvement of a real person. Theft requires that a good is taken out of the control of a real person – as was the case.

Some additional remarks should be made with regard to this case, because it is a perfect example of the 'functional' or 'teleological' approach the Supreme Court follows in the interpretation of the elements of an offence. The decision in the Runescape case is in line with previous case law pertaining to the interpretation of the term 'goods', which is also discussed in the present case. In 1921 it was ruled that 'electrical energy', although intangible, was an asset that could be appropriated and therefore could be the subject of theft.[55] In this case the Supreme Court did not address the question of what electricity *was*, but considered certain *properties* of electricity to be relevant: it has an independent existence, is transferable, has a certain asset value and can be appropriated. Particularly in view of the *ratio* of criminalising theft – namely, to protect other people's assets – these properties mean that electricity must be regarded as a good.[56] Nevertheless, there are limits. The Supreme Court reaffirms in the Runescape case that an intangible object may be considered a good provided it is an object that by its nature can be removed from the *de facto* control of another person.[57]

---

[54] Apart from the 'goods' issue, there is the question as to whether the virtual items belong to the victim. Theft entails taking away property which belongs to another. One may think that the supplier and manager of the game is the owner of the virtual items and that he never had lost actual possession of the items. This argument does not stand up. 'Belonging to' in this context is not the same as 'owned by' under civil law; it is a broader concept. Goods can belong to a person without this person having the property rights. A person's passport is owned by the state, but can nevertheless be taken out of the holder's possession through theft. In this case the virtual items were in the victim's possession and thus they 'belonged' to the victim (from a ciminal law point of view). The fact that if players break the rules, the manager can intervene in the course of the game and ensure that the virtual items are returned to the victim's account is irrelevant, since any such intervention does not alter the fact that the 'cheat' has taken the virtual item away from the other person (against the rules), and the offence has as such been completed.

[55] DSC 23 May 1926, NJ 1921, p. 564.

[56] Previous judgments have also determined that electronic money (bank money) can be the subject of property offences. The Supreme Court has held that given the *function* of electronic money in society, viewing such funds as goods was a reasonable interpretation of the term 'goods' (Judgment of 11 May 1982, NJ 1982/583).

[57] That is why the memorized knowledge of a payment card's PIN code cannot be considered a good within the context of extortion (DSC 13 June 1995, NJ 1995/635).

As we have seen before, this is also the view of the legislator. This limitation also played a cardinal role in the first case in which the Dutch Supreme Court had to consider whether or not computer data can be regarded as goods.[58] The defendant, a systems administrator at a company, had copied and saved computer files he had in his possession for his job on disks and taken them home with him. He was charged with embezzlement of the files. According to the Supreme Court, computer data are not goods, because an essential property of goods is that the person who has control of them must lose it if another person gains control of them, and digital data lack this property. Whether or not this last statement is true under all circumstances, it certainly holds when data are copied.

It is precisely this case about computer data that the defence in the RuneScape case referred to in order to support its position that virtual items are not goods. The defence's reasoning was that a virtual item does not 'really' exist. Such an item is merely the visual representation of bits and bytes and therefore an illusion. The relocation of a virtual item is really just an alteration of data which causes a visual alteration on the screen. Therefore virtual items – to the extent that they are 'something' – cannot be regarded as anything more than data, and data are not goods.[59] The flaw in this reasoning is that precisely because virtual items such as those in question are the visual representation of data, they can be distinguished from the data themselves. While a person who has control over data may not necessarily lose that control if another person gains control over the data, this does not apply to the virtual items in question. The case makes this quite clear: the victim had control over the item and lost it due to the actions of the defendant. The case also shows how misleading the term 'virtual' is. What is the meaning of the assertion that a virtual mask does not 'really' exist? Obviously it is not a tangible mask, but that does not mean that it is therefore 'nothing'. As the Advocate General observed in his advisory opinion, a virtual mask is not purely imaginary, unlike the imaginary (virtual) board and pieces 'used' in a play of blindfold chess. It also becomes evident from the fact that the items in this case had a certain value for both the victim and the defendant. In fact, if it were different, the whole RuneScape game would be pointless.

In the context of Dutch law, the judgment in the present case does not really come as much of a surprise.[60] The Supreme Court has taken the same (pragmatic) functional or teleological approach as in previous cases.[61] Just as in the earlier case the Supreme Court was not interested in discussing what 'electrical energy'

---

[58] Judgment of 3 December 1996, NJ 1997/ 574.

[59] See also Moszkowicz 2009.

[60] See also M.J. Borgers comment on the judgment of the Court of Appeal in this case: Court of Appeal Leeuwarden 10 November 2009, NJ 2010/616.

[61] For an overview, see Groenhuijsen & Wiemans 1989.

actually was, in this case it did not go into detail about the technicalities – the bits and bytes - of virtual items. In a functional approach the main concern are the properties of such an item and the ratio of the provision determines which properties are relevant. With the criminal provision of theft, it is relevant that the object has a certain value and that an individual can be deprived of control of the object. The functional interpretation of the term 'goods' along the same lines in previous cases also makes this judgment acceptable from the view point of legality: Regarding the virtual items as goods is 'consistent with the essence of the offence and could reasonably be foreseen'.[62]

7 Non-Compliance Offences

The most important non-compliance offence is contained in Art. 184 DPC. According to this Article intentionally not obeying an order or demand, by virtue of a statutory prescription expressed by a civil servant who is in charge of investigating criminal offences is a criminal offence. The same applies if it is the task of the civil servant to exercise some form of control, supervision or surveillance. It is also a criminal offence to intentionally prevent or hinder an act, undertaken by such a civil servant to implement a statutory prescription. The maximum penalty is three months imprisonment.

In the Dutch Code of Criminal Procedure (DCCP) several Articles authorize civil servants in charge of investigating criminal offences (police officers, but also some civil servants employed by other authorities) to express demands to civilians. Especially relevant to cyber offences are the articles regarding investigation of communication by automated works (Articles 126la-126nb DCCP) and the articles regarding demanding data (Articles 126nc-126ni DCCP). Many of these articles are structured in (more or less) the same way: if a civil servant in charge of investigating criminal offences has reason to believe that a crime (of a certain gravity) has been committed, he or she can demand from a (specified) natural person or corporate entity that this person or entity furnishes specified data. Art. 126n DCCP for instance gives these civil servants (like policemen) the right to demand from a provider of a communications service to furnish data, specified in a regulation, concerning a user of a telecommunications service. Art. 126nc DCCP gives these civil servants –within certain limits- the right to demand identifying data (like name, address, birth date). Other demands can only be made by the prosecutor, sometimes after he has been authorized to do so by the investigating judge. A prosecutor is also a civil servant in charge of investigating criminal offences. If the demand is intentionally not met, the person who is addressed can be convicted on account of Art. 184 DPC.

---

[62] European Court of Human Rights 22 November 1995 A 335 C, C.R. v. The United Kingdom; see also the advisory opinion to the Supreme Court of the Advocate General.

In many cases, however, the demand cannot be directed at the person who is suspected to have committed the criminal offence. And persons who by a legal privilege are authorized to keep information secret, are not obliged to fulfill the demand.

References

Commissie Computercriminaliteit 1987

Commissie Computercriminaliteit, *Informatietechniek & Strafrecht*, Den Haag: Staatsuitgeverij, Ministerie van Justitie, 1987

Dijkstra & Keijzer

A. Dijkstra & N. Keijzer, 'Enkele honderd jaar oude strafbepalingen in verband gebracht met moderne gegevensverwerkingstechnieken', *Gedenkboek Honderd jaar Wetboek van Strafrecht*, Arnhem 1986, p. 453-469

Groenhuijsen & Wiemans 1989

M.S. Groenhuijsen & F.P.E. Wiemans, *Van elektriciteit naar computercriminaliteit*, Arnhem: Gouda Quint 1989

De Hullu 2012,

J. de Hullu, *Materieel strafrecht*, vijfde druk, Deventer: Kluwer 2012

Janssens & Nieuwenhuis 2011

A.L.J. Janssens & A.J. Nieuwenhuis, *Uitingsdelicten*, Deventer: Kluwer 2011

Van Kasperen 1990

H.W.K. van Kasperen, *Strafbaarstelling van computermisbruik*, Antwerpen/Deventer: Kluwer 1990

Koops & De Roos 2007

Bert-Jaap Koops & Theo de Roos, Materieel strafrecht en ICT, in B.J. Koops (ed.), *Strafrecht en ICT, Den Haag*: Sdu Uitgevers 2007 (2nd ed.), p. 23-75

Koops 2010a

B.J. Koops, 'Cybercrime Legislation in the Netherlands', in: *Netherlands Report to the Eighteenth International Congress of Comparative Law*, J.H.J.M. van Erp and L.P.W. van Vliet (eds.), Antwerp-Oxford-Portland: Intersentia 2010, p. 595-633

Koops 2010b

B.J. Koops, 'Tijd voor Computercriminaliteit III', *Nederlands Juristenblad* 2010, p. 2461-2466

Van der Meulen 2011

N.S. van der Meulen, *Financial Identity Theft*, The Hague: T.M.C. Asser Press 2011

Moszkowicz 2009

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

Oerlemans & Koops 2011

Jan-Jaap Oerlemans en Bert-Jaap Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *Nederlands Juristenblad 2011*, p. 1181-1185

Vellinga-Schootstra 1988

F. Vellinga-Schootstra, Gegevensbescherming en strafrecht, *Handelingen 1988 der Nederlandse Juristen Vereniging* 1988 deel I, Zwolle: Tjeenk Willink 1989

Viersma & Keupink 2006

M. Viersma & B.J.V. Keupink, 'Virtuele criminaliteit: all in the game', in: Arno Lodder (ed.), *Recht in een virtuele wereld. Juridische aspecten van Massive Multiplayer Online Role Playing Games (MMORPG)*, Nederlandse Vereniging voor Informatietechnologie en Recht 2006, p. 41-59

Wolswijk 2012

H.D. Wolswijk, 'Theft: Taking a Virtual Object in RuneScape', *The Journal of Criminal Law* 2012, p. 459-462