Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

CRIMINAL LAW ON CYBER CRIME IN THE NETHERLANDS; GENERAL PART AIDP COUNTRY REPORT SECTION I*

Evert F. STAMHUIS*

Chapter 1

Introduction

The case of the Facebook murder, before the Arnhem District Court on 20 to 21 of August 2012, attracted enormous media attention, not only in the Netherlands but also abroad. A young girl was stabbed by a teenager boy, who previously had a relation with the girl. The defendant was allegedly incited to the act by his friends through messages on the social network platform Facebook, which brought about the prosecution of those friends as accessories and gave the case its name. [1] The details of the case are not so relevant for this report, but the question arises: Do we witness here the situation in which homicide is also upgraded to the status of cyber crime? With that question we find ourselves in the midst of one of the hot items in a general part on cyber crime: finding a tool with which we can decide whether certain behavior is or should be categorized as cyber crime and what the consequences might be. In other words: can we arrive at a principled approach to cyber crime, learning form the legislation or doctrine in a certain jurisdiction. In this report on the legal state of the art in the Netherlands I will try to demonstrate how the Dutch legal system has approached this issue from the outset and which developments with respect to general doctrinal topics we have witnessed since the earliest legislation.

An account of the Dutch legal situation cannot succeed without reference to international developments. [2] Many new elements of Dutch criminal law on cyber crime were introduced as a follow up to international obligations, for the main part from European sources. The Council of Europe has contributed substantially to the development of law on cyber crime and the Dutch government has readily adopted the various international instruments that were the offspring of that development, thereby accepting the obligation to implement them into national law. I refer in this report to the Recommendation on Computer Related Crime, Council of Europe R(89)9, dated 13-09-1989; the

* 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. Evert F. Stamhuis LLM*. Chair for Criminal law and procedure and Dean of the School of Law, Open University (NL); honorary member Court of Appeal, Den Bosch (NL). The author is much indebted to Arno G.H. Kentgens, PhD candidate at Open University (NL) for having access to and permission to use some material from the concept texts of the dissertation. The views expressed in this report are of the author only. evert.stamhuis@ou.nl

[1] The trial of the principal murderer was concluded and sentence was handed down on September 3, 2012. He was convicted and sentenced to the maximum detention and treatment period for juveniles. The trial of the accessories was adjourned until later this fall for further examination. See for the sentence Arnhem District Court, 03-09-2012, LJN BX6328. For the convenience of those who read Dutch I refer to the number of all relevant cases in the open database of www.rechtspraak.nl, the so called LJN.

[2] See Kentgens & Stamhuis 2012

Cybercrime Convention, CETS 185 of 23-11-2001 and the Convention of Lanzarote, CETS 201 of 25-10-2007. The European Communities and later on the European Union also formulated legal instruments that influenced the content of Dutch national law. Specifically relevant are the EC Directive on Electronic Commerce 08-06-2000, 2000/31/EC OJ L 178/1 (17.07.2000) and the Framework Decision on attacks against information systems 2005/222/JHA of 24-02-2005 OJ L 069 (16.03.2005), although the latter did not induce many changes in Dutch law.

Beside the international dimension we need to mention the Report of the Commission on Computer Crime. This Commission was appointed by the minister of justice and published an important report in 1987, in which it presented an in-depth analysis of the state of affairs accompanied by detailed proposals for new legislation. The work of this Commission was in many aspects decisive for the following initiatives of the Dutch government and the Report remains an important source for the study of the Dutch approach until today. The commission observed that computer crime differed in so many aspects from ordinary crime that new descriptions of criminal behavior were called for.[3] The potential damage to important interests in society was found serious enough as to merit the use of criminal law, after appropriate adaptation to the new circumstances.[4] For that adaptation it provided ample material.

This report describes relevant general issues of criminal law as were discussed in Dutch law and doctrine. The connection to the AIDP questionnaire in Newsletter 1/2012 will be visible in the sequence of the chapters. First we will take a look at the criminalization topics and legislative technique; chapters 2 and 3. Then the topics of preparation and participation will follow in chapters 4 and 5, dealing with matters of the extent of criminal accountability and the position of intermediaries and service providers. To alternatives to criminalization attention is paid in chapter 6. Some remaining questions will be answered in chapter 7. Wherever possible I have tried to refrain form repetition with the material that will be discovered in the report in section II, but some overlap was unavoidable. An unofficial translation of some relevant parts of the Dutch Criminal Code (hereafter abbreviated as CCNL) is enclosed after the references.

Chapter 2

Interests, overlap and *lacunae*

The omnipresence of ICT in our society today renders a meaningful definition of cyber crime, that is a definition in which not everything is included, hard to attain. In the AIDP Newsletter 1/2012 the drafters of the questionnaire opt for an inclusive approach, which is all right for the purpose of the reports, but does not automatically mirror the state of affairs in the national jurisdictions. Nowadays, it seems hard to imagine an interest that cannot be affected by crime related to abuse of ICT. However, in this section we will focus on the choices that the Dutch legislator made, explicitly or implicitly, in its enactments of statutes amending the Criminal Code.

Guided by the abovementioned Commission on Computer Crime choices have been made in the late 80s and early 90s that appeared to be seminal for a considerable period of time. Particularly the strict separation the commission proposed between computer data and goods, ownership of the latter being protected by the property crimes, turned

[3] Large parts of substantive law were later found to be sufficiently technology neutral to provide for relevant instruments to combat crime in which an ICT element was present; Kamerstukken II 1997-98, 25880, nr. 2, p. 85, (Government Paper on Legislation for the Electronic Highway).
[4] Commission Report 1987, p. 29-30

out to determine many debates. As a result, protection of data ownership as such was not included in the criminal law and other crimes related to ownership could not apply on ICT criminals.

This conclusion on the nature and qualification of computer data served as a point of departure for the new legislation. Computer data differed from goods to such a large extent, that property rights to data were not definable as such. The exclusive availability of data to the owner was not an interest that could generally be protected by the criminal law.[5] For example, the data representing personal identity cannot be stolen from the person who carries the identity[6] and data on which intellectual property rights rested were not generally protected by provisions in the criminal code. An interference with personal privacy is as such not criminalized[7] and interference with data registrations related to personal identity is not a separate category as far as such interference with data is criminalized in general. The issue of identity theft will receive some attention further down in this paragraph and to data leakage we will pay some attention in the chapter on Alternatives. As for intellectual property: the Dutch Copyrights Act provides mainly for protection under civil law, but the limited protection of these intellectual property rights will receive some attention further down.

As a consequence of the conclusion that protection of data as such is impossible to aim at, the legislation is framed on protecting the systems and networks through which data are processed and the proper functioning of devices, systems and networks. The commission aims at serving the interests of availability, integrity and exclusivity of the physical instruments and of the data[8]; the hardware and the software as it was in those years, but also paid attention to the firmware, such as chips, the small components full of data, who only have use in combination with other hardware and software. Both the confidentiality/secrecy of data as well as the exclusive rights to using certain data were included in the Commission's concept of exclusivity.[9]

Many crimes, in the commission of which ICT plays a vital role, do not infringe typical cyber interests. However, these crimes are by many considered to be a threat to cyber safety and at least a part of it is included in the (international) initiatives to promote cyber safety using the criminal law. When we look at property crimes, child pornography, threats and reputation crimes (insult, slander[10]), crimes against equal treatment and security of minorities, breaches of confidentiality of non-public communication[11] (a special form of personal privacy violation), breaches of company secrecy, we see that the arrival of ICT has led to a new dimension of the classic crime. The more the ICT component determines the nature and/or impact of these crimes, the lesser classic crime descriptions express the moral judgment on them appropriately.[12] In some instances the ICT development has lead to additional criminalization. In that case the new forms of crime often bear features that are taken from the original non cyber version. That easily

[5] Koops & De Roos 2007, p. 23
[6] Identity theft will receive attention further down.
[7] Koops 2010, p. 20
[8] Commission Report 1987, p. 39
[9] Commission Report 1987, p. 47
[10] See for a case of a slanderous message on Hyves: Dutch Supreme Court 05-07-2011, LJN BQ2009
[11] Including communication between colleagues at work over a Local Area Network (LAN).
[12] Compare the first Additional Protocol to the Cybercrime Convention, concerning content crimes related to racism and xenophobia, 2003, CETS 189, where parties agree to additional criminalization of the distribution of racist or xenophobic material through a computer system.

leads to accumulation of crime definitions where the classic description is not repealed most of the times. A risk of overlap and unclear demarcation between separate crimes is the consequence. For example content cyber crimes (i.e. distribution of illegal content over the worldwide web) are considered to be a serious breach of internet integrity, but are in origin violations of other interests. This multiple nature of the cyber crimes and the overlapping of interests and elements in specific instances are also reflected in Dutch criminal law.

Let us look at the example of distribution of data retrieved with a violation of confidentiality (Art. 139e CCNL). In addition to the actual breach by obtaining the data, the further distribution constitutes an extra infringement of the protected interest of confidentiality. However, the activity also bears similarity with the crime of handling stolen goods, which is under Dutch law limited to cases where the illegal obtaining was not committed by the distributor.[13] The introduction of Art.139e CCNL in Dutch law was justified by reference to telecom confidentiality protection. The actual unity or difference between obtaining and distribution is irrelevant for the protection of that interest. Who took and who distributed the data can be one person or more, the confidentiality is violated more seriously anyway when the information is distributed.

With this crime the legislator tried to overcome the evidential difficulties one might encounter as to who actually tapped or stored the data from their origin. That might be hard to find out after data have been found roaming over the internet. When data are discovered in someone's data store facilities the case is rather clear-cut. The only *actus reus* to prove is the connection between storage device and person, e.g. ownership, and the lack of authority at the side of that person. That part can easily be substantiated by the absence of permission stated by the original owner of the data. In this respect the similarity with the crime of handling stolen goods comes to mind, where under Dutch law the presence of stolen goods in the 'hands' of the agent and the lack of permission from the owner suffices to prove *actus reus*. Being the person that illegally obtained the goods in the first place amounts to a successful defense against a charge of handling stolen goods, but contains a confession for theft. For the crime of Art. 139e CCNL as described above, the same defense bears no consequence of that nature.

Also the crime of Art. 273 par. 1 sub 2, CCNL demonstrates resemblance with this type of data handling. The *actus reus* is: publishing or using for profit data that are illicitly retrieved from an automated device owned by a commercial, industrial or service company; boiling down to abuse of company secrets. It is understood that, contrary to the crime of handling stolen goods and parallel to Art. 139e as describes above, it is irrelevant for the crime of Art. 273 who illegally obtained the data in the first place. Prosecution of handling data that are illegally obtained under the general provisions of handling stolen goods (Art. 416 – 417bis CCNL) was until recent times blocked by the basic assumption of the Dutch legislator, that data are not 'goods'.[14] The crime definitions discussed above (Art 139e and 273 CCNL) are therefore a necessary addition as long as the strict separation between data and goods is upheld. In addition, the

[13] Handling stolen goods being a crime of promoting other crimes; contrary to Commission Report 1987, p. 61-62, stating: handling stolen goods for profit is a property crime.

[14] In Dutch Supreme Court 31-01-2012, LJN BQ6575 and Dutch Supreme Court 17-04-2012, LJN BV9064, credits for telecommunication service were qualified as goods, observing the economic function of the credits in society. They can be object of appropriation (theft) and handling illegally obtained goods as in Art. 416 and 417bis CCNL. The Supreme Court refers in the first judgment to the overlap that exists between theft of credits and the crime of art. 326c CCNL: illicit use of telecom services, inserted in the code to protect the service providers as well as others.

insertion of these crimes provides a convenient opportunity to exempt from the rule that "he who commits the crime cannot be qualified as the promoter of the same". However, these crimes are limited to data with a specific nature (in breach of telecom confidentiality; in breach of company secrets). New legislation has been announced to provide for a wider range of criminalization of illicit data handling and of copying without right of non-public data to which one had lawful access.[15] When inserted under the chapter of handling stolen goods, the rule that one cannot promote one's own crime will apply. So far, no draft texts have been sent to parliament.

The explicit choice of Dutch legislation to draw a clear line between goods and data, that is helpful to categorize handling 'stolen' data, seems subject to erosion. It is not the prosecution of ICT crimes under ordinary property crimes that necessarily amounts to this erosive effect. Theft by using illicitly obtained chip cards, PIN's, passwords etc. still concerns illegal appropriation of money, although it may imply false manipulation of data. Qualification as property crime does have erosive effect on the clear separation of goods and data when objects in the digital world are recognized to represent a certain value in the real world that can illegally be taken from the owner. The case of RuneScape has to be discussed here, in which the Dutch Supreme Court released its judgment on 30-01-2012, LJN BQ9251.

In this case, as well as in the Habbo Hotel case[16], we enter the world of games. Digital games are played according to rules and usually carry (sequences of) success or failure, either rewarded or punished with advance or setback, in relation either to one's competitors or to the finish, or both. In sophisticated games, many of which are played via the World Wide Web, the players can accumulate and store successes by way of virtual credits, often named in accordance with the virtual world or atmosphere in which the players move about. In some games these virtual assets can also be bought or exchanged for real money, but in many they just represent the success and endurance of the individual player.

In the RuneScape case the victim had obtained virtual assets (called an amulet and a sword of some kind) by playing long and successfully. He then was threatened by schoolmates into providing access to these assets in the game world. These mates took the sword and the amulet from the store and used them to their own benefit; all inside the game. The matter was reported to the police and a prosecution for a property crime ensued subsequently. The obvious question before the court was whether these virtual assets could become object of a property crime, since the Dutch legislator had stressed time and time again that a strict distinction was intended between data on the one hand and goods on the other hand.

Under the Dutch law for property crime the meaning of the word "good" (central in property crime) was already extended to immaterial assets that can be taken from the authority of the owner. In the RuneScape judgment the Supreme Court refers to its case law on electricity (1921) and money on a bank account (1982), both accepted as "goods" under the criminal law. On the contrary, extortion of a PIN was not a property crime (1995). Crucial for the

[15] Kamerstukken II 2008-09, 28684, nr. 232, p. 4. Compare the proposal in Commission Report 1987, p. 62

[16] Koops 2010, 13 also refers to this Habbo Hotel case, that did not reach the SC, but basically had the same outcome: Amsterdam District Court 02-04-2009, LJN BH9789 – BH9791. The (juvenile) court in this case is less explicit on the issues of goods and appropriation, but pays more attention to the requirements for co-perpetration. Its observations on the non-applicability of art. 138a CCNL (art. 138ab as is now stands) carry some reference to the qualification of taking virtual furniture in Habbo Hotel as appropriation.

classification appears to be whether the availability of the asset to the owner ends as a consequence of the illicit appropriation by the perpetrator. Besides, that was indeed the decisive motive at the time of the first legislation on computer crime to distinguish data from goods: appropriation of computer data means copying what remains with the owner. No exclusive availability is transferred from the owner to the taker.[17]

In the RuneScape case the exclusivity feature was clearly established by the judge of facts for the digital assets: the sword and the amulet. That enabled the Supreme Court to adhere to its line of case law: these game assets are immaterial and exclusive and can be protected by the law on illegal appropriation. The Supreme Court's judgment refers to the value that those assets have in the context of the game, which value is accumulated with effort and time investment and can be taken from the owner, who normally has the exclusive ownership of these assets.

By being virtual the assets at stake, the sword and the amulet, also meet the general description in the Criminal Code of data in Art. 80quinquies CCNL. The argument was raised before the Supreme Court that for this reason a qualification as "good" is against the law. This reference to a strict distinction is rejected by the Supreme Court. Being categorized under "data" does not as such preclude being categorized under "good" as well. The Court recognizes borderline cases to occur in its case law that goods can be immaterial, but those cases have to be resolved according to the factual context. The Supreme Court desists from giving further general rules or criteria.

Important in the RuneScape case is, that the termination of exclusive authority of the owner was well established. This exclusivity being an essential feature of "good" was earlier underlined by the Supreme Court in a case (stemming from Aruba) of computer data of 1996. To this case the attorney general refers in his opinion, but surprisingly the Supreme Court does not mention the judgment in its observations.

As the Supreme Court in the RuneScape case expresses: virtual objects in the digital world can be qualified at the same time as being "computer data" and a "good" in terms of the property crimes. To my appreciation this marks the erosion of the intention of the legislators as a consequence of ICT developments. A clear demarcation was expected to be achieved by stressing that data are not goods, and it worked like that for a time. As already mentioned, it helped to clarify the position of handling illegally obtained data. The non applicability of the provisions on handling stolen goods was based on the reasoning that data could not be qualified as goods. That opinion obviously predates the RuneScape case.[18] A consequence of the Supreme Court's reasoning could be, that the use of the stolen RuneScape amulet by someone else who had not actually taken it, can be qualified as the crime of handling stolen goods.[19]

The question can be raised where to go to from here. Is the next step to abolish the distinction between goods and data? In my appreciation it does not serve us to push that particular debate too far. A less dichotomous approach might bear fruit as well for the categorization of illicit actions in relation to data. Maybe a strict borderline between the objects of crime (data versus goods) is not necessary, where we could distinguish between the separate actions. Appropriation (of goods, either material, immaterial or virtual) stands for an action where the availability is transferred

[17] See Commission Report 1987, p. 38: goods are exclusive, data are multiple.
[18] See Kamerstukken II, 2007-08, Aanhangsel van de Handelingen 888.
[19] In the case of Dutch Supreme Court 17-04-2012, LJN BV9064, referred to above, the Supreme Court found that credits for telecommunication service can be qualified as objects of handling illegally obtained goods.

from the owner to the agent, opposite to interference which does not have that same consequence[20]. In case of the former, categorization as a property crime[21] is possible, where it is not for the latter. In essence this does not divert very much from the approach of the Commission, which also derived its categories from the action results and not from the respective objects.[22] We only abandon the last step of the Commission's line of argument, where it said that consequently data cannot be appropriated. We now know that they can.

Both the appropriation of the virtual assets as in the RuneScape case and the difficulties in finding the appropriate language to address *actus reus,* to be dealt with in the next chapter, bring us to some observations on the issue of identity theft. Identity theft covers a wide range of illicit behavior and is not limited to cyberspace. It varies from fraudulent taking and/or using of someone's real name or any ID tool in order to gain (financial) benefits, to obtaining someone's carefully constructed virtual identity in a virtual world to gain benefit or to cause harm.[23] The extortion of a PIN or TAN code counts as such, but also the abuse of a person's social security number or driver's license. Somewhere in this gamma we may even find the interference with someone's social network site identity, which is the accumulation of personal data, messages, virtual connections ('friends') and posted media messages, or the participation in Twitter traffic with the false use of the identity of a VIP. Apart from the actual harm in financial terms, the victims of all these various types of fraud suffer at length from the burden to clear their name or reputation from the damage.[24]

Under Dutch law these illicit actions are not always criminalized specifically, if at all. Deception to gain benefit (Art. 326 CCNL) is a category in which many of these action fall, where the various statutory instruments for deception are taken broadly. A large part of the field in which ICT is involved is covered by the crime of deceit to provide data. In addition tot that, now that the Supreme Court accepted in the RuneScape judgment that a virtual asset with economic value, that is only a compilation of computer data (in the statutory meaning of Art. 80quinquies CCNL) can be object of appropriation, an extra part of ID theft is covered. Harm to a person's reputation however has to be as serious as insult or slander (Art. 266 and 262 CCNL) before it could fall under the criminal law. Many actions of this kind can only be countered by using civil law suits, for which tracking down the actual agent poses a problem to the victim.[25] This does not amount to a plea for additional criminalization. My appreciation is, that the *actus reus* for

[20] See the brief introduction into American, English and German law in the Attorney General's opinion in the RuneScape case.
[21] To avoid misunderstanding: I refer to Titles XXII, XXIII and XXIV of the Second Book of CCNL. For the crime of fraud (deceit; art. 326 CCNL) the matter is resolved by the explicit insertion of: "deceit into providing data".
[22] See Commission Report 1987, p. 38-39.
[23] Compare Roadmap "Legislative proposal on criminalization of identity theft (included in the European strategy on identity management) on http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_013_identity_theft_en.pdf (accessed Aug. 2012)
[24] Van der Meulen & Koops 2012, discussing several reprimands the Dutch Government received from the National Ombudsman and the Strassbourg Court in ECHR 14-02-2012, app.nr. 7094/06 (Romet/The Netherlands); in the light of the authorities' responsibility for correction of data in registration systems in cases of identity fraud.
[25] I refer to the limited availability of a civil court warrant addressed to the ISP to deliver details on the owner of a specific account, mentioned in chapter 6 of this report on Alternatives.

identity theft in all its variety can only be covered by very broad words, that will turn out to be all but a repetition of the crime of deceit.[26]

Chapter 3

Overview of legislative technique: instruments, objects and terminology

The purpose of this chapter is to provide insight into the way the ICT components of crimes feature in Dutch criminal law. A distinction is presented between the ICT component as an instrument in the description of the crime as opposite to the ICT component as the object of the crime. A translation of the Dutch text into English is used, for which no one vouches but myself. A direct use of the English terminology, such as used in the Cybercrime Convention, was not possible on all occasions. After that overview some extra attention is paid to the choice of appropriate verbs to describe *actus reus*, relevant in particular for the quest for technology neutral legislation. In passing some classic terminology that proved relevant for ICT applications will be mentioned.

Before we run down the list of instruments and objects, we read the articles in the Dutch Criminal Code in which definitions are inserted. One title of the General Part of the code is dedicated to definitions, Title IX of Book 1, and the earliest legislation on computer crime inserted some definitions that are relevant for cyber crime, proposed by the abovementioned Commission on Computer Crime. Art. 80*quinquies* CCNL defines data as: "every reproduction of facts, concepts or instructions, in an agreed way/manner, adapted/appropriate for transmission, interpretation or processing by persons or automated devices". We can see here that this definition is not limited to ICT related data and that the ICT component is instrumental only in the final part of the definition. Art. 80*sexies* CCNL defines automated device as: "an installation destined to store, process and transmit data electronically", in which we can see the ICT component expressed as the instrument in "electronically", in order to distinguish from data processing/storage on paper.[27]

The ICT component is instrumental to the commission of the crime

We encounter the ICT component in its instrumental capacity in various wordings. In the list I present the words in my translation of the Dutch statutory text, followed by the numbers of the articles of the CCNL, unless otherwise indicated.

ICT component	***Art. of CCNL***
By automated device	240b, 248e
Using automated route/way	232
Using/deploying a technical instrument	139c
By telecommunication (network)(service)	

[26] The criminal policy observations of Van der Meulen en Koops (o.c.) merit support, where they plead for an approach of the risks of identity fraud other than just (further) criminalization. There is a central window for reporting identity fraud on the government website www.overheid.nl.

[27] The use of the word processing will receive attention towards the end of this chapter. Unfortunately the verb of processing is here juxtaposed to store and transmit, where elsewhere the storage is included in the word processing and we only see: process or transmit.

(see Art.1.1 sub c Telecommunication Act) 161sexies, 161septies, 326c, 54a

By using communication service

(see Art. 126*la* Code of Criminal Procedure:

communication with the use of

an automated device) 240b, 248e

Note: The communication with the use of an automated device includes mobile phones and was meant to extend communication from the old style cable network to the modern style ether/digital network. This distinction between communication over the telecom network and communication with the use of an automated device becomes less and less relevant now. Smart phones are predominant in today's communication practice, a combination of phone and mobile mini computer that uses the telecom network for all kinds of services. The only relevant category to remain beside communication over the telecom network (i.e. a combination of ether and cable) may be the communication over a LAN.

The ICT component is object of the commission of the crime

In its object capacity the ICT component is also present in the Criminal Code in different expressions. The limited variety might suggest a higher level of uniformity than can actually be found. Therefore the (translation of the) context is summarized in the list in order to give a representation of the variety of wordings in ICT crimes.

ICT component	***context***	***Art. of CCNL***
Automated device	illegal access to	138ab
	obstruction of access to or use of	138b
	illegal tapping of data transmitted by	139c
	preparation to the crimes of 138ab, 138b and 139c	139d par. 2, 3
	handling data etc. produced by 139c	139e
	destroy, damage or render unfit for use of with specified consequences	161sexies
	publishing/handling company data, illegally obtained from	273
	illegal interference with data stored, processed or transmitted by, hacking included	350a, par 1,2
	provision or distribution of data destined to damage	350a, par. 3
	culpable version of 350a	350b

	damage of … for public service	
	or national defense	351
	culpable version of 351	351bis
Telecommunication	illegal tapping of data transmitted by	139c
	preparation to the crime of 139c	139d
	handling data etc. produced by 139c	139e
	destroy, damage, render unfit for use of with specified	
	consequences	161sexies
	culpable version of 161sexies	161septies
	violation of telecom confidentiality	273d
	false use of service, provided to	
	the public by	326c
	bribery in relation to	328quater
	illegal interference with data stored,	
	processed or transmitted by …,	
	hacking included	350a
	culpable version of 350a	350b
	damage of … for public service	
	or national defense	351
	culpable version of 351	351bis
	illegal request for traffic data	
	to person working for	371
Data	copy, tap, record	138ab
	extortion to provide	317
	blackmail to provide	318
	deceit into providing	326
	provision or distribution of …	
	destined to damage …	350a, par. 3
Technical instrument	possess with specified intent	139d par 1
	produce, sell, obtain, import, distribute	
	or otherwise provide or possess with	
	specified intent	139d, par. 2, 3;

Before we move on, a concise discussion seems appropriate of some classic phrases from the Criminal Code that have been interpreted by the Dutch courts to cover ICT applications, just to demonstrate the considerable level of flexibility that has been attained. The crime of falsification of documents (Art. 225 CCNL) was of course intended to cover fraudulent writing or printing. Nevertheless, it is accepted under Dutch law to qualify the compilation of a false digital document that is only read from a computer screen and never printed, as a breach of Art. 225 CCNL. Another example relates to taking money from an ATM with the false use of a chip card, either by manipulation of the data on the chip or by using a stolen card with PIN. It qualifies as aggravated theft, using a false key (Art. 311 CCNL), although the term "key" was originally supposed to cover only the iron instrument that we use to open a lock.[28]

The phrase "data carrier", used in various sectors of Dutch law, represents a separate issue. At a glance it may explicitly refer to computer data, comprising the devices on which we store these data. Theoretically, it could have been used in the description of crimes regarding illicit data interference. These devices may change rather quickly over the course of the years – it is hard to spot a CD ROM nowadays – but the word "carrier" appears to be sufficiently flexible. The term is not extensively used in substantive cyber crime law[29] and can also be found in the code of criminal procedure. Its meaning is not explicitly defined under the Definitions in Title VI of Book 1 of the Criminal Procedure Code. It was intended to cover both printed and digital information as well as other forms of electronically stored information such as sound tapes. Since it includes both printing and all electronic or digital forms, it might not be exclusively ICT related, but we may reconsider its use in substantive law, e.g. should the decision to criminalize identity theft be taken. That crime might comprise the use of any data carrier to state false identity.

To arrive at technology neutral language is one of the problems for modern cyber crime legislation. I already referred to the use of the verb "interfere" when dealing with the *actus reus* for crimes other than appropriation, but that remains vague terminology. There are good reasons for the legislator to seek refuge in broad terms in order to avoid losing track with rapid technological changes, but the Dutch legality principle has apparently pushed towards more concrete language, on top of the fact that a suitable Dutch translation of "interference" is hard to find. In Dutch statutory crime descriptions other words are used to further clarify the meaning of the *actus reus* (and thereby limit it). To give some examples: copy, tap, record (Art. 138ab par. 2 CCNL[30]); alter, erase, render useless or inaccessible, add data to (Art. 350a par. 1 CCNL[31]). Those actions may all fall under the umbrella of interference.[32]

Let us continue the search for technology neutral terms just one second. Another option for a verb to indicate *actus reus* might be "to process", a word common in data protection legislation and also imported here and there into the criminal law. Data processing seems to cover everything one can do with data. Therefore it might serve as an umbrella term as well and hold for a while under new technological innovations. In Dutch criminal law processing is

---

[28] De Hullu 2012, p. 104; see art. 90 CCNL for the definition: False keys include all utensils that are not intended *to open the lock*.
[29] The concept 'information carrier" in art. 46 CCNL comes very close to it, but may cover slightly differing collections. "Data carrier" as a term has replaced "information carrier" in art. 240b CCNL. See already Commission Report 1987, p. 66
[30] The text of Art. 138ab CCNL is provided after the references.
[31] The text of Art. 350a CCNL is provided after the references.
[32] See also Koops 2010, p. 8: in his opinion "adding to existing data" is not covered by "interfering".

not used, although it could have been available for the *actus reus* of for example Art. 139e or Art. 273 CCNL. I am not aware of any reason for not using this term other than its broad content. The Commission on Computer Crime did not discuss it in its report.

Another option for the expression of *actus reus* of many ICT crimes might be: to manipulate data. That might cover the change of the original status of data as well as additions to data. Where "processing" appears to be a neutral term, "interfere" and "manipulate" seems to be appreciative language, implying lack of authority. Whatever the distinctive nature of the terms is, all three options reveal the difficulty when seeking less change sensitive language. One moves easily towards too broad container terminology which causes tension with the *lex certa* rule that many European jurisdictions try to respect.[33]

Chapter 4

Criminalization of *potential* damage; inchoate crimes

In the Netherlands, as in many other jurisdictions, the national criminal law comprises inchoate crimes. Basically, general doctrine recognizes three separate forms of these: attempt, preparation and conspiracy. Conspiracy is criminalized only for offences against the state and terrorist attacks,[34] where there is a widespread hesitation to criminalize conspiracy as under the common law. Criminal liability is preferably connected to an overt act, to be specified in the statutory description of the crime. Therefore a broad general criminalization of conspiracy is rejected as lacking the necessary specification. At het moment it has no statutory basis. In this chapter we will deal with some general observations on attempt and preparation as incomplete forms of causing damage to the interests protected by the law on cyber crime. Preparation takes the largest part, because in the Dutch legislation some specific forms of preparatory activity have been criminalized. Obviously the incomplete forms posed sufficient risk as to merit their own place in the criminal code, particularly with a view to the limited scope of the general provision on preparation in Art. 46 CCNL.[35]

A punishable attempt is generally defined in Art. 45 CCNL[36] and is only relevant for crimes and not for misdemeanors. In case of conviction the maximum penalty for the attempt is reduced to two thirds of the statutory maximum of the crime to which the attempt was related. General requirements for attempt are the intent to commit the crime and an actual commencement of the execution of that intent. In case the execution of the crime was not completed due to a voluntary and timely retreat by the agent, no conviction for attempt can be obtained; Art. 46b CCNL. As to the intent requirements, the general doctrine on this subjective element applies and includes all varieties of intent that are accepted in the case law of the Dutch Supreme Court. Much more than on intent, the doctrinal and case law development is focused on what commencement of the execution of that intent implies.[37]

---

[33] The case law of the Strassbourg Human Rights Court on legality under art. 7 ECHR recognizes the need to using broad terminology, especially in rapidly changing circumstances or technological specific branches. See ECHR 26-04-1979, Sunday Times/UK; ECHR 22-11-1995, C.R./UK; ECHR 15-11-1996, Cantoni/France.

[34] Probably what US President Obama had in mind in his post on http://online.wsj.com dated July 19, 2012: Taking the Cyberattack Threat Seriously.

[35] The text of Art. 46 CCNL is provided after the references.

[36] The text of Art. 45 CCNL is provided after the references.

[37] De Hullu 2012, p. 375

Generally the required commencement works as a precaution against prosecutions of malicious intent only. To intentions it supposedly adds sufficient objective actions so that real danger in the outside world is separated from dangerous contemplations in the psyche of an individual. The Dutch Supreme Court arrived at the following criterion that it applies until this day[38]: liable for attempt is anyone whose actions are, judging on their outside appearance, aimed at the completion of the crime. This is a phrase in which the enormous variety of day-to-day reality as well as features of the specific crime can be included.

For attempts to cyber crimes the abovementioned general approach applies. The legislation does carry some specific forms of incomplete crimes, to which we will come immediately hereafter, but they come closer to preparation than to attempt.[39] Of course many forms of incomplete actions, that is actions that did not cause the harm or consequence the criminal code requires for liability, can be imagined in the field of cyber crime. As the law stands those incomplete actions can be qualified as one out of three options: (a) as attempt to a complete crime; (b) as the specifically included crimes of preparation; (c) as an attempt to these specific preparatory crimes. The last variety may be an awkward combination, but cannot be excluded as a doctrinal consequence of the inclusion of the specific preparatory crimes in the code. Basically, attempt is possible to any crime.

Koops & De Roos argue that a port scan could under circumstances lead to liability for attempted hacking.[40] Their observations concern mainly the service providers that scan connected computers for open ports as a part of their security policy. Since such practice is covered by either contract or statutory duty, the activity is not without right and therefore no crime, according to these authors. What they probably mean is that the intent requirement will be absent, since those agents will not have the intent to gain access illegally, which is required for an attempt to commission of the crime of Art. 138ab CCNL. This intent will also serve to clarify other cases of port scanning, to which the authors refer. Elsewhere Koops points at the example of virus toolkit distribution that might be covered neither by a specific offence, nor by the general attempt provision.[41] This indeed appears to be an example where the provider cannot, but the receiver can be held accountable under the criminal law, provided that the necessary *mens rea* is discovered at the receivers side.

Including preparation as a separate offence in the criminal code serves various purposes. First of all, the preparatory stage represents already a serious threat to the interests protected by the law and therefore cannot be ignored. Secondly, on some occasions the actual harm to the protected interests may already have occurred, but the actual discovery of the perpetrator promises such enormous difficulties that the ability to hold liable those who shared some responsibility for that occurrence and whose actions are easier to discover, represents the sole instrument in reality

[38] De Hullu 2012, p. 379-382. Originally the case law particularly served the purpose of distinguishing attempt from the – at that time - not yet criminalized preparatory activity. Since 1994 the General Part of the Criminal Code carries a provision on preparation, art. 46 CCNL, but the Supreme Court did not exchange its approach to attempt for a new one since.

[39] Koops 2010, p. 10, argues that art. 350a par. 3 CCNL is a form of attempt more than of preparation contrary to the statement of the minister. For the decision on that specific point I refer to the debate in section II. The parliamentary sources may provide a less mixed message than Koops points out. In my reading of Kamerstukken II, 2004/05, 26671, nr. 7, p. 36 the minister refers to the additions to art. 139d CCNL and not to art. 350a par. 3 CCNL, leading to the assumption that the minister and Koops share the same opinion.

[40] Koops & De Roos 2007, p. 30

[41] Koops 2010, p. 10

to combat the actual harm. When deciding that preparation to a crime should be a criminal act itself, the options for the legislator are twofold: a general provision for all crimes, such as for attempt, or insertion of special preparatory crimes. The legislator in the Netherlands professed preference to use both options in the law on cyber crime.

Art. 46 CCNL is the general provision for criminal preparation. This criminalization of preparatory actions is limited to preparation of serious crimes. Art. 46 CCNL only covers actions in relation to crimes that carry a maximum penalty of 8 years and over. That level of seriousness is only met in two aggravated forms of the crime of Art. 161sexies CCNL. Therefore, the implementation of the international agreement to criminalize the preparatory stage (Art. 6 Cybercrime Convention) led to inclusion of new separate crimes. That prevented the legislator from a possibly controversial enlargement of the scope of Art. 46 CCNL. A collateral asset of separate criminalization was the freedom to determine maximum penalty as to fit the specific crimes. As a result of the general regulation in Art. 46 CCNL, the maximum penalty for the preparation would be fixed to 50 % of the maximum carried by the crime that was prepared. By opting for the addition of new crimes the legislator could set the maximum as he found it appropriate. For example, designing hacking software was found to be as serious as the actual hacking, although the former can be perceived as preparing the latter. Equal treatment of both would have been impossible when limited to the general provision of Art. 46 CCNL. Now the Code carries the same maximum penalty for both crimes as separately incorporated in the code.[42]

As already said, the criminalization of the preparatory stage is mainly a consequence of the Cybercrime Convention.[43] The evidential requirements are not too complicated, as was the purpose of the Convention. For example, Art. 139d par. 2 CCNL mentioned the production, distribution etcetera of a technical instrument with the "primary" and not the "sole" designation to commit various ICT crimes. As the Explanatory Report to the Cybercrime Convention stated: "exclusively and specifically … could lead to insurmountable difficulties of proof".[44]

Separate crimes for preparatory activities do not share in the general provision for voluntary retreat, that is included in Art. 46b CCNL.[45] As a general rule for attempt as well as preparation no liability exists in case the agent prevents the commission of the crime he has prepared. This general rule has no effect on the preparatory crimes that are present in the law on cyber crime. The result is particularly unbalanced now that for the less serious crimes the 'conversion' of the agent, followed by appropriate action to prevent the commission of the crime, bears no consequences where it does so for the preparation of more serious crimes. Having prepared the more serious crimes can be considered as having exposed society to a higher risk, but the agent still profits from his timely retreat. The sole justification for that might be, that for these higher risks the temptation to retreat must last as long as possible. It may hardly ever occur in cyber crime, but in my view this difference between general rule and special crimes merits attention in a balanced criminalization of the pre-commission phase.[46]

---

[42] The support for the difference with 46 CCNL could have been firmer. See Kamerstukken I, 26 671 en 30 036 (R 1784), nr. D, p. 14.

[43] Commission Report 1987, p. 58, already considered the risk for more serious harm posed by less invasive acts: illegal access as preparatory for damaging. Art 326c CCNL was introduced in the first computer crime legislation in 1993.

[44] Explanatory Report 2001, 73

[45] De Hullu 2012, p. 411-412

[46] The limitations mentioned in Explanatory Report 2001, 76 and 77, do not present a remedy to this unbalance.

The negotiators preparing the Cybercrime Convention were worried that the good may suffer with the bad in a too broad criminalization of preparatory activity. They arrived at a liability exclusion for security experts, antivirus software designers and the like in article 6 par. 2 of the Cybercrime Convention. This provision is implemented in the specific extra *mens rea* requirement of Art. 139d, par 2 and 3 CCNL: "with the purpose of …..". The computer security expert is thereby protected against unjust criminalization when availing himself of devices as listed in Art.139d, par. 2 CCNL. The (sometimes self appointed) security experts however, who practice hacking as one of their tools to discover security risks in a system and report their successful hacking to the owner of the system, are not saved from liability. The description of the relevant crime, Art. 138ab CCNL, does not carry an extra "with the purpose of …" element.[47] The position of these Robin Hoods of cyberspace has been discussed in the parliamentary legislation process, where the minister explicitly rejected immunity, even for those acting with the best intentions. The hacking of a system is in itself too risky to apply as a tool without prior authorization by the owner (and with proper safeguards in place). Good intentions may only be rewarded by a reduced sentence.[48]

The position under Dutch law of the ineffective preparation, that is the preparatory activity that could never have successfully contributed to the commission of the crime, is also derived from the specific as well as the general doctrine. Under Art. 139d par. 2 CCNL the inadequate devices are to be appreciated in the same way as the clumsy actions in general theory on preparation. By a certain interpretation of "destined to commit the crime" as can be concluded from the parliamentary documents, liability is excluded, when this destination was out of reach. The chances of realization of the intended offence must effectively be raised by the agent, which implies a level of aptitude of the device, password etc, in an objective perspective. Objective perspective here refers to the discovery afterwards. No such destination can be attributed to the invalid password, although the dishonest intent of the actor was to provide a password to someone for hacking purposes. It is not the dishonesty of the agent alone that renders a specific device or instrument fit for the illicit purpose. On the other hand, liability is not limited to the preparation with devices that obviously, in objective observation, carried the required designation to be useful. The established capacities of the device in combination with the *mens rea* of the agent amount to the liability for preparation.[49]

As a conclusion of this chapter, two specific preparation crime will be mentioned here, but merely in passing since they will receive more attention in section II: the behavior potentially leading to child abuse and the preparation of violations of intellectual property rights on software.[50] Let me start with the latter. Art. 32a Copyright Act carries a copyright version of Art. 139d, par. 2 CCNL. The *actus reus* is put in slightly different words, as well as the destination of the instruments. For the latter the Act refers to: the *exclusive* designation to facilitate the removal or avoidance of a technical device that protects the software. The word exclusive is remarkable here, where it was expected to pose too many evidential difficulties for the crime of Art. 139d, par. 2 CCNL and exclusive purpose is also not required in the general provision of Art. 46 CCNL. As to the *actus reus* the Act lists: (a) to offer publicly for distribution; (b) to possess for distribution; (c) import, transport, export; (d) store for profit. It would take matters

[47] Art 350a par. 4 CCNL also connects to specific *mens rea,* but follows the opposite route: providing or distributing potentially damaging data is exempted from liability when committed with the purpose of limiting damage. The text of Art. 138ab and 350a CCNL is provided after the references.
[48] Kamerstukken II 1990-91, 21 551, nr. 6, p. 29
[49] See on art. 46 CCNL Keulen 2009, 48-49 and on art 139d CCNL Ten Voorde 2010, aant.8.g.
[50] Koops 201, p. 18

beyond the scope of this general report to dig deeply into the meaning of these terms. For now the conclusion suffices that the legislation suffers from some inconsistencies. To my knowledge that has not led to great difficulties in practice.

The crime of grooming is also at the bottom-line a preparation for other crimes.[51] It is included in Art. 248e CCNL as an implementation of the Convention of Lanzarote (see chapter 1). The activity of the agent serves the purpose of either indecent acts with the person under 16 or to produce pornography in which this person is involved. To propose a meeting, using an automated device or communication service, with this person under 16 with the special intent to arrive at one of these activities is a crime, provided that acts have been shown that are destined to realize the meeting. As one can see, the construction contains an accumulation of *mens rea* elements: the verb "propose" already carries intent and in addition to that as special intent the law requires: the purpose of certain activity with a minor under 16. On top of that, in the appreciation of the acts destined to realize the meeting the intent of the agent also plays a part, as shown above when dealing with instruments for preparation. One could argue that the issue of voluntary retreat is at least partially dealt with in this provision. When after having conversed with the potential victim the agent does not pursue his intentions and abstains from actions to realize the meeting, no liability exists. To return in one's footsteps after such actions however does not have the same effect.

Chapter 5

Assistance and joint perpetration

Accessory perpetration, aiding, facilitation

Dutch law on perpetration by more than one person distinguishes in various constructs, such as incitement, joint perpetration, purely instrumental perpetration and facilitation/assistance. For this report is suffices to pay attention to joint perpetration and assistance, mentioned in Art. 47 and 48 CCNL.[52] In addition to that we will pay attention to some issues, special for the commission of crimes on the internet that are closely related to joint or accessory perpetration: the position of the internet service providers (ISP) and weblog monitors and the application of hyperlinks.

The general requirements for joint perpetration can be summarized as: intentional and close cooperation and joint execution. A wide diversity of activities' distribution between the participants can amount to joint execution. For a conviction the evidence must support all the elements of the relevant crime, but these may be distributed between the participants unevenly. The facilitation or assistance, mentioned in Art. 48 CCNL, refers to a lower level of involvement where the text of the code criminalizes the assistance by providing means, information or opportunity before the time of the actual commission and assistance at the time of the actual commission of the crime by someone else. Assistance to a crime the commission of which cannot be established in evidence is not punishable. The distinction between the two, joint perpetration or mere assistance, can be made by looking at the intent of the agents, the intensity of the joint operation and the share of the assistant in the execution activities. However, a grey area remains between the two, however relevant the categorization may be in terms of maximum penalty. Joint perpetrators risk the statutory maximum penalty of the crime, whereas assistance carries a maximum of two thirds of that maximum.

---

[51] De Hullu 2012, p. 405

[52] The text of Art. 47 and 48 CCNL is provided after the references.

The requirements for accessory perpetration, as summarized above, may lead to evidential hazards. All elements of the crime to which the perpetration is accessory, have to be proven and also *mens rea* in relation to all those elements.[53] To overcome these hazards the Criminal Code carries some special facilitation crimes. As was the case with preparation, the freedom to determine maximum penalty apart from regulation in General Part of Criminal Code was found to present an extra bonus of separate criminalization We go over a few examples. Assistance to the crime of false use of telecom services in Art. 326c CCNL by way of providing technical equipment would be almost impossible to prove, because the illicit activity with the delivered devices hardly ever sees the light of day. To prevent the immunity that may be the consequence for the provider of the devices the legislator adopted art 326c, par. 2 CCNL. The paragraph criminalizes forms of offering, possessing or producing an object or data, obviously designated to the commission of false use of telecom services.[54] In this form the assistance to the crime is hard to distinguish from the preparation of the same. The difference between Art. 139d par. 2 CCNL and Art. 326c par 2 CCNL is that the former requires an additional *mens rea* in the purpose to commit at the side of the agent, whereas the latter does not reach beyond the "obvious" designation. That might imply a more objective perspective.

Art. 350a, par. 3 CCNL and Art. 350b par. 2 CCNL also represent examples of accessory perpetration, especially the crimes with the *actus reus* "provide". The variety with the verb "distribute" bears more similarity with the preparatory crimes of Art. 139d par. 2 CCNL. The terminology is to provide "data designated to cause damage in an automated device", without the word "obviously". An extra *mens rea* requirement is left out as well (e.g. with the purpose of …) leading to the question whether and to what degree a subjective element still has to be proven under the phrases in the definition referring to the designation of the data.

Intermediaries: service providers and weblog monitors

The EC Directive on E-commerce brought about legislation in which the position of intermediaries was included. The member states were obliged to strike a delicate balance, because coming down too harshly on service providers would have adverse effects on this perfectly respectable and necessary line of business. One of the main goals of the Directive was to prevent proactive censoring and chilling effects on the free flow of information.[55]

The balance is expressed for the criminal law in Art. 54a CCNL.[56] In that provision the liability for intermediaries is lifted under some conditions. An intermediary can be held liable for content crimes, at least for the facilitation as covered by Art. 48 CCNL, where some forms of knowledge of the distribution of illegal content suffice to prove the necessary intent. Effectively that would imply a form of constant monitoring that leads to additional costs at the providers' side and to censoring. Art. 54a provides for exemption from prosecution after obeying a warrant from a prosecutor to take all reasonably possible steps to render the illegal content inaccessible. Refusing to obey establishes criminal liability for refusing an official warrant (Art. 184 CCNL) and in addition to that the accessory accountability for the content related crime remains. Even when the elements of accessory liability are not in

[53] See De Hullu 2012, p. 473-474, who also adds that a formal conviction of the principal is not required for a successful prosecution of the accessory.
[54] Interesting to note that the term "obviously" was withdrawn from art. 46 CCNL, because it caused some confusion in practice; Keulen 2009, p. 48
[55] Koops & De Roos 2007, p. 72
[56] The text of Art. 54a CCNL is provided after the references.

evidence, the refusal of the warrant constitutes a breach of Art. 184 CCNL. Fulfillment of all elements of assistance under Art. 48 CCNL (see above) is not incorporated in the validity test of the warrant. [57]

On the specific features of the liability for intermediaries there is not much case law. In particular the activity of more or less professional monitors and hotlines (www.meldpunt.nl; www.inhope.org) may lead to regular reporting of illegal content distribution, as a result of which the intermediary gains knowledge of the crimes to which they may be assisting. Does Art. 54a CCNL imply that prosecution without a prior warning is improper and that disobedience to the warrant of the prosecutor constitutes the necessary proof of intent?

Here we take a look at the case of Assen District Court 22-07-2008, LJN BD8451; quashed by Leeuwarden Appeal Court 20-04-2009, LJN BI1643 and BI1645 and retried by the Assen District Court 24-11-2009, LJN BK4226. On a website, hosted by a particular internet service provider company, allegations were accessible that amounted to the crime of slander. A warrant was issued to the service provider, but the necessary authorization from a judge to issue it had been denied. As a consequence of the lack of authorization the only warning on the table was an unofficial letter from the prosecution service. The provider did not remove or render inaccessible the information on the indicated website and was prosecuted primarily for joint perpetration of slander and subsidiarily for assistance to slander.

The District Court in its first judgment found that a valid warrant should be issued before the internet service provider could successfully be prosecuted for the continuous co-perpetration of slander on a website that it had hosted. In the case before it the court could not establish the warrant being issued validly, because the order from the prosecution service lacked the required authorization from a judge. The court therefore denied the right to prosecute and declared the prosecution inadmissible. The Appeal Court in the same case however found that the charges in the indictment demonstrated the prosecution not to aim at the involvement of the ISP company as an intermediary in terms of Art. 54a CCNL. According to the parliamentary documentation Art. 54a serves only a very limited category of involvement in the crimes as intermediary: mere conduit, caching and hosting. The indictment revealed the prosecution for actions falling outside the scope of Art. 54a, particularly the joint perpetration of slander being more than mere facilitation. For that reason the District Court erred in denying the right to prosecute where there is no preceding valid warrant in this case. The ISP's involvement in this case was the delivery of webhosting service to the person who distributed on a specific website slanderous allegations against a specifically identified person. Conclusively, the judgment of the District Court was quashed and the case was sent back to the same court.

That court then admitted the prosecution and subsequently found that there is not sufficient evidence to fulfill the requirements of joint perpetration. It acquitted accordingly, stating:

> *The ISP company had 30.000 clients. The activities of the company do not exceed the mere technical: the procurement of a reseller package from the owner of the server and the re-lease of parts of that package as websites to its clients. No actual involvement in any way of the ISP company in the content or design of the relevant website was shown*. (quote from the written judgment; my rewrite of the Dutch text; EFS)

[57] Kamerstukken II, 2001/02, 28197, nr. 3, p. 66. See for criticism on the regulation Koops & De Roos 2007, p. 75, pointing at the omission to give the warrant an explicit and clear statutory basis.

The indictment carried subsidiary charges, on which the court had to judge where it acquitted for the primary charges of joint perpetration. Subsidiarily the ISP company was charged with assisting the original slanderer by providing internet access to this person for his website, or by providing to internet users access to the slanderous site. This again raised the question of the application of Art. 54a CCNL, because in this charge the provider was prosecuted in his specific, limited capacity. In its observations the court quotes from the parliamentary documentation, where the text uses words that clearly state: it is the purpose to prevent prosecution of ISPs for aiding in the content crimes, unless a valid warrant under Art. 54a CCNL has been issued and ignored. The judicial authorization for the warrant is a crucial requirement, where the EC Directive on e-commerce explicitly mentioned the involvement of a judge as a safeguard against undue censoring. For these reasons the prosecution for the subsidiary charges of aiding in the commission of slander was inadmissible where there was no valid warrant.[58]

The position of the professional internet service providers will receive additional attention further down, where the code of conduct will be discussed under self regulation. We now move on to an issue that confronts us with related questions of criminal liability, the maintenance of weblogs and internet fora. The position of weblog and internet forum supervisors under the criminal law is relevant for content crimes and related crimes such as incitement to hatred and/or violence, slander, insult, threats. In a regular case the blogger places content (a post) on someone else's weblog, either in text or by way of a hyperlink[59] (see below for hyperlinks) and sometimes this content constitutes a crime. The liability of the blogger is easy to establish, easier than his identity, but what is the position of the weblog owner/supervisor. That person might be held to provide assistance to the commission of the crime by the blogger and found liable under Art. 48 CCNL or maybe even under Art. 47 CCNL for joint perpetration. The question however is whether one can constitute the necessary intent just by not monitoring? The answer concluded from the doctrine on intent is negative, because there is no proof of knowledge and will. But when someone else has notified the weblog owner/supervisor of the illegal content after a notification by another, the knowledge is there.

For joint perpetration a level of cooperation is required as *actus reus*, that usually will not be fulfilled. The Amsterdam District Court 01-10-2009, LJN BK1571, observed that leaving and not removing a post on the weblog is not sufficient to meet the requirements for joint perpetration, neither *actus reus* nor *mens rea*. A lower level of involvement, the assistance under Art. 48 CCNL, was relevant in the case of Rotterdam District Court 02-02-2009, LJN BH1711.The court convicted a webmaster for assisting the commission of insult and incitement. The defendant had facilitated that the illicit texts were published, since he has created the relevant site, has paid for its continuance and has omitted to erase the texts from the forum, contrary to what he ought to have done on the basis of his authority on the forum as administrator/moderator. In this way the intent of the defendant was aimed at insulting and incitement to hatred, discrimination and violence against Jews and Muslims, as well as on the publication thereof. (my rewrite of the Dutch text; EFS) Clearly weblog moderators/owners have a duty of care to supervise and remove as soon after the discovery as possible, in order to prevent liability for assistance ex Art. 48 CCNL.

The issue of intent was on the table in Den Haag District Court 12-05-2011, LJN BQ4468. The court acquitted because the evidence did not support the web forum owner to have seen the illicit content on the forum. The

[58] An appeal disposal of this second judgment could not be traced; last search on www.rechtspraak.nl dated 04-09-2012.
[59] See for a recent example of threats by way of linking to footage on YouTube: Middelburg District Court 26-07-2012, LJN BX2749.

Amsterdam District Court 01-10-2009, LJN BK1571, concluded in the same vein. With no proof of knowledge, being a moderator in itself does not suffice to establish responsibility (and criminal liability).

To proof of knowledge a concrete complaint e.g. of lobby organizations or victims to the weblog's moderator assists. The liability appears to lean on: willingly and knowingly leaving and not removing posts with illegal content, although the agent has authority to do so. In my observation that is a doctrinal *corpus alienum*. The criminal assistance is rendered by a combination of providing the instrument to commission and *mens rea* arising from omission after the fact. Where the phrasing of Art. 48 CCNL only refers to facilitation preceding or during the commission by the principal, it seems to be against the text of the criminal code to attach such weight to circumstances after the commission by the principal. On top of that, a general principle in Dutch law is that participation after the fact does not amount to criminal liability.[60]

Hyperlinks

Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. With this quote from the Explanatory Report to the Cybercrime Convention[61] I introduce the last separate issue in this chapter: hyperlinks. That refers to the opportunity to create an easy connection from one source of information to another by showing/typing a URL. Clearly the insertion of other content in a text/information by way of typing a link and then distributing that text/ information also means distributing the content to which the link relates.[62] However, to distinguish between conscious hyperlinkers and other distributors of information is necessary to exculpate especially search engines.[63] Those may otherwise be held liable for at least assisting in the distribution of illegal content anytime such content is referred to by links on the results page.

In Rotterdam District Court 30-10-2007, LJN BB7174, the defendant was charged with the crime of incitement by linking in her texts on the internet (a.o. in an MSN conversation) to inciting text elsewhere. The court observed that is was not the intention of the legislator to identify all links with the underlying illegal content, because that would categorize all links on the search engine results pages to illegal content under the criminal law. Whether or not the hyperlinker to illegal content shares in the liability of the producer of the content depends on the circumstances of the case. The court then continues to observe the specific features of the case and refers e.g. to the knowledge the defendant must have had of the nature of the content.

As more or less implicit in the observations of the Rotterdam District Court, the *mens rea* requirement serves to determine liability appropriately for individuals. The matter is not easily resolved for search engines when they distribute links on the results page. The general intent under Dutch law is rather indiscrete where is comprises the

---

[60] De Hullu 2012, p. 417-418 and 437, who discusses the assumption that the end of the commission of the crime can always be clearly established.

[61] Explanatory Report 2001, 72

[62] See the identification of URLs with images in Amsterdam District Court 23-07-2012, LJN BX2325, a child pornography case with charges of distribution and possession. Sending the URLs in an active chat program to a specific addressee with the sole purpose of sharing the underlying image can be qualified as distribution, according to the court. Storage of the URLs in the chatlog, preserved by the defendant, qualifies as possession.

[63] See Kentgens 2008

conditional intent (*dolus eventualis*). It is easy to prove the intent to distribute. That is what search engines do: find and provide information. But Dutch law on joint perpetration or assistance also requires intent on the commission of the crime by another, as we have seen at the beginning of this chapter. A certain knowledge of the commission and an element of willing need to be established, but can under certain circumstances be concluded from general knowledge of the chances and omission to check them. How much checking suffices to avoid criminal liability depends on what we find reasonable as balanced level of care to be expected from the providers of these very useful services.

The accentuation of the intent requirement raises the question of negligent assistance. Under Dutch law negligent assisting is not a crime in general. Negligent distribution is only specially criminalized for data destined to cause damage in an automated device; Art. 350b CCNL. Under the negligence doctrine one can easily connect with reasonable duties of care. The negligent version of malware distribution might only apply to professionals and not to ordinary end users from whom we may not expect the required level of security.[64] Whether or not the clear demarcation between professionals and end users holds, depends on the appreciation of new roll models in the Web 2.0 and is food for debate.

Two final remarks on duties of care follow here before we move on to the next chapter. In the quest for internet security we can witness that some elements of the crimes presuppose care at the side of the victim. An example is the duty to modify the web browser in order to avoid automatic penetrations of a system to leave cookies or bots. That penetration is not in itself without right, because the user (or webmaster) can adapt the settings.[65] We see a duty of care at the other side of the relation agent – victim. A previous version of Art. 138ab CCNL (at that time Art. 138a) also related to duties at the side of the victim. The *actus reus* implied security actions on the side of the victim. This was withdrawn in the process of implementing the Cybercrime Convention, Art. 2, in 2006.[66] The second remark concerns the duty to protect databases containing personal data under the Personal Data Protection Act. As the Commission on Computer Crime already stated, that is a duty too general to enforce by way of the criminal law.[67] We will briefly return to database protection duties and data leaks in the next chapter, dedicated to alternatives to criminal law enforcement.

Chapter 6

Alternatives to criminal law enforcement

The various alternatives will be briefly indicated here as an overview of the options. An in-depth and complete report in these would exceed the assignment. We will look at some examples of administrative law, civil law and separately to the self regulation, so popular among policy makers in the Netherlands (and Europe).

Administrative law

The distribution of spam is subsumed under administrative law enforcement by 11.7 Telecom Act. Punitive sanctions can be imposed by the Independent Post and Telecom Authority (OPTA), in 2013 to be absorbed in a more

[64] Koops & De Roos 2007. p. 43
[65] Explanatory Report 2001, 48
[66] See Koops 2010, p. 7
[67] Commission Report 1987, p. 54

comprehensive supervisor: Authority Consumer and Market. The OPTA maintains a web address for receiving complaints, www.spamklacht.nl, on the basis of which it can deploy its investigative power. In Art. 15.4 Telecom Act we find the penalties: a maximum fine of € 450000. The individual fine decision of the OPTA expresses seriousness and duration and the culpability. Taken altogether this enforcement modus can be appreciated as a type of pseudo criminal law enforcement. Sanctions are punitive and personalized to the seriousness of the offence. It is doubtful whether this really counts as an alternative or as mere change of labels.

Data leakage/breach, that is the penetration and/or loss of data from a protected database, is object of recent and expected legislation, national and European, that address either the person or organization responsible for a personal data registration, providers of public telecom services or certain financial service providers.[68] Those are subjected to duties to report data breaches in their systems to a relevant authority, which duty is backed by enforcement instruments under administrative law, a fine in particular. Various digital front windows are available to report the events. See www.meldplichttelecomwet.nl and www.cpbweb.nl/pages/ind_melden.aspx

Art. 65 Personal Data Protection Act provides the Personal Data Protection Authority with an intervention competency under administrative law for cases where those governed by the Act (especially organizations/enterprises) prove persistent in violating the Act. The Authority can impose an order with the opportunity to act on behalf of the addressee and on his costs. This power might be deployed in case of continuous ignoring the duty to safeguard network security for all owners of personal data files; Art. 13 of the Act.

Civil law

Copyrights piracy is a first example of breaches of the law in cyberspace for which civil law is the important instrument. Another will be dealt with under self regulation. Dutch copyright law is for the main part enforced by way of civil suits from or on behalf of the owner[69]. We can witness an active role of BREIN Foundation, who acts on behalf of authors, artists, publishers and producers in the entertainment industry. This foundation already succeeded in cases against internet service providers to block the Pirate Bay site that offered downloads of music, software, movies and games. Obviously private persons do not avail of the powers for investigation that authorities have. Support for civil suits comes from Art. 8 Directive 2004/48/EC of 29-04-2004, providing for an injunction to obtain from an ISP details of person to which IP address is connected. With that information one comes a step closer to the person or organization one has to sue in order to protect intellectual property. The Dutch Supreme Court has given some guidance as to the cases in which the courts may issue such an injunction; see Dutch Supreme Court 25-11-2005, LJN AU4019 (Lycos/Pessers).

Self regulation

Self regulation is presented here apart form civil law and as an alternative to criminal law enforcement. However, we must realize that in self regulation contract law plays an important part. Additionally, as we will see, the criminal law enforcement is not at all strictly separated from self regulatory instruments. Criminal law remains present as a fall back option when the other instruments do not bring about the desired result.

---

[68] Van der Jagt 2012 referring a.o. to the Personal Data Protection Act, the Telecom Act, the Act on Financial Supervision and proposals in the EU context.
[69] Koops 2010, p. 18

The Notice-and-Take-Down (NTD) code of conduct of ISP sector is a strong example of self regulatory activity. It is a regulation of proper conduct, that was negotiated under the umbrella of the National Infrastructure Cybercrime and published by the sector organization ISPConnect. This branch organization maintains a quality hallmark. Every service provider who wants to maintain that ISPConnect Hallmark has to accept the code of conduct as a format for dealing with a client distributing illegal information.[70] In the code the following scenario is described. When a person or an institution encounters illicit activity or information on a website, he can report to the service provider. The complaint is then sent to the customer, who has two working days for a reply, apart from emergencies. In case there is no reply or the reply is not satisfactory the ISP will decide on taking down the site or removing the illicit information. The ISP can also opt for a complaint to the police in case of a crime. This sequence of actions should be covered for all customers in the general contract conditions, a model of which is presented in the code of conduct. The provision to be enclosed in every contract discloses the test that the ISP will apply on a complaint.

> *Client will not publish or provide through the ISP intermediary information that constitutes a violation of Dutch law. That includes in particular, but not exclusively: information provided without permission of the copyright holder, information that is slanderous, threatening, insulting, racist, inciting hatred or discrimination, information containing child pornography, information violating the privacy of others or that amounts to a form of stalking. Whether this information is provided or published directly or by hyperlink, torrent or other reference to sites of third persons anywhere in the world is irrelevant, even when the information might be in accordance with the law of that foreign jurisdiction.* (my translation; EFS)

This is an example where the sector joined forces to combat illicit use of the services on a voluntary basis. For cases where that would not work the government proposed a takedown order to be inserted in the Code of Criminal Procedure, but this s not yet enacted.[71] For websites hosted outside the country the takedown is also organized on a voluntary basis. An agreement between the national police and the ISP sector has been reached on child porn sites, to the effect that the ISPs will block those websites that are blacklisted.[72]

When we connect this complaints practice with the earlier parts on the possible liability of the service provider, it will be clear that a users' complaint itself does not constitute a valid warrant in terms of Art. 54a CCNL. In addition to that, when a complaint does not result in voluntarily taking down the allegedly illicit website or removing the content, esp. when both customer and ISP/intermediary resist the opinion that a violation of Dutch law occurred, the prosecution of the ISP for assistance still has to be preceded by the warrant mentioned in Art. 54a CCNL. For the awareness at the side of the ISP that he may assist in distributing illicit content this warrant is irrelevant. But, as we can learn from the observations in the Assen case above, charging the ISP after a valid warrant will result in the court to investigate the involvement of the ISP. As a result of the complaint under the NTD code of conduct the ISP has gained knowledge of the presence of the content in his service pack and consciously left it there.[73] Lack of intent on

[70] See www.ispconnectkeurmerk.nl

[71] See B.J. Koops, Tijd voor computercriminaliteit III, 85 *Nederlands Juristenblad,* 2010, p. 2461 - 2466

[72] See further Koops 2010, p. 32

[73] From the parliamentary documents we can learn that the capability of the intermediary ISP to take down or remove is presupposed. When not reasonably able to obey the take-down warrant ex art. 54a, the intermediary can either plead lack of

the ISP side will then be hard to state convincingly. As a result there is an incentive for the ISP to move on the safe side and implement stricter self censoring than necessary. The obvious down side of that is that complainants will be in charge. As soon as there is a complaint (in strong terms and with some publicity) the ISP may lean towards taking down in order to avoid criminal prosecution himself. This presupposes a decent approach of "professional" complainants, such as anti discrimination lobbyists. Under Dutch criminal procedure a correction could be found in a wise prosecution policy, which in turn is under review of the Appeal Court on a complaint against the decision not to proceed. But, decisions to prosecute or not are many steps further down the line of law enforcement whereas wisdom is called for in the early stage of discovery by complainant and service provider.

Chapter 7

Miscellaneous and final observations

Some topics from the questionnaire are left out so far, particularly items F and G on the list. The main reason is, that those items do not subsume under criminal law. The obligations of internet service providers, for example the user data retention duties[74], are incorporated in the Telecom Act and are enforced under administrative law. The duties to inform the authorities and deliver encryption codes is regulated in criminal procedure, as far as it concerns a criminal investigation. They will surely receive attention in section III reports. To note just one point here: under the Criminal Procedure Code the suspect cannot be obliged to furnish information, since that type of cooperation was found to be contrary to the safeguard against self-incrimination (Art. 6 ECHR).

As to the application of Dutch substantive criminal law on action abroad, the code does not contain a special arrangement for cyber crimes other than mentioned below. The Cybercrime Convention (Art. 22) provided for a jurisdiction harmonization that easily connected with what was already present in title I of Book 1 of the Criminal Code. Dutch criminal law applies on cyber crime, committed inside the national territory and on board of ships or aircrafts registered in the Netherlands. In addition it applies to the action of Dutch nationals who committed the crime abroad. Art. 5 CCNL requires a double incrimination: both in the Netherlands and in the country of the *locus delicti* (Art. 5, par. 1 sub 2 CCNL). However, for many cyber offences this is not required. The code exempts in sub 4 of the same paragraph of Art. 5 the offences that were introduced as implementation of the Cybercrime Convention. Sub 3 of the same article of the Code introduces the same exemption for sex crimes with children, committed abroad, thereby including child porn cyber crimes and grooming. For those the double incrimination is not an issue anymore.

To conclude this report I can underline what Koops already stated[75], that in Dutch criminal law one encounters many results of international harmonization that have not disrupted the system as a whole. The changes over the course of time have been substantial, but they have been absorbed quite easily. The flexibility of case law and doctrine, for example on *mens rea* has proven its value to that end. For the future of substantive criminal law we might expect an exacerbation of duties of intermediaries, where the climate at the time is quite repressive, the public outrage on child abuse unlimited and the frustration of not being able to operate effectively against cyber criminals outside the borders

---

actus reus or raise a defense of duress (*force major*). The minister refers to mere conduit as an example of incapability; Kamerstukken II, 2001/02, 28197, nr. 3, p. 65

[74] As implementation of the Data Retention Directive 2006/24/EC of 15-03-2006 OJ L 105/54 (13.4.2006)

[75] Koops 2010, p. 34

is mounting. At the moment the balance sways to more supervision and control and it is hard to predict when the scales will return to free flow of information etcetera as basic principles of the rule of law.[76]

References

Commission Report 1987

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

De Hullu 2012

De Hullu, J, Materieel Strafrecht, Deventer: Kluwer, 2012 (5th ed.)

Explanatory Report 2001

Convention on Cybercrime Explanatory Report ETS 185, available on http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (accessed Sept. 2012)

Van der Jagt 2012

Jagt, Frederike van der, Iets te melden. De diverse datalekmeldplichten in kaart gebracht, *Nederlands Juristenblad* 22-06-2012, nr. 25, 1713-1719

Kentgens 2008

Kentgens, A.G.H., Verspreiden in het digitale tijdperk, *Nederlands Juristenblad* 2008, p. 1984-1989

Kentgens & Stamhuis 2012

Kentgens, Arno & Evert Stamhuis, The development of international legal instruments for promoting cyber safety, in E.R. Leukfelt & W.H. Stol (eds.) *Cyber Safety: an Introduction*, The Hague: Eleven International Publishers 2012, p. 57-72

Keulen 2009

Keulen, B.F., Grenzen aan de strafbare voorbereiding, in E. Gritter (ed.) *Opstellen Materieel Strafrecht*, Nijmegen: Ars Aequi Libri 2009, p. 45-76

Koops & De Roos 2007

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

Koops 2010

Koops, Bert-Jaap, *Cybercrime Legislation in the Netherlands*, *Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes',* available at http://ssrn.com/abstract=1633958

[76] See Koops & De Roos 2007, p. 72, quoting from the minister of justice in 2001.

Van der Meulen en Koops 2012

Meulen, Nicole van der & Bert-Jaap Koops, Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude, *Nederlands Juristenblad* 22-06-2012, nr. 25, p. 1706-1712,

Ten Voorde 2010

Voorde, J.M. ten, Aantekeningen op Art. 139d, in C.P.M. Cleiren & M.J.M. Verpalen, Tekst & Commentaar Strafrecht, Deventer: Kluwer 2010

Some articles of the Criminal Code of the Netherlands

(unofficial translation)

Art. 45 CCNL

(1) Attempt to a crime is punishable, when the intention of the perpetrator is expressed in the actual commencement of the execution of that intention.

Art. 46 CCNL

(1) Preparation to a crime on which the statutory description carries a maximum penalty of eight years and over, is punishable when the perpetrator intentionally obtains, produces, imports, transports, exports or possesses objects, materials, information carriers, spaces or means of transport, destined to the commission of that crime.

Art. 47 CCNL

(1) As perpetrators of a punishable act are punished:

1* those who commit, have commit or jointly commit that act

2* ....

Art. 48 CCNL

As assistants to a crime are punished

1* those who intentionally assist in the commission of the crime;

2* those who intentionally provide opportunity, means or information to the commission of the crime.

Art. 54a CCNL

An intermediary, who provides the transmission or storage of data coming from someone else as a telecommunication service, will not be prosecuted as such if he obeys a warrant from a prosecutor, issued after authorization from an investigating judge upon request of the prosecutor, to take all measures that reasonably can be required from him to render those data inaccessible.

Art. 138ab CCNL

(1) A person who intentionally and unlawfully intrudes into an automated device or part thereof is guilty of computer intrusion and liable to a term of imprisonment of not more than one year or a fine of the fourth category. Intrusion includes access:

a. by breaching a security device,
b. by a technical operation,

c. with the help of false signals or a false key, or
d. by assuming a false capacity.

(2) Computer intrusion is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently, for his own use or for that of another, copies, taps or records the data stored, processed or transferred in the automated device in which he has intruded.

(3) Computer intrusion committed through a public telecommunication facility is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently

a. uses processing capacity of an automated device with the purpose of obtaining unlawful benefit for himself or for another person;
b. through the automated device into which he has intruded gains access to the automated device of a third person.

Art. 138b CCNL

A person who intentionally and unlawfully obstructs the access to or the use of an automated device by offering or sending data to that device is liable to a term of imprisonment of not more than one year or a fine of the fourth category.

Art. 350a CCNL

(1) A person who intentionally and unlawfully alters, erases, renders useless or inaccessible data stored, processed or transferred by means of an automated device or by telecommunication, or adds other data thereto, is liable to a term of imprisonment of not more than two years or a fine of the fourth category.
(2) A person who commits the offence specified in section 1 after having unlawfully intruded, through a public telecommunication facility, into an automated device, and there causes serious damage with respect to such data, is liable to a term of imprisonment of not more than four years or a fine of the fourth category.
(3) A person who intentionally and unlawfully provides or disseminates data designated to cause damage in an automated device, is liable to a term of imprisonment of not more than four years or a fine of the fifth category.
(4) A person who commits the act specified in section 3 with the object of limiting the damage resulting from such data is not criminally liable.

Art. 350b CCNL

(1) A person who by negligence is responsible for unlawfully altering, erasing or rendering useless or inaccessible data stored, processed or transferred by means of an automated device or by telecommunication, or for adding other data thereto, is liable to a term of imprisonment or detention of not more than one month or a fine of the second category, where serious damage with respect to such data is thereby caused.
(2) A person who by negligence is responsible for unlawfully providing or disseminating data intended to cause damage in an automated device is liable to a term of imprisonment or detention of not more than one month or a fine of the second category.