Criminal law on cyber crime in the Netherlands

AIDP Country Report Section 4 *

***Mr. A.M.G. Smit*[1]**

a.m.smit@rechtspraak.nl

January 2013

[1] Judge at the Court of Appeal in the Den Bosch (Netherlands). The author is much indebted to Barend van Wonderen LLM MA who assisted her with the text of the rapport and translations. The views expressed in this report are of the author only.

* 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.

Table of contents

Chapter 1 Introduction

Since the invention of computers, crime by means of computer systems is a dominant theme in futuristic film scenario's. Even the last James Bond movie, Skyfall, is about a criminal mastermind who gains money and power through hacking governmental computer systems. In spite of these fantasies cybercrime is a serious threat for our economy and the safety of society. An indication of the scale of cyber crime offences provides the following headline published on the website of the Dutch Bank Association: 'Fraud with internet banking rises with 14% in the first two quarters'.[2] The short article, which is based on information of the Dutch Bank Association, puts forward that the financial damage due to fraud with internet banking has augmented from 23,8 million Euro in the last two quarters of 2011 to 27,3 million Euro in the first two quarters of 2012. The article also states that the financial damage caused by 'skimming' was 18,2 million Euro in the first two quarters of 2012. In 2011 the known financial damage for banks regarding cyber crime amounted to 92,1 million Euro. These are substantial expenses. However, national governments lose vastly more in consequence of illegal lotteries and gambling games on the internet. The Dutch Scientific Research and Documentation Centre has estimated that in the Netherlands 180 million Euro was spent in illegal gambling activities.[3] Some other figures about cybercrime can be found on the following link: http://www.youtube.com/watch?v=PIELVMQhvXc.
Moreover, today's internet and communication technology allows for new possibilities to commit old offences. This is the case with Missing Trader Fraud or carousel fraud. In carousel fraud schemes certain goods are transferred several times from one enterprise to another foreign enterprise, because these kind of exports are Value Added Tax free. However, the final undertaking in the chain, which would bring the products on the market and would pay the VAT, goes bankrupt. For this reason the goods can be delivered without paying the VAT to the concerning government. Prior to the expansion of Information and Communication Technology (ICT), the goods would be physically transported across Europe before arriving closely to the enterprise from which the goods originally took off. Through the

[2] Dutch association of banks, 26 September 2012, 'Fraud with internetbanking increases with 14% in the First semester.', available at: http://www.nvb.nl/nieuws/2012/687/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14.html [Accessed on 9 January 2013].

[3] National Research and Documentation Centre, *A smart gamble? Research on the ways to determine the nature and volume of illegal gambling in the Netherlands*, 18 January 2008, available at: http://www.wodc.nl/onderzoeksdatabase/1575a-aard-en-omvang-illegale-kansspelen-in-nederland-inventarisatiefase.aspx?nav=ra&l=wetgeving_en_beleid&l=wet_op_de_kansspelen [Accessed on 9 January 2013].

utilisation of the internet goods are only transferred digitally. An example of this kind of fraud in the digital age occurs in the trade of emission rights. The internet allows goods which only exist in the digital cloud to pass several companies in different continents and end up at a short-lived undertaking which maybe existed only digitally. Emission fraud amounted to hundreds of millions of euros and these kinds of schemes were difficult to detect.[4] (Note: due to recent legislative adjustments this kind of emission fraud is no longer possible). Digital fraud schemes are difficult to detect by the tax authorities, and it is even more difficult to detect and prosecute the people behind these schemes.

The difficulty of tracing people behind digital activities touches upon another important aspect of cybercrime, namely the probability of detection. Or rather the improbability of detection. Cybercrime offences are committed without any climbing over fences, balaclavas, or angry dogs and property owners. There is only somewhere in the world a computer, which is controlled by a particular person, from which thousands of emails are sent asking for personal banking data (a form of phishing). If one in thousand people respond, it is possible to steal more from these accounts than one can possibly obtain from a night of breaking into houses, without being disposed to the risks of a burglar. The seizing of such information through hacking or viruses is likely to cause incalculable damage. In such cases it is highly difficult to detect the perpetrator(s). The computers can be found and the money can be followed, though it is very difficult to get a hold on those behind the IP addresses and bank accounts. There are no other possible traces, no accidental trespassers, no DNA or fingerprints. It may even be possible that the offenders are in a country with which the Netherlands do not have an extradition treaty.

To give another example of an international cyber crime offence a video link is attached regarding a so-called botnet: http://nos.nl/artikel/193720-crimineel-computernetwerk-opgerold.html**.** The botnet works as follows. A programme 'bot' is inserted in a computer, which programme can be controlled via the internet from a central computer. While the Netherlands have a good ICT infrastructure, the Netherlands is a good location to operate from in a case like this. In the video attached it was an Armenian national who operated from the Netherlands.

Because national territories are of little importance to cyber crime offenders, it is essential for the prosecution of these crimes that national governments cooperate. Without international

[4] http://www.bbc.co.uk/news/business-20695042 [Accessed on 9 January 2013]

cooperation it would be impossible to find and institute proceedings against those responsible. Part D of this section deals with international cooperation aspects.
Today, Information and Communication Technology have an enormous role in our every day lives due to the continuous developments in this field. Not only in our private lives, but all the more in our professional activities ICT has become indispensable. In the Netherlands, for instance, all medical dossiers are being digitalised. These kinds of information systems contain very sensitive, private information. Therefore, the information and the system as such are of interest to criminals. Persons may illegally gain access to personal files even if the government acts as reliably as possible. There may be leaks due to third parties who during the maintenance of the system install possibilities to enter the network. Furthermore, viruses, which give access to the computer and the network, can be installed on new computers.[5] The persons acquainted with these so-called bots may be able to enter the network, follow our actions, inform themselves about personal information of others, and maybe even change the data. Can intrusions in large ICT systems be avoided by means of security measures and back-ups? This is a question which can be posed, but not answered.
Moreover, the internet is everywhere. Almost all communication in our daily work makes use of the internet, as work mail, home working systems, and skype. A country would be severely damaged if the internet providers are to be shut off. Recently, providers were closed down in Syria, where it was unclear if this was an accident or an intentional act of the Assad regime. In analogy one wonders if it would be possible for terrorist organisations to turn off the internet.

In answering the questionnaire of this Section 4 of the AIDP Country Report, I made use of the broad and narrow definition of cybercrime. For these definitions I refer to the analysis of Prof. dr. Evert F. Stamhuis "Criminal law on cybercrime in the Netherlands; general report AIDP country report Section I.[6]" The narrow definition of cybercrime refers to crimes in which ICT systems are the target. These are 'new' crimes using new tools. For these crimes new criminal offences are included in the penal code. For example 'hacking' is made liable to punishment. Cybercrime in the broad sense refers to crimes which make use or have something to do with ICT. The common denominator of narrow and broad cybercrimes is the

[5] In September 2012 Microsoft released a statement with regards to previous insecurities of botnets, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx [Accessed on 10 January 2013].

[6] Chapter 2, p. 5 - 11

use of computer systems, networks and data. Cybercrime may not only refer to crimes in which computer systems were used, but to ‘old crimes’ as well, such as theft or racketing. In this cases ‘old crimes’ are committed with new tools. In this report the broad definition of cybercrime is used.

Chapter 2 Jurisdiction issues

1. How does your country locate the place of the commission of a crime in cyberspace?

In answering this question about the place of crime in cyberspace one first has to reflect on the crimes which can be committed in cyberspace. An example of such a crime is offending a person and blasphemy. Someone puts a text on an internet site which according to the standards of society has a considerable insulting effect. Another example is the circulation of child pornography on a website of the World Wide Web. Other offences may concern stirring up hatred.[7]

The Articles 2 – 7 CCNL contain provisions on the applicability of Dutch criminal law. Art. 2 of the Criminal Code of the Netherlands (CCNL) provides that the Netherlands has jurisdiction in case the offence is committed in the Netherlands. In answering this question, Dutch jurisprudence gives further guidance on defining the *locus delicti*.

According to Dutch jurisprudence a crime can be committed on several places. In ranking the first place where a crime is committed is the place where the perpetrator acted (the doctrine of the bodily conduct). A crime is also committed at the place where the instrument was used (the doctrine of the instrument). The third place of a crime is the place where the effects of the crime occur (the doctrine of the result). The result is that a crime can be committed on several places (the ubiquity doctrine).

In consequence, the determination of the place where the crime was committed does not pose jurisdictional issues in Dutch law in cybercrime cases. The location from which the perpetrator undertook his actions, as well as the place(s) where these actions have their effects, and also the place where the used instruments have their effect, are seen as locations where the offence took place. Therefore, issues regarding jurisdiction and the location of the offence in cyber crime cases do rarely get attention in Dutch criminal proceedings.

One example of a case in which the counsel of the defence put forward that the proceedings were inadmissible, because the Public Prosecutor had no jurisdiction occurred in a judgement of the Court of Breda.[8] This case regarded a Dutch national who was suspected to have posted certain messages at an American website. The defence argued that in line with the doctrine of

[7] Art. 266 CCNL, deformation, Art. 147 CCNL, blasphemy, Art. 240a CCNL child pornography, Art. 137c CCNL stirring up hatred.

[8] Judgement of the Court of Breda of 9 November 2011, LJN BO 3363. (Case law is available in Dutch at http://www.rechtspraak.nl, indicated with reference numbers LJN).

the instrument the offence was committed in the United States, as the website was based in that country. In its verdict the Court made clear that the place of the crime is not only determined on the basis of the doctrine of the instrument. According to the Court the offence was committed in the Netherlands as well, in line with the doctrine of the bodily conduct, while the messages were sent from a computer inside the Netherlands. In addition, in line with the doctrine of the result, the effects of the offence could be considered to be situated in the Netherlands, because the threats posted on the website were directed at schools in the surroundings of Breda. The Court ruled that both the Netherlands and the United States were to be considered *locus delicti*. Henceforth, the Court dismissed the argument of the defence regarding jurisdiction.

In relation to jurisdiction, the Supreme Court in a decision of 30 September 1997 considered that: "if apart from places "in" also places "outside" the Netherlands are to be considered as places where a crime is committed, the crime may under the law of the Netherlands be prosecuted in the Netherlands (Art. 2 CCNL)." [9] Therefore, if the state has jurisdiction, the prosecution in the Netherlands may also regard elements of the offence which were manifested abroad.[10]

As put forward earlier, the place of the crime is also the place where the consequences of the criminalised behaviour take place. With regard to a crime which is committed in cyberspace, the results of the crime only exist if a computer is connected to the crime and files are downloaded or viewed.

An existing question for practitioners is whether the mere act of putting certain data on an internet site already constitutes a crime, or only if this website is visited by others who thereby gain access to the data. Would a person be punishable who puts child pornography on a website which remains unvisited? In case someone puts this kind of content on an internet site, the individual involved would of course already commit a crime by being in the possession of child pornography. The question is whether this act may be perceived to amount to spreading the pornographic content? (The spreading of child pornography is as a separate crime punishable according to Art. 273 f CCNL.) Or is the crime of spreading child pornography only committed if people take cognizance of the pictures?

If people take notice of the pictures, the crime of spreading child pornography is not only committed on the spot where the pictures are put on the internet but also where people have seen the pictures. The internet can be seen as the instrument with the help of which the

[9] Judgment of the Supreme Court, 30 September 1997. NJ 1998, 117

[10] Judgment of the Supreme Court, 2 February 2010, LJN BK 6328.

pictures are spread. The instrument has taken effect on the place where the pictures are viewed.
The same can be said about hate speeches on the internet; speeches which have the intent to activate people to committing violence. Is this crime already committed by putting the words on the internet, or only in case the message reaches the people for whom it is written? In practice, the police predominantly starts an investigation after people have filed a complaint regarding particular content on the internet. In general it can be said that, next to the place where the suspect has put the data on the internet, also the place or places where the people have taken notice of the data on the internet can be considered as *locus delicti*.
Crimes which can only be prosecuted after a complaint by a victim are special in this regard. An example for this is offending Art. 266 CCNL, or if it concerns a governmental employee doing his duty: Art. 267 CCNL. In such cases the prosecutor can only start a prosecution after a complaint by the offended person. Therefore, the place at which the offender has put the data on the internet is *locus delicti* as well as the place where the victim was informed about the insult.
The place of commission of a crime committed in cyberspace does not pose a problem. There is no negative jurisdiction problem on this issue. It is rather a problem that a crime can be committed on several places. In case someone puts hate speeches on the internet it may be the case that this data are read on a lot of places in the world. In consequence many states could start a prosecution.

b. Does your national law consider it necessary and possible to locate the place where information and evidence is held.

To identify the place where the crime is committed it is of no importance where the evidence of that crime is stored. The evidence may be required by the police from the internet or obtained as a result of a search in a computer where the material is stored. Considering procedures of investigation it can be of great importance where the information is held, though this is irrelevant for jurisdictional issues.

2. Can cyber crime do without a determination of the *locus delicti* in your criminal justice system? Why not?

A cybercrime offence needs a *locus delicti* in the Dutch procedural system. On the basis of Art. 261 Code of Criminal Procedure of the Netherlands (CCPNL) the *locus delicti* of the crime must be mentioned in a warrant. In the Dutch system, the *locus delicti* does not have to be stated very precisely. The *locus delicti* "in the Netherlands" may be sufficient. The verdict of the Court of Assen of July 2012 is a concrete example of this.[11]
On the basis of the law, the determination of the *locus delicti* is imperative. If computer equipment is used, it is often very difficult to investigate where the information is put "in the cloud". Furthermore this information can be reached from everywhere in the world In such cases the charge may suffice with a description such as 'in the Netherlands' or 'in Belgium'. The question is whether in the future the determination of the *locus delicti* in cybercrime cases may perhaps be omitted while it has no added value.

3. Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc.? If your state does not have jurisdiction over such offences, is that considered as a problem.

An overview of cybercrime offences is the following: (this overview is derived from the report of Prof. dr. Evert F. Stamhuis "Criminal law on cybercrime in the Netherlands; general report AIDP country report Section I."):

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)	
(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

[11] Court of Assen, 7 July 2012, LJN BX 0155.

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; 161sexies, par. 2

The Netherlands has jurisdiction over these offences. In general, the jurisdictional basis is to be found in the Articles 2 – 8 CCNL. A special arrangement for cybercrime offences was not considered necessary. The principle of territoriality is laid down in Article 2 CCNL. If a crime is committed on Dutch territory, the Dutch law is applicable. Above, I have already discussed Dutch interpretation and jurisprudence according to the *locus delicti*. The Dutch law also applies to cybercrimes committed on board of ships or aircrafts registered in the Netherlands (Art. 3 CCNL). Cybercrime acts committed on board of a ship or of an aircraft are punishable in the Netherlands even if this ship or aircraft is on the open sea. The active nationality principle is laid down in Art. 5 CCNL. According to Art. 5 the Netherlands has jurisdiction over its own nationals in case they commit (cyber)crimes outside Dutch territory. This can either be a crime especially designated in Art. 5, or an offence that constitutes a crime under Dutch criminal law and is punishable under the law of the country where the offence is committed. The designated crimes are (among others) infringements on the security of the Dutch state and on royal dignity. Hence, in general, the application of Art. 5 CCNL requires dual incrimination. The acts should be punishable both in the Netherlands and in the country of the *locus delicti*. Regarding cybercrime offences an exception to this rule is made in Art. 5

par 1, subsection 4.[12] This subsection was added by the Computer Crime II Act (*Wet computercriminaliteit II*) of 2006.[13] According to the Explanatory Memorandum added to this amendment, Art. 5 CCCN is a result of the obligation laid down in Art. 22 of the Cybercrime Treaty.[14] Some scholars have argued that the text of subsection 5 goes beyond what is required by Art. 22 of the Cybercrime Convention, while it annuls the precondition of dual incrimination for Dutch nationals who act from abroad.[15] Art. 22 subsection d. of the Cybercrime Convention obliges the Parties of the Convention to establish jurisdiction on the basis of the facts "by one of its nationals, if the offence is punishable under the criminal law where it was committed, or if the offence is committed outside the territorial jurisdiction of any State". To comply with the obligation it would be required to determine jurisdiction regarding offences which are committed "outside the jurisdiction of any state". As an example, the Explanatory Memorandum mentions offences committed on a vessel or airplane which has not been registered in any country.[16] In case a Dutch national commits a (cyber)crime in a country where his behavior is forbidden by law, he still is punishable in the Netherlands according to Art. 5 par. 1 subsection 2. Traditionally such cases would require dual incrimination. The present formulation of Art. 5 par. 1 subs. 4 establishes jurisdiction concerning offences as designated in this article if the facts are committed in a State where this particular conduct is not considered a crime.

In Art. 4 CCNL the principle of universality is laid down for some crimes mentioned in this article. The listed crimes regard the interest of the Netherlands or Dutch financial interests outside Dutch territory. An example of such a crime is money counterfeiting. Art. 4 CCNL does not mention cybercrime offences as such. The principle of universality only applies to cybercrime offences if such crimes, for example hacking (Art. 350a CCNL), are committed in the context of a terrorist attacks or in the context of the financing of terrorism. Only in case the crimes target a Dutch citizen or the suspect is located in the Netherlands, universality

[12] Art. 5, first paragraph, CCNL: 'The criminal law of The Netherlands is applicable to any Netherlands citizen who commits outside The Netherlands:…'.
4° any of the crimes defined in the Articles 138ab, 138b, 139c, 139d, 161sexies, 225, 226, 227, 240a, 240b, 326, 326c, 350, 350a and 351, as far as the offence fulfils the definition of the Articles 2 through 10 of the Convention on Cybercrime (Budapest, 23 November 2001, Bulletin of Treaties 2002, 18, and 2004, 290) and any of the crimes defined in Art. 137c through 137e, 261, 262, 266, 284 and 285, as far as the offence fulfils the definition of the Articles 3 through 6 of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of Acts of a racist or xenophobic nature committed through computer systems (Strasbourg, 28 January 2003).

[13] *Staatsblad* 2006, 300. (The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published).

[14] Kamerstukken II 2004/05, 26 671, nr. 7, p. 31. (The *Kamerstukken* are Parliamentary Documents. "II" refers to the Second Chamber, "I" to the First Chamber).

[15] Tekst en Commentaar strafrecht, note 3 sub e. at Art. 5 Sr.

[16] Kamerstukken II 2004/05, 26 671, nr. 7, p. 31.

applies. This article also refers to forgery, including computer forgery, if committed abroad by employees of the Dutch government (Art. 4 par. 11 CCNL).
The Dutch criminal code also contains the domicile principle. According to Art. 5a CCNL, jurisdiction exists regarding someone of non-Dutch nationality who is resident in the Netherlands and who has committed a crime as designated in Art. 5a CCNL. Among the designated crimes are involvement in terrorist acts, genital mutilation and child pornography. Therefore, if such a crime is committed outside Dutch territory by foreigners who have a residence in the Netherlands, Dutch criminal law is applicable. This is also the case if the person has chosen this residence after having committed the crime.
Under Art. 6 CCNL Dutch criminal law applies to public officials employed by a Dutch public service, who commit crimes as mentioned in this article outside the Netherlands. These are very serious crimes and offences involving the abuse of office.
Finally Art. 4a is important. Dutch criminal law applies to a person whose prosecution has been transferred to the Netherlands by a foreign state, if this transfer is based on a treaty providing for the transfer of prosecution to the Netherlands.

4. Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

To prevent a person from being punished twice for the same act, Art. 68 CCNL implements the *"ne-bis-in-dem*" principle. The Article states that a person who is already convicted or acquitted, may not be prosecuted again for the identical facts. Verdicts passed in other countries may have the consequence that the Netherlands may not start a new prosecution, even if the sentence was only partly executed or if the punishment would be rather insignificant. For a detailed explanation about the subject I refer to the Netherlands' report for the AIDP on *"ne-bis-in-idem"* by André Klip and Harmen van der Wilt published in 2004.[17] Within Europe the "*ne bis in idem*" principle has been discussed for a long time. At present, the principle is laid down in the Art. 54 – 58 of the Schengen acquis.[18] The principle is also part of the EU Charter of Fundamental Rights.[19] In Art. 50 of the Charter is stated that no one can be brought before trial or punished in a criminal procedure if there has been an

[17]Revué International de droit Pénal 2002 (published in 2004), p. 1091 – 1137.
[18] Convention from 19 June 1990 applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, L 239, 22/09/2000.
[19] Charter of fundamental rights of the European Union, 18 December 2000 C/2000 304/01

irrevocable conviction or acquittal according to the law within the European Union. However, according to Luchtman the powers of the European Union are limited, and therefore he postulates that the European Union cannot provide any security to a civilian who has been prosecuted for a crime, for which he has already been prosecuted in another country.[20]
In case there is jurisdiction in more than one country concerning one crime it is important for the countries involved to have a mutual consultation. Otherwise the consequence could be that the country which prosecuted the suspect first, prevents the authorities of other states from bringing the case to court. A 'first come' system could lead to situations in which not the most prepared or the most appropriated national authorities would deal with the case. Moreover, it could sometimes be more convenient to start the case in the country in which the suspect is living or in which the victims are living.
For these reasons Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings was established. As a consequence of inter alia this council framework decision, the Dutch Public Prosecutors Office has published a directive "Aanwijzing rechtsmachtgeschillen bij strafprocedures[21]" (Directive concerning the procedure in conflicts of jurisdiction"). This directive is in force since the 15th of June 2012. The Council Framework decision provides several solutions in case a judicial procedure targets the same facts in more countries:

- to stop the investigation in the Netherlands or abroad;
- to take over the prosecution of the case by the Netherlands or by a foreign country (this possibility is laid down in Art. 4a CCNL);
- to continue the investigations in both countries, but agree on the question who will prosecute which specific crimes and where the prosecution will take place;
- to start a Joint Investigation team (JIT) in which both countries cooperate.

According to the Council Framework Decision of 2009/426/JBZ of 16th December 2008, Eurojust should be notified in case of a probable conflict of jurisdiction between countries and the conflict falls within the competence of Eurojust.
Concerning the issue of "*ne-bis-in-idem*" it is important to address the definition of "the same fact". In Dutch jurisprudence the primal condition is that the crime is committed on the same place and on the same time. With cybercrime offences this may not be often the case. In a case regarding pictures containing child pornography, which are put on the "internet cloud", a

[20].J.J.M. Luchtman Transnationale rechtshandhaving in de EU en het ne-bis – in –idem beginsel, SEW, Tijdschrift voor Europees en Economisch recht, June 2011
[21] Staatscourant, 2012 Nr. 11716 (The Staatscourant is the official Dutch newspaper in which official Dutch announcements are published.)

person (A) can view these in country (X) and another person (B) on the same moment in country (Y). One could argue that these facts should not be considered as one crime, but as two separated crimes. In case of two separate crimes it would be possible to prosecute and punish both crimes. Therefore, the different places where and times when people have taken cognizance, the two crimes may be seen as different facts. Because these facts are not strictly 'one' in the sense of the "*ne-bis-in-idem*" jurisprudence, however, it is important to have consultation among the countries considering prosecution of similar facts that have been committed by one person or group of persons in the same period of time.

This kind of consultation takes place between the Netherlands and other countries in case of a jurisdictional conflict or if both countries want to discuss the investigations concerning the same person or the same group. Such a consultation often just takes place at a police station or in a prosecutors' office; the consultations can also be organized at the premises of Eurojust. Eurojust is an on call organization, and can be reached 24/7. In case two or more countries wish to coordinate an investigation, Eurojust can arrange a meeting between the Examining Magistrates, prosecutors and/or investigators.[22] In this consultation, the cases are discussed, investigations are matched, and future appointments can be made. This deliberation between both countries may lead to the establishment of a Joint Investigation Team (JIT). Eurojust can materially and financially support the establishment of a JIT.[23] Before a JIT can take off there has to be signed an agreement between the countries establishing the JIT. The Dutch procedure regarding JITs is laid down in the Art. 552 qa – 552 qe CPCNL. In the Netherlands it is the Public Prosecutor who may sign such an agreement (Art. 552qa). In this agreement decisions may, among others, be laid down concerning the question which country will prosecute the suspect(s). In cross-border investigations, as cybercrime cases often are, a joint investigation team can make the cooperation between several national investigation teams easier. Under Art. 552 qc, official reports from investigators of other countries of the JIT can be used as evidence in Dutch court. In case a JIT agreement is signed, letters of request asking for mutual assistance have become redundant. The national teams can work together and share the results of the investigations. Subsequently, the result of the various teams can be used as evidence in court in the various countries. In cybercrime cases it can be important to work within a short timeframe and for this purpose cooperating through a Joint Investigation Team can be very useful tool.

[22] http://eurojust.europa.eu/Pages/home.aspx; Eurojust was established by Council Decision 2003/659/JHA of 18 June 2003. This Council Decision was amended by Council Decision 2009/426/JHA of 16 December 2008.
[23] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jitsfunding/Brochure/JITs-funding-brochure-2012-EN.pdf

Chapter 3 Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

All cyber crime acts may have a transnational dimension. Cybercrimes definitions do not have an international element, but most of the time these crimes have an international element. Often the suspect lives and acts abroad, or the victims live in another country, or the hosting company of the internet site is situated in another country. An example of a cybercrime offence is "skimming". The principal element of "skimming" is the forced use of a bank card. In preparation for this crime the criminals place observation and recording equipment at a cash dispensing point. With this equipment the data of the bank card are copied and the PIN-code is recorded. Few hours later the criminals log on at the website of the bank with this information, and money to which the criminals had no right is transferred to another account. In practice these crimes have in nearly all cases a cross border nature. The recordings take place in another country as where the money is obtained. Under the law of the Netherlands, such acts are punishable under Art. 232 CCNL. This crime was introduced in the Criminal Code of the Netherlands by the first Computer Crime Law.[24] It implements the Council of Europe Framework Decision of 28 May 2001, regarding fraud and forgery by ways of payment other than cash.[25] Article 232 CCNL defines the forgery of bank cards as a criminal act. The maximum penalty for this offence is six years of imprisonment. Preparation for "skimming" has been made punishable by a separate Article, namely Art. 234 CCNL. "Skimming" is considered a typical cybercrime due to the way computer technology is used to commit this offence. Basically, forgery of bank cards, and theft by using a false key (using a PIN code to which one is not entitled is considered as the use of a false key) are not typical cybercrime offences. In relation to computers, however, these offences implement the Cybercrime Convention, Articles 7 (computer falsifications) and 8 (computer related fraud).

[24] Staatsblad (Bulletin of Acts and Decrees) 1993, 33.
[25] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JBZ), PbEG L. 149.

To what extent do definitions of cyber crime offences contain jurisdictional elements?

Forms of cybercrime are punishable under a lot of old and new crime definitions. These definitions do not contain jurisdictional elements as such. The offence of "hacking",[26] for instance, regards the use of an automated device. The offence is not limited to computers situated in the Netherlands.

Some of the crimes considered cybercrimes contain elements that have an international dimension. An example is Art. 240b CCNL.[27] In this article the possession of child pornography is established as a criminal offence. A person is considered to possess child pornography if he has access to such pictures. It may happen, for instance if the pictures are attached to an email, that the data are stored on a computer which is situated in another country. The result is that a person in the Netherlands possibly possesses child pornography while the data are stored in a computer not located on Dutch territory.

Also other elements of this crime have international elements, namely for example "import" and "export". If data are sent from one person to another it may occur that these data are "exported" to another country or "imported" from another country although the perpetrator is not aware that by his action a border is passed.

[26] 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.

[27] Article 240b of the CCNL

1. A prison sentence of a term not exceeding four years or a fine of the fifth category will be imposed on any person who distributes, offers, publicly displays, manufactures, imports, forwards, exports, acquires, keeps in their possession or provides, with a computer system or via a telecommunication service, access to an image or data carrier which contains an image of a sexual act which involves, or seemingly involves, a person who has evidently not reached the age of eighteen.
2. A prison sentence of a term not exceeding eight years or a fine of the fifth category will be imposed on any person who commits one of the criminal offences referred to in the first paragraph as a profession or by habit.

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

Similarly, the general provision regarding the preparation of a crime (Art. 46 CCNL) and the provision by which the attempt of a crime is defined (Art. 45 CCNL) do not have any jurisdictional elements. The same can be said about the articles concerning co-perpetratorship and complicity (Art. 47 CCNL and Art. 48 CCNL. respectively). Conspiracy (Art. 96 CCNL) is only an offence in connection with certain severe crimes, which are mentioned in Art. 92 – 95a CCNL. These offences do not contain specific jurisdictional elements either, though these crimes may also be prosecuted if committed abroad.

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

As any other crime, cybercrimes can be dealt with by a state on its own by passing new criminal legislation regarding existing or new offences or which change or create possibilities for investigating cybercrimes. However, while cybercrimes have nearly always a cross border nature, international cooperation in legislation and investigation is preferable. The Cybercrime Convention of the Council of Europe of 23 November 2001is of course a very important treaty that has led to harmonisation of laws in the field of cybercrime in a lot of countries. The scope of this Convention is far beyond European borders, while also countries as the United States of America and South Africa are Parties to it. The Convention provides for a wide range of provisions on substantial, procedural and mutual assistance matters.
In the Netherlands, the first changes of the criminal code and the criminal procedural code in order to fight cybercrime date from 1993.[28] This is the first Computer Crime Act *(Wet computercriminaliteit*).[29] Computer crime definitions are not laid down in a separate statute, but are incorporated in the Dutch criminal code. When after some years some changes were necessary, a second Computer Act was adopted in 2006[30], which also implemented the Cybercrime Treaty.[31] Besides, changes in the Dutch law concerning cybercrime often result from joint efforts.

[28] An extended overview of Dutch legislation on the field of Cybercrime is given by G.J. Koops, Cybercrime legislation in the Netherlands, Cybercrime report for the 18th International Congress on comparative law, Washington DC, 25 – 31 July, 2010.
[29] Staatsblad 1993, 33.
[30] Staatsblad 2006, 301
[31] Staatsblad 2006, 299.

In the European Union several initiatives for cooperation in the field of cybercrime have been developed. Recently, the proposal for a Directive on attacks against information systems was made public.[32] The proposal for the Directive on attacks against information systems is for a large part the same as the Council Framework Decision 2005/222/JHA, which criminalizes the illegal access, illegal system interference and illegal data interference of information systems. The Directive obliges the countries to create a 24/7 contact point (including an obligation to react within eight hours to urgent requests). The task of this contact point is also to be helpful to provide speedy legal aid between member states.
Another European initiative is the European Cybercrime Centre (EC3). This Centre opened its doors on 1 January 2013 in The Hague in the Netherlands, in the building of Europol. The purpose of this European Centre is dealing with cybercrime and investigating the illegal activities of organized criminal gangs on the internet. The European Centre is mandated to tackle the following areas of cybercrime:

a. Crimes committed by organised groups to generate large criminal profits such as online fraud.
b. Crimes which cause serious harm to the victim such as online child sexual exploitation.
c. Crimes which affect critical infrastructure and information systems in the European Union.

Does your national criminal law provide for criminal responsibility for (international) corporations/providers? Does the attribution of responsibility have any jurisdictional implications?

Our national law provides for criminal responsibility of (international) corporations/providers. A corporation/provider acting as an intermediary may be held criminally liable for "content"

[32] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.

crimes. It can under certain circumstances be seen as a co-perpetrator of the person who puts the information on the internet. At least the corporation/provider can be held responsible as an accessory of the crime if it had knowledge of the distribution of the illegal content (Art. 48 CCNL),[33] The criminal liability of legal entities is laid down in art. 51 CCNL. In this article is state that crimes can be committed by individuals and legal entities.

The jurisdictional principles of the Netherlands were pointed out in chapter 2. The principle of territoriality is laid down in Art. 2 CCNL. This is the basis for the applicability of Dutch law if the illegal content is accessible on Dutch territory. Under circumstances also Art. 5 (active nationality principle) can be important if the person or the company is Dutch.

Art. 54a CCNL introduces conditions which may lift the liability of an intermediary.[34] If after a warrant from a Public Prosecutor the corporation has taken all reasonable and possible steps to render the illegal content inaccessible, these conditions are met. Refusing to comply with such a warrant is a crime by itself (Art. 184 CCNL) and, in addition, the company remains accountable as an accessory in the content related crime.[35] For giving such an order the Public Prosecutor needs the authorization from the Examining Magistrate. This has been laid down in the "Aanpassingswet Richtlijn inzake electronische handel" (Implementing Law of the Directive on Electronic Commerce).[36] Section 4 of this Directive contains rules which limit the liability of providers that act as an intermediary. To guarantee the free flow of information Providers should under certain circumstances not be punishable. To implement this Directive Art. 54a CCNL was added in the Dutch Criminal Code.

The scope of an order of the Public Prosecutor, authorized by the Examining Magistrate, to remove certain data from the internet is not limited to the Netherlands. Article 184 CCNL makes punishable the non-compliance by companies in the Netherlands. These may also be branches of foreign companies which are based in the Netherlands. The Dutch government may exercise its jurisdiction towards the branch in the Netherlands. However, the Dutch branch of the company may for the executing of the order need assistance of the parent

---

33 Article 48 CCNL: The following persons are liable for punishment as accessories to a serious offence:
(1) those who intentionally assist during the commission of the serious offence;
(2) those who intentionally provide opportunity, means or information to aid in the commission of the serious offence.

34 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

35 Prof. Stamhuis, AIDP cybercrime report 2, p. 23 gives a detailed explanation about this topic. He also discusses the Dutch jurisprudence on this subject.

36 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

company. Ignoring the order by the company concerned would create criminal liability for the content for the intermediary and also creates criminal liability for the crime of Art. 184 CCNL. With regard to companies which have no branch in the Netherlands, the Public Prosecutor has no competence to issue orders, as an order directed at a foreign firm could be seen as an infringement of the sovereignty of the relevant state. However, a company that offers services on the Dutch market has to comply with Dutch law. Therefore, an internet provider can be held criminally liable for the content on a website which it hosts, if the company is knowledgeable about the content, even if the Public Prosecutor is not competent to issue the 'take down' order.

The result of this is that if the hosting website or provider is not situated in the Netherlands, there are limited possibilities to enforce cooperation. Hence, in practice, the order by the Public Prosecutor is only enacted in cases that it may be enforced. If the provider is not situated or represented on Dutch soil, the Dutch authorities will alert the authorities of the state where the provider is located regarding a specific content on the website involved that is against the law, for instance child pornography, and ask them to take the necessary steps. The fact that the prosecutor can not enforce the order to take down does not change the criminal responsibility of the provider if the provider is aware of the illegal content of the data and still does not take action against the content and its distribution. In that case the provider can be prosecuted in the Netherlands.

There is a proposal to change Art. 54a CCNL[37]. In the proposed text the responsibility of the provider exists if there is awareness in the company about the concerning illegal content. In the proposed text of the article it is not necessary that an order of the prosecutor is ignored to create criminal liability.

This issue is further elaborated on in chapter 4, question 9, in discussing the 'notice-and-take-down' procedure.

[37] Art. 54a (not yet enacted revision) CCNL
A provider of a communications service shall, in case of a criminal offence committed by that service, not as such be prosecuted if he

a. is not aware of this offence or, as soon as he is aware of it, immediately takes all measures that can reasonably be required of him for making the data regarding this offence inaccessible;
b. fulfils an order as meant in Art. 125p of the Code of Criminal Procedure
c.

Chapter 4 Cooperation in international matters

1. To what extent do specificities of information technology change the nature of mutual assistance?

Information technology does not change the nature of mutual assistance. Law enforcement authorities of sovereign states request each other's assistance for investigating and prosecuting cross border crimes.
Information technology could be an instrument to make cooperation between law enforcement authorities simpler and quicker. Today's rather formal mutual assistance procedures could be adjusted to the possibilities provided by information technology. For instance, it would benefit the fastness of cooperation if letters of request, and the responses to those requests, could be sent digitally. For facilitating cooperation, the requirement of a signature of the competent authority on the request could for instance be considered to be fulfilled by a signature on a scanned document, which would make it possible for requests to be sent by email. Doubts about the identity of the sender should obviously be avoided.
A good example of using modern information technology in the execution of a request on assistance is the direct transmitting intercepted telephone communications to law enforcement authorities in a foreign country. This possibility is laid down in Art. 552 ob CCPNL.[38]
The use of information technology makes it possible for cooperating law enforcement authorities in different jurisdictions to inform each other instantaneously of investigation results. This practice may lead to better and faster cooperation, and could make the handing over of information months after the request, which happens all too often, something of the past.

2. (a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions.

The Dutch Criminal Procedural Code provides the possibility of the interception of (wireless) telecommunication. The possibility of intercepting wireless communication is laid down in Art. 126 m of the CCPNL. The order to intercept is given by the Public Prosecutor after authorization by the Examining Magistrate. The order can only be given if there is reasonable

[38] More about this article in the answer of question c. of Chapter 4.

suspicion that a serious crime has been committed (a crime for which pre-trial detention is allowed). An additional requirement is that the crime by its nature constitutes a serious threat to society. According to Dutch law public providers of telecommunication services have to make it possible that their network or services can be intercepted. This obligation is laid down in Art. 13.1 Telecommunication Law (*Telecommunicatiewet*).[39] According to the relevant Explanatory Memorandum of the government, this obligation only applies if a service is "publicly offered and available for anyone who wants to make use of this public offer against the conditions stated in the offer."[40] The article is applicable to telephone companies and to internet providers. Detailed arrangements are set in the Intercepting Public Telecommunications Networks and Services Decree (*Besluit aftappen openbare telecommunicatienetwerken en -diensten*)[41]; and in the Regulation on Intercepting Public Telecommunications Networks and Services (*Regeling aftappen openbare telecommunicatiewerken en –diensten*).[42]

Interception is not restricted to persons suspected of having committed a crime. It is possible to intercept anyone if it is clear that relevant information communicated via his telephone lines are required for an investigation. It is not allowed to intercept communications of a person with the right of non-disclosure (lawyers, public notaries, clergy, medical practitioners) (Art. 126aa subsection 2 CCPNL). This is only different when the person in question is himself suspected of a crime.

On the basis of Art. 126m sub 3 CCPNL the order to intercept the communication may be issued to the provider of a public telecommunications network or to a public telecommunications service. This is only possible in cases regarding providers as defined in Art. 1.1 sub ee and ff Telecommunication Law. Public providers of telecommunication networks are obliged to carry out orders given on this basis.

The consequence is that services which are not public, but only available for a closed group of users, are not subject to this obligation. The Dutch District Court of Rotterdam dealt with this issue in its ruling of 27 March 2009.[43] The Court decided in that case that the company

---

[39] Article 13.1 1. Providers of public telecommunication networks may only make their telecommunicationnetworks and telecommunication services available to consumers provied that the communication can be intercepted.
2. By general governmental decree rules may be issued regarding the technical prerequisites for the interceptability of public telecommunication networks and public telecommunication services.

[40] Kamerstukken II 1996/97, 25 533, nr. 3, p. 72 (MvT Telecommunicatiewet) "publicly offered and made available for everyone who would like to make use of the offer on the basis of the publicly stated conditions.(*'openbaarwordtaangeboden en beschikbaar is voor een ieder die van dat aanbod gebruik wil maken tegen de in het openbare aanbod vermelde condities*").

[41] Staatsblad 1998, 642.

[42] Staatscourant 2001, No 107, p. 20.

[43] LJN BH 9324

“Surfnet” cannot be regarded as a public electronic network. “Surfnet” offered its services only to scientific institutions and universities. The Court regarded their services too limited for being considered a public network.
Dutch procedural criminal law does not make a distinction between the interception of information sent by phones, computers and other devices. On the basis of Art. 126 m, an order to cooperate in the interception can be given to both (mobile) telecom providers and internet service providers.
Another article relevant for the interception of telecommunication is Art. 126t. In case there is suspicion that a crime is committed for which pre-trial detention is possible, and this crime is because of its nature or because of its connection with other crimes, which have severely shocked Dutch society, the Public Prosecutor may order to an investigation officer to record, using technical equipment, communication which is not meant to be public and which takes places inside the services of a provider of a communication service. In subsection 5 of this article it is prescribed that the Public Prosecutor needs the authorization of the Examining Magistrate for giving such an order. Art. 126 la defines the concept of a “provider of a communication service”. Art. 126 la determines a provider of a communication service to be a person or company which offers his services to people by offering the possibility to communicate with the help of automated systems, or to process or save data for the purpose of such a service or for the users of that service. Providers of communication services can for example be companies offering a webhosting service (as Leaseweb) or operators of a website (as Hyves). Articles 126m and 126t have a similar outlook, though are different. For services which are offered publicly the Telecommunication Law provides the obligation to providers that transmitted information should be possible to intercept. This obligation does not exist for providers of communication services as mentioned in art. 126t. On the basis of Art. 126m law enforcement authorities may record transmitted communications, though there is no obligation for the provider to make the information interceptable. Therefore, in the cases when communications are intercepted on the basis of Article 126t, the retrieved date can be illegible, while providers of communication services that are not publicly offered are not obliged to make it possible that the communications be intercepted. This is an important difference between these two articles. This is all the more of important, while in daily practice more and more people and also criminals use systems in which the transmitted information can be (and often is) encrypted. The most important example is “skype”. In my view, “skype” is not a public telecommunication network, but a provider of a communication service. For that reason only the communication between the two automated devices may be intercepted,

but the company is under no obligation to provide the possibility that the communication can be intercepted. Even if the definitions of 'network provider' and 'communication service' are interpreted differently, and "skype" was to be considered a public telecommunication network, the issue that this company is not situated in the Netherlands remains.[44] I will get back on this jurisdictional issue later.

In case the intercepted communication is encrypted, the (legal) person who is likely to be acquainted with the decryption means may be ordered to decrypt the data. The possibility to give such an order is laid down in Art. 126m subs. 6 and 7 and in Art. 126t sub 6 CCPNL. This order cannot be given to a suspect. The issuing of such an order rarely leads to the unravelling of the code; good encryption is is hard to decrypt.

Because of the encryption of internet communications, it has become more difficult to know the content of these communications. The use of encryption can be seen as a sign that someone has something to hide. However, it is important that providers of internet services can offer services which are directed at the protection of individual communications on the internet. Therefore, encryption of the communication in internet services has its value. For law enforcement authorities, the only solution to this problem is entering the computer or smartphone and put some electronic device in it in order to look at or listen to the communication before the encryption takes place. Technically this can be done, though to date there is no legislation on this matter. With a letter to the Parliament, the Minister of Justice and Security has announced that new legislation is in preparation to render it possible to penetrate electronic devices.[45][46]

Similar to orders to intercept wireless communications, an order may be issued regarding further information about the communications, the so-called traffic data. This order makes it possible to gain intelligence on the telephone number of the contacts and the name under which the telephone number is registered etc.. Art. 126n CCPNL provides the possibility to give this order with regard to the users of the communication service and the transmittance of the communication. In addition, Art. 126 na CCPNL provides for the requisition of the names and address details of the persons involved. Art. 126 nb CCPNL gives the possibility to get the information about a telephone or another device with special technical equipment. For this

[44] Another opinion is given by Odinot and De Jong in: Justitiële Verkenningen, tappen en infiltreren, *G. Odinot en D. de Jong,* 'Wie belt er nou nog? De veranderende opbrengst van de telefoontap', p. 26.

[45] Since 2002 the intelligence- and security services may make use of such competencies on the basis of Article 24 of the law on intelligence and secret services. In Dutch Parliamentary history the Parliament explicitly stated that normal law enforcement authorities cannot excercise the competency to enter automated devices. According to the Parliament such competencies were not necessary for criminal investigations.

[46] Letter of Minster of Security and Justice Mr. Van Opstelten to the chair of the Parliament of 15 October 2012.

purpose the police uses an IMSI (International Mobile Subscriber Identity) catcher. An IMSI catcher is a device that resembles a mobile phone base station, which attracts the traffic of mobile phones in its vicinity.
Another important provision is Art. 126 ni CCPNL. This article entitles the Public Prosecutor to order the preservation of data stored on a computer, which are particularly vulnerable to loss or change. The Public Prosecutor may issue this order in case of a suspicion of a crime for which pre-trial detention is allowed and which would seriously infringe the rule of law. This order may be given for a period of not more than 90 days. This period is once extendible for another 90 days. In subsection two of this article the obligation is laid down for the provider to also provide the data necessary for retrieving the identity of other providers whose networks or services were used for the relevant communication.
In Dutch law there is no distinction between the interception of telecommunication by means of telephones or by computers. While a phone tap is placed on a telephone number, an internet wiretap is placed on an IP (internet protocol) address. This IP address is the identification number of a computer on the internet. In the Netherlands only Dutch IP addresses can be intercepted. If the Dutch prosecutor wants to intercept a foreign IP address he would have to send a letter of request to his counterparts in the country where the IP-address is registered. This is the same when he wants to intercept a foreign phone number.
In case an IP address is wiretapped, all data of the computer are intercepted including the data traffic of other persons using the same IP-address.
Before a request is submitted, it has first to be verified at the Central Information Desk Telecommunication Research (CIOT) that the phone number or the IP-address is still in use. This centre is the link between the telecommunication providers and the investigators. Providers of telephone and internet companies are obliged to give all information about their customers within 24 hours.
If the internet is wiretapped this means that all information from and to the IP-address involved is sent by the provider to the central police registration unit, where all data are kept and stored in a safe environment. The consequence of such wiretaps is that a large amount of data is intercepted, for instance downloaded movies and website visits. The Public Prosecutor has as well the possibility to only intercept e-mail traffic by the specific IP-address. In addition, the provider could be ordered to provide the internet traffic data.

The Dutch telecommunication law prescribes that data regarding the use of the internet have to be stored.[47] As from 16 July 2011, the period in which these data have to be kept is six months.[48] The data which have to be stored are among others the time when a person logs in, the IP-address, information regarding email contacts of the sender and the receiver and the IP-addresses of the internet pages that have been visited.

Statistics regarding fixed telephone Lines and mobile Phone taps in the Netherlands

	Number of Telephone numbers		Number of Telephone taps		Percentage of tapped telephones	
	Fixed	Mobile	Fixed	Mobile	Fixed	MobileMobiel
1993	7.634.000	216.000	3.610	0	0,05%	0%
1994	7.859.000	321.000	3.284	0	0,04%	0%
1998	9.337.000	3.351.000	3.000	7.000	0,03%	0,21%
2007	7.404.300	19.285.000	3.997*	20.985*	0,05%	0,11%
2008	7.317.200	20.627.000	2.642	23.783	0,04%	0,12%
2009	7.320.000	21.182.000	3.461	21.263	0,05%	0,10%

Bron: telecomgegevensaansluitingen: ITU, World Telecommunication/ICT indicators

In the Netherlands the instrument of telecommunication interception is often used in investigations. Since 1998 the number of telephone taps has increased. According to a report of the WODC (Scientific Research and Documentation Centre), the reason for this is the rise of the use of mobile phones.[49] In 2010 the number of taps amounted to 22.006. Regarding internet taps, there were 1704 requests for an IP-address interception in 2010. It is expected that this number will increase in the coming years.

Up until now the Dutch authorities address differently the interception of telephone lines and the interception of internet data. Due to the use of smartphones, people increasingly use the same instrument for both telecommunication networks. Today's practice is that two separate requests are made: one for a telephone tap and one for an internet tap. It is expected that in future orders to intercept internet data and to intercept telephone communication will be combined more and more. It is also expected that the use of internet taps will increase rapidly and may outnumber the orders for interception of telephone lines.[50] Data on 2011 and 2012 are unfortunately not yet available.

Interception of wireless communications can also be realised directly, instead of via a telecommunication provider. The Public Prosecutor may with the authorisation from the

[47] Art. 13.2a, par. 3 subsection b Telecommunication Law.
[48] Kamerstukken II 2009/10, 32 185, nr. 2, p. 1.
[49] WODC report, Het gebruik van de telefoon- en internettap in de opsporing, p. 81
[50] Justitiële Verkenningen, Tappen en infiltreren, G. Odinot en D. de Jong Wie belt er nou nog? De veranderende opbrengst van de telefoontap, p. 13

Examining Magistrate order an investigation officer to record confidential communications with the help of a technical device (Art. 126l CCPNL). Such an order may only be given if there is suspicion of a crime for which pre-trial detention is allowed and which would seriously infringe the legal order. With regard to this article confidential communication is defined as ”communication between two or more persons which takes place in private”.[51] Confidential communication occurs not only in situations where two people just talk to each other directly, but also if someone is talking on the phone or communicating via a computer, monitor etc. Various technical devices are used for this kind of interception, for example directional microphones and keystroke loggers. If it is necessary to enter a residence to install the required technical equipment, this is allowed under the conditions described in the law.[52]

b. To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

For the execution of the order of the prosecutor to intercept (wireless) communication it is important where the provider of the public telecommunication network or service is located. The obligation for public providers of internet networks or services to comply with orders to intercept under the Telecommunication Act only applies in the Netherlands. Consequently, this obligation does not exist for providers abroad, such as Skype. Even if such companies were seen as a provider of public telecommunication, Dutch authorities could not enforce the Dutch telecommunication law which requires that the information be interceptable.
An order under Art. 126m or Art. 126t CCPNL may only be issued and executed if the company is under Dutch jurisdiction. In case a company, or a branch of the company, is situated in the Netherlands, it falls under Dutch jurisdiction. It also happens that a company is represented in the Netherlands. For example Microsoft is a company obviously based in the United States, but is represented in The Netherlands, by Kennedy van Der Laan Counsellors. If the company has neither branches nor legal representatives in the Netherlands, the Public Prosecutor will sent a request for mutual assistance to the country where the company involved is registered.
Only through mutual assistance can an order to a telecommunication provider abroad be enforced. Of course it depends on the rules of the relevant country whether the order will be executed. With regard to mutual assistance, law enforcement authorities should in general

[51] Supreme Court, 12 October 2010, LJN BN 0526
[52] Art. 126l subsection 2.

keep in mind that serious delays in the execution of interception orders may occur. Moreover, even if the order is executed in time, extra efforts may be necessary because the available information may be encrypted.

c. Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it.

Our national law provides for the possibility for mutual legal assistance regarding the interception of telecommunication. On the basis of several international treaties a letter of request can be sent to the Netherlands for intercepting telecommunications. Such a request may only be executed if all conditions of Dutch law regarding wiretapping, mentioned above, are fulfilled. Art. 552k sub 1 CCPNL states that, if a letter of request from a foreign law enforcement authority is based on a treaty, it will be executed as far as possible. Art. 552oa CCPNL determines that a request from a foreign public authority, which is based on a treaty, may be executed in accordance with inter alia Art. 126m CCPNL and Art. 126t CCPNL. In particular, Article 552ob CCPNL provides the interception of telecommunications and direct transmittance of the intercepted lines on a request of and to the foreign authority involved. However, there must be a Treaty which gives rules for this kind of mutual assistance, in particular for direct transmittance. For instance, Article 18 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union provides for this possibility. In cases of mutual assistance on this legal basis the Dutch authorities will not even take cognizance of the intercepted communications.
Art. 552oc CCPNL deals with the notice that under a treaty has to be sent by a foreign government, informing that communication of a person who is on Dutch soil will be intercepted by the law enforcement authorities of that State. Art. 20 of the Convention on Mutual Assistance in Criminal Matters between the Members States of the European Union is an example of a Treaty which provides for this possibility.
The Dutch criminal procedural law does not contain rules for letters of request to be sent abroad by the Dutch authorities. These rules are to be found in the treaty on which the mutual assistance is based. Below I have listed a number of treaties regarding mutual assistance:

- European Convention on mutual assistance in criminal matters (Strasbourg 20-4-1959)
- The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (29 May 2000)
- Schengen Implementation Agreement (Schengen, 19 June 1990)

- Benelux Treaty on extradition and mutual assistance in criminal matters (Brussels, 27 June 1962)
- Treaty between the Kingdom of the Netherlands and the United States of America regarding mutual assistance in criminal matters (’The Hague, 29 September 2004)
- Treaty between Canada and the Kingdom of the Netherlands on Mutual Assistance in Criminal matters and protocol(The Hague, 1 May 1991)
- Treaty between the Kingdom of the Netherlands and Australia concerning mutual assistance in criminal matters (Canberra, 26 October 1988).
- Agreement between the government of the Hong Kong Special Administrative Region of the Peoples Republic of China and the Government of the Kingdom of het Netherlands concerning mutual legal assistance in criminal matters (Hong Kong, 26 August 2002)
- Convention on mutual assistance and cooperation between customs administrations (Naples II, 18 December 1997)
- VN Convention against transnational organized crime (15 November 2000)
- Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (Treaty of Prüm, 27 May 2005).

Next to the treaties concerning assistance there is cooperation between countries on the basis of mutual recognition. The first possibility is the order of freezing property or evidence, laid down in the Council Framework Decision on this subject.[53] For the purpose of a cross-border procedure a ‘freezing order’ means any measure taken by a judicial authority in a Member State to prevent the destruction, transformation, displacement, etc. of property or evidence. Evidence means objects, documents or data which could be produced as evidence in criminal proceedings. This Council Framework Decision is implemented in the Dutch procedural criminal law. The Articles 552 jj – 552 qq contain rules concerning the recognition and execution of an order from a foreign State. The Articles 552 rr – 552 vv give procedural rules concerning Dutch orders requested to be executed in another country. On the basis of such an order it is for instance possible that a computer can be seized which contains important evidence in a case. Also data stored on a server may be ‘freezed’ in a foreign country on this basis.

[53] Council Framework Decision 2003/577/HA of 22 July 2003 on the execution in the European Union of freezing property or evidence.

Mutual recognition is also the basis of the European Evidence Warrant (EEW). The European Evidence Warrant is created for the purpose of obtaining objects, documents and data for the use in criminal proceedings. For implementing the relevant Council Framework Decision[54] the new Articles 552 ww through 552 hhh have been enacted.[55] According to the new Article 552 ww it will be possible to recognize and execute an order given by an authorized judicial authority of another Member State of the European Union. Such an order may regard the seizure of objects or documents available anywhere in the territory of the European Union. The order may also regard stored or recorded data available in Dutch territory or accessible under Dutch law. It is expected that the Dutch implementation act will enter into force on the first of July 2013.

3. To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

The Netherlands only has the possibility to execute letters of request if they can be carried out on Dutch territory. If a request is made for a search in a computer or a network situated elsewhere in the world and not in the Netherlands, this request will be refused.

4. Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised.

If I understand the question right, the hypothetical case is that another state requests cooperation from the Netherlands for a crime which caused effects and is punishable in the Netherlands, but the perpetrator was acting from a state where the conduct was allowed. First of all, the conduct must obviously be punishable in the requesting state. Secondly, in case another state asks mutual assistance the Dutch law enforcement authorities will look at the Dutch legislation to see if the facts are a criminal act in our laws. Only if this is the case mutual assistance will be given (if there are no objections on other points). The situation that the person acted from a state where such acts are allowed is not relevant.

[54] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters

[55] Wet van 13 december 2012 tot implementatie van het kaderbesluit nr. 2008/978/JBZ van de Raad van de Europese Unie van 18 december 2008 betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures (PbEU L 350)

5. Does your national law allow for extraterritorial investigations? Under what conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

In general, investigations take place in the Netherlands. Though, in some circumstances extra territorial investigations are executed abroad. According to Art. 539a CCPNL a Dutch investigation officer is allowed to act outside the territory of the Netherlands. Several treaties include measures for law enforcement authorities to act abroad. For example the Schengen acquis[56] contains such a measure in the Articles 40 and 41. An important condition is if the extraterritorial actions have to be allowed beforehand or can be allowed after the actions. If approval has to be provided beforehand cooperation is needed and therefore there is no infringement of sovereignty possible. In urgent cases for example when the police chases the suspect across the border into another country it is possible to achieve the consent afterwards from the country involved.

Besides, Dutch law enforcement authorities may act abroad in the framework of a Joint Investigation Team. The Dutch Supreme Court ruled on the issue of extraterritorial law enforcement in its judgement of 5 October 2010.[57]

In its judgement the Supreme Court considers among others that the Dutch court is responsible to verify if the investigative actions of Dutch law enforcement authorities abroad complied with Dutch procedural rules. It is remarkable that the Court determined that it is not for the Dutch court to check whether provisions of international public law have been complied with. According to the Court, compliance with international public law is a matter for the state where the actions took place and not of the suspect.

As a result of the EU Treaty on Mutual Assistance of 2000[58] there are also some other possibilities of exterritorial investigations incorporated in Dutch procedural law. These exceptions are laid down in Art. 126 ma CCPNL. Two different situations can be distinguished in cases regarding investigations including wiretapping. The first situation is if

[56]Convention from 19 June 1990 applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, L 239, 22/09/2000.

[57] Supreme Court, 5 October 2010, LJN BL5629.NJ 2011, 169 with the comments by. T.M. Schalken

[58]Convention on Mutual Assistance in Criminal Matters between the Member States ofthe European Union, 29 May 2000, *OJ*C197/1, 12.7.2000.

it is known beforehand that the person whose phone or computer is wiretapped goes or is abroad. In such a case a notification is sent to the relevant State before the wiretapping takes place. The second situation is where a person leaves the country unexpectedly, and while the wiretapping is continued information from abroad is intercepted as well. In such a case the notification should be sent afterwards.[59]

> 6 and 7. Is self service (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate to public and protected information. What is the (both active and passive) practice in your country? If so does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

On the basis of Art. 125i CCPNL a computer and the data stored at this electronic device maybe searched.[60] Moreover, Article 125j CCPNL allows searches in computer networks. A network search is only allowed to the degree to which the network is lawfully accessible to the persons regularly using the computer concerned. The law enforcement authorities are not allowed to hack into the whole network. In relation to such a network search, Art. 32 of the Cybercrime convention is important. [61] According to this provision, publicly available information including (open) source stored computer data, may be accessed, regardless of the geographical location where the data are stored. Another way to have lawful access to data is access with the consent of the person or organisation entitled to disclose the data. These data

[59] Art. 126ma
Paragraph 1
If it is known, when an order is being issued as meant in Art. 126m, third paragraph, that the user of the number, as meant in Art. 126m, second paragraph sub c, is in the territory of another state, this other state shall, as far as prescribed by a treaty and with application of that treaty, be informed of the intention to record telecommunication, and approval of that state shall be obtained before the order will be executed.
Paragraph 2
If, after the recording of telecommunication on the basis of the order, it becomes known that the user is in the territory of another state, this other state shall, as far as prescribed by a treaty and with application of that treaty, be informed of the recording of telecommunication, and approval of that state shall be obtained.

[60] Art. 125i Code of Criminal Procedure
The examining magistrate, the public prosecutor, the assistant public prosecutor and the investigating official are under the same conditions as meant in Art. 96b, Art. 96c, first, second and third paragraph, Art. 97, first through fourth paragraph, and Art. 110, first and second paragraph, entitled to search premises for the recording of data that could in those premises be recorded or stored on a data carrier. They may record those data in the interest of the investigation. Art. 96, second paragraph, 98, 99, and 99a are equally applicable. .

[61] Art. 32 Cybercrime treaty: A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

may be stored on a server abroad. An internet search may only take place while searching the computer of a suspect. After the search is finished and the computer has been seized according to Article 96 CCPNL, the internet search may no longer take place.
As mentioned before, "self service" by public investigators is allowed as far as it regards public information. The District Court of The Hague addressed this issue in its decision of 23 December 2011.[62] The Court reasoned that police forces may search the internet, in analogy with overseeing the non-digital public sphere. Therefore, an explicit legal provision is unnecessary for searches on the internet. In this particular case, the police had used Google Earth to have a look at the garden of the suspect. The police file included a print of the garden. According to the Court, this conduct was legal.
The gathering of protected information by law enforcement authorities is different. For the search of protected information the consent of the user of the computer is needed, as discussed above. In case of such a search it is possible that the computer is situated in another country. In such a case it is possible that the territoriality of this particular country is violated. With regard to the issue of searches in computers, two decisions in the same case before the District Court of Rotterdam and the Appeals Court of The Hague are interesting. The facts of the case are as follows. The police got information that a large shipment of cocaine was being brought to the Netherlands. The received messages revealed that there was further information about this drugs transaction on a hotmail account. Three possible passwords of this hotmail account were given. The Public Prosecutor, with the authorization of the Examining Magistrate, gave an order to the Microsoft office, situated in the United States, to provide information on certain emails. To effectuate this order a letter of request had to be sent to the United States. Because of the urgency of retrieving the information, the Public Prosecutor had ordered a policeman to log in at the hotmail account and get the information about the cocaine transport. Detailed information about the ship by which the cocaine was brought to Rotterdam was indeed present in the inbox. The District Court in Rotterdam decided on 26 April 2010 that the police had no permission to log in on the email account and take cognizance of the email messages.[63] For getting the information, the Public Prosecutor would have been obliged to approach the Microsoft Company, in response to a letter of request sent to the United States law enforcement authorities. This procedural defect resulted in a reduction of the punishment. The Appeals Court in The Hague came to another decision on 27 April 2011.[64] The court

[62]LJN BU 9525.
[63]LJN: BM 520
[64]LJN: BR 6836

considered that the suspect had during his hearings stated that he was not the proprietor of the hotmail account and that it was not in his use. The Appeals Court stated that even if there was a procedural defect, this had no effect on the case of the suspect. This is the so-called "Schutznorm" requirement. While by logging into the hotmail account there was no infringement of the interests of the suspect, he could not successfully invoke the intrusion into the hotmail account.

In my opinion another argument is relevant in this case as well. The police got their information legally according to Dutch criminal procedural law. By looking at the emails, the police violated only the territoriality of the United States while the storage of data of hotmail accounts is situated there. Nonetheless, this is a matter between States. There is not a violation of the rights of the suspect. My conclusion is the same, even if there was a procedural defect; this had no effect on the case of the suspect.

As it is not allowed for Dutch authorities to take cognizance of protected information situated abroad, foreign authorities are not allowed to search for hidden information that is situated in the Netherlands. For getting access to such information a letter of request is required (Art. 552 h CCPNL).

In the letter of the Minister for Justice and Security to the chair of the Parliament of 12th October 2012, the Minister states that an important issue is that it is not always clear in which country the data are stored. If it is known where the information is kept, a letter of request have to be sent. If it is unknown where the information is stored, however, the Minister argues that the police should be allowed to search in the systems without consent of the owner. The Minister plans to propose a change of the law in order to make this possible.

With this in mind, the question remains whether universal enforcement jurisdiction in cyberspace is necessary for successful investigations. While data (systems) can be reached from all over the world, shouldn't investigations be allowed from all over the world as well? One may argue that the sovereignty of a state is at issue if a search is directed at internet data stored in that State. This kind of "violation" is very different, however, from a house search by law enforcement authorities in the territory of another State. While it is often highly difficult to trace the source, and the territory where the data are stored, it might be a good solution to allow for searches without consent if the location of the data is unknown.[65]

[65] Another opinion you find in the article of M. Hildebrandt and M.E. Koning, Universelehandhavingsjurisdictie in Cybrspace, Strafblad, March 2012, p. 195 – 203; http://merelkoning.krikkit.nl/wp-content/uploads/2012/06/HildebrandtKoning-Strafblad-2012-3-final.pdf

8. Is your country a party to Passenger Name Record (PNR) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have anon call unit that is staffed on 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigations.

The Netherlands is party to the Passenger Name Record (PNR) agreements. The Dutch government may request passengers' data from the airline company who brings passengers to Dutch soil. This competence is based on Art. 4 par. 3 of the Aliens Act 2000.[66] This Article implements Council Directive 2004/82/EG.[67] The passengers data which have to be delivered by the airline companies are (among others):

- the number and the source of the travelling document;
- the nationality of the traveller;
- the complete name;
- the date of birth;
- the place where the traveller entered the country;
- means of transport;
- time of leaving and arriving;
- the total of persons carried on in that means of transport;
- the initial point of embarkation.

The Royal Military Police (Koninklijke Marechaussee) has a special service, which can be reached 24/7 to get information about Passengers Data. Passengers Data are also provided to Australia, Canada and the United States. The legal bases are agreements between the EU and these countries.[68]

At present a proposal on the basis of Art. 82 paragraph 1 sub d TFEU is pending regarding the use of "passenger data". The objective of the Directive is to provide further measures for the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes.[69]

[66] Art. 4 paragraph 3 Aliens Act; A transporter as meant in the first paragraph may, in the interest of border surveillance and counteracting illegal immigration, be obliged to collect passenger data and to supply these to the border surveillance officials.
[67] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data L 261/24
[68] Agreement between the European Union and the United States of America on the procession and transfer of Passenger Name Record (PNR) dat by air carries to the United Nations Department of Homeland Security (DHS) (PNR agreement 2007), Washington 26 July 2007.
Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data. 21.3.2006. (L 82/15).
Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service. 8.8.2008. (L 213/51).
[69] COM (2011)32

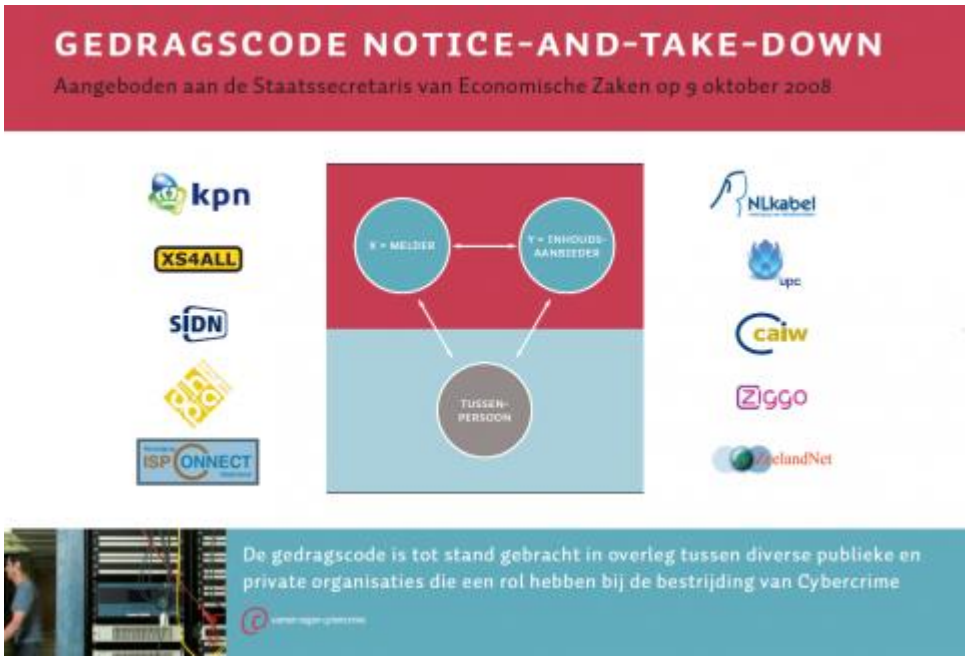
9. To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/correct/delete information? To what extent can this information be used as evidence?

Data which have been gathered can be exchanged with other police forces or foreign law enforcement authorities on the normal legal basis. The exchange of data may take place via police to police information exchange, or via mutual legal assistance.
There are some specific treaties regarding the protection of data. Directive 95/46/EC concerns the protection of passengers' data.[70] Moreover, Dutch laws regarding the right to privacy are applicable. According to Directive 95/46/EC a passenger has the right to send a request to the airline company to get acquainted with the data that are stored by it related to him. A passenger may also request the correction of the data in case they are incorrect. Corrections can only be made, of course, if the data are not yet destroyed. On the basis of the Law on Police Data[71], passengers have the same rights regarding data stored at the Royal Military Police. Every passenger may send a request to ask which data are stored there, and corrections may be requested in case of supposed errors. These requests are dealt with by the Commander of the Royal Military Police in The Hague.
The gathered information regarding passengers may be used as evidence in Court. Information may be included which is derived from the PNR record. Such a police report is admissible evidence on the basis of Art. 344 section 1 sub 2 CCPNL.

Does the law of your country allow for a Notice and Take Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

In our country a Notice and Take Down procedure is in place.

[70]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[71] Chapter 4, Wet op de politiegegevens (Law on the Police Data), Staatsblad 2007, 549



Next to this procedure, there is a procedure for individuals for complaining about the content of an internet site.[72] This procedure is the result of The National Infrastructure Cybercrime, a working group of many parties, among which Dutch hosting providers organisation, Google, Ebay, the Ministry of Security and Justice, etc. This procedure provides rules for investigating complaints about internet sites. It constitutes a self-regulating system. This mutually agreed procedure allows providers to take appropriate action on their own behalf. In cases of serious crimes, such as child pornography, the hosts can be ordered by the public prosecutor to take down the website.

The Public Prosecutor may order the internet service provider (ISP) to take down an internet site, after authorization by the Examining Magistrate**.** The legal basis of this order is Art. 54a CCNL[73] and Art. 125o CCPNL. [74]The order may only be issued if the host of the website, either a person or a company, is located in the Netherlands or is represented in the

[72] On this internet site you can fine the English translation of het Dutch code concerning notice and take down: http://www.ecp-epn.nl/sites/default/files/NTD_Gedragscode_Engels.pdf

[73]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**.**

[74]Art. 125o Criminal Procedure Code.

1. If during a search in an automated device data are found with regard to which or by means of which the offence has been committed, the public prosecutor or, during the preliminary inquiry, the examining magistrate, may decide that those data shall be made inaccessible as far as necessary for the breaking up of a criminal offence or for the prevention of new criminal offences.
2. Making data inaccessible is understood to mean the taking of measures for preventing the administrator of the automated device meant in the first paragraph or third persons from further cognizance or use of those data, as well as for the prevention of further distribution of those data. Making inaccessible includes removing the data from the automated device, preserving them for the prosecution.
3. As soon as the interest of the prosecution allows the discontinuance of the measures meant in the second paragraph, the public prosecutor or, during the preliminary inquiry, the examining magistrate may decide that those data shall be restored to the disposal of the administrator of the automated device.

Netherlands. In case the provider is located abroad the ISP may be alerted. On a voluntary basis ISP may be asked to undertake the necessary steps. The information concerning the site can also be given to the relevant State. On the basis of this information the authorities can decide on the next steps.

Another problem is whether it is possible to give a notice and take down order taking into account that the ISP is just an intermediary for information that is stored on a computer outside the country. According to the Dutch Parliament Art. 125o is in such a situation not applicable.[75] The order to take down an internet site may not be issued with regard to data that are stored on a computer outside the country. However, an order can be given to prevent the dissemination of this information to the Netherlands. The Public Prosecutor may order the Dutch ISP to make the information unavailable for people on Dutch territory.

An example of a case where the content of website was destroyed is the decision of the District Court in The Hague of 10 July 2008.[76] The suspect in this case sold drugs via two internet sites. The Public Prosecutor had made the websites inaccessible, on the basis of Art. 125o CCPNL. The court destroyed the websites on the basis of Art. 354 CCPNL,[77] because the criminal acts were committed by making use of these websites and because of the danger that new crimes might otherwise be committed with the use of these websites.

At present, the legal basis for the order of the public prosecutor to take down information from the internet is unclear. For that reason the Minister of Security and Justice has made proposals for changing the law. A new Art. 125p CPCNL[78] is proposed, which would entitle the Public Prosecutor to order the inaccessibility of data that are stored or transferred. Moreover, if someone does not comply with the order it would create the possibility for the Public Prosecutor to determine a penalty payment. This will be arranged in the (also)

---

[75] Kamerstukken II 1998 – 1999, nr. 3, p. 36.

[76] LJN BD 7012

[77] Article 354 (1): In those cases, referred to in Article 353 sub 1, the court as well decides on the application of Article 125o regarding the data which were made inaccessible if the concerning measures were not yet lifted. (2) The court may decide that the data are destroyed provided that the data concerned the violation of a crime, as far as the destruction of the data is necessary to prevent subsequent crimes. In all other cases the Court will decide on making the data available again to the administrator of the automated device.

[78] Art. 125p (not yet enacted) of the Code of Criminal Procedure

1. The public prosecutor may order a provider of a communications service or a person in control of an automated device to take all measures that can reasonably be required of him for making data that are stored or transferred inaccessible, as far as necessary for breaking up a criminal offence or for the prevention of other criminal offences.
2. The order shall be in writing and state:
a. the criminal offence and if known the name or else an as precise as possible indication of the suspect;
b. the facts and circumstances showing that making the data inaccessible is necessary for breaking up or preventing the criminal offence;
c. if necessary the penalty payment due in case of the order not or too late being fulfilled.
3. Art. 125o, second and third paragraph, is equally applicable.
4.

proposed Art. 125q CPCNl. If it is important that the website is removed quickly, the public prosecutor will be entitled to impose a penalty payment. In relation to the order as defined in Art. 125p it is also proposed to change Art. 54a CCNL.[79] In case the order were to be ignored this provision would create criminal liability for a provider or a communication service.

10. Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

In my opinion it is possible to create an international enforcement system to implement decisions in the area of cyber crime. According to the same method by which verdicts may be recognized in other States, a system can be developed in which decisions concerning the internet would be carried out. Especially a "Notice and take down" forum could be organised internationally. At this moment the Dutch authorities may not issue a take down notice if the ISP is situated outside the country. While the order cannot be issued, there is not a criminal act committed by the provider ignoring the order and it is also impossible to ask mutual assistance from the country where the websites are registered according to this crime. As it is not possible to give such an order under Dutch law no crime is committed by the provider and a request for mutual assistance can not be sent in order to ask assistance in investigating this crime. For adequately controlling criminal behaviour on the world wide web, I recommend the establishment of international rules regarding the criminal behaviour on internet websites and making possible the take down of these internet sites. If an order is given by a country to take down because the content of an internet site is against these rules it should be recognized internationally.

11. Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

[79] Art. 54a (not yet enacted revision) Criminal Code
A provider of a communications service shall, in case of a criminal offence committed by that service, not as such be prosecuted if he

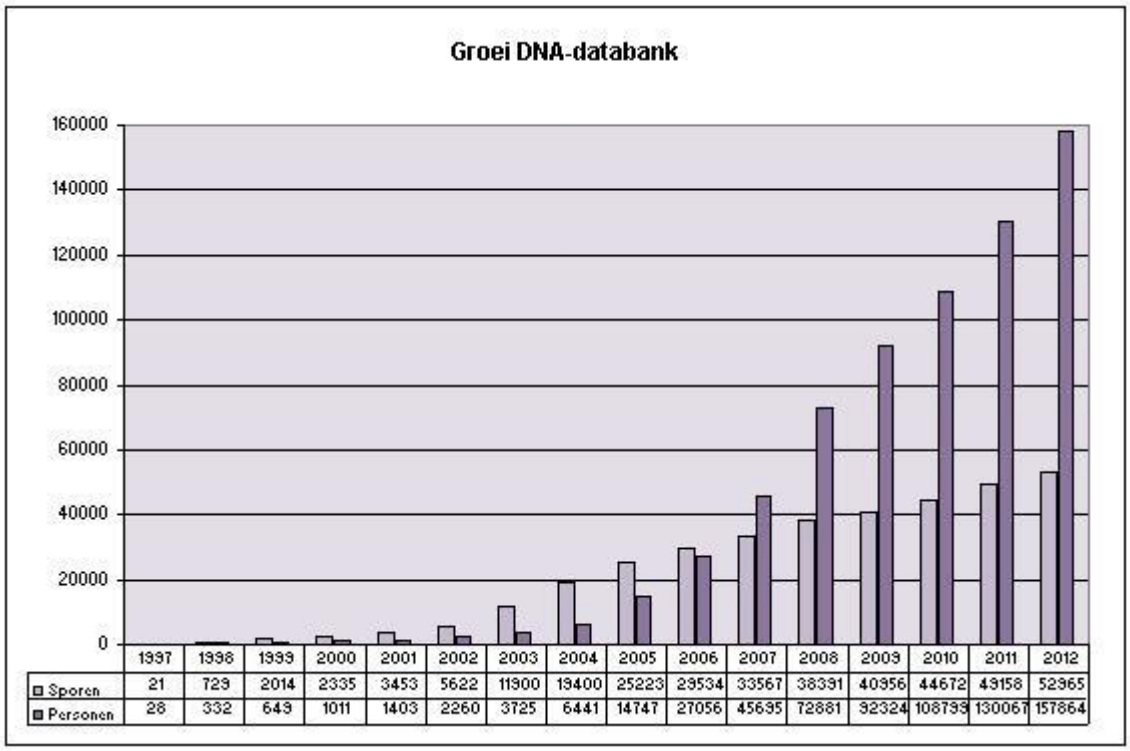
a. is not aware of this offence or, as soon as he is aware of it, immediately takes all measures that can reasonably be required of him for making the data regarding this offence inaccessible;
b. fulfils an order as meant in Art. 125p of the Code of Criminal Procedure.

Yes, as a consequence of the Prüm treaty it is possible for agencies of other Member States to have direct access to the Dutch DNA database, and the database containing license plates for cars. In principle, the Dutch Police authorities also have direct access to the fingerprint databases of a group of EU countries. The reason for the malfunctioning of the matching of these databases is of a technical nature. The systems of matching fingerprints differ from one State to another, and it is rather difficult to align the systems. At this moment an experiment is going between Dutch law enforcement authorities and the district of Wiesbaden in Germany to do searches in each other's fingerprint database.

The Dutch DNA databank is hosted by the Dutch Forensic Institute in Rijswijk. Every trace in the databank goes to all participating countries in the data exchange project. The Netherlands received 255.000 profiles in 2009; 25.000 profiles were sent by the Netherlands. Mr. Van Beek, working at the Dutch Forensic Institute, has stated the following: "At the Dutch Forensic Institute every morning between 6.00 and 7.00 a new copy of the databank is made. All new or changed profiles go automatically to the nine countries who are operational at the moment."[80] Up until now the matching of international profiles resulted in 1735 matches in the Netherlands. About half of these matches were with profiles in Germany. In case of a hit via the matching of DNA profiles, a letter of request has to be sent to the responsible national authority to get further personal information.

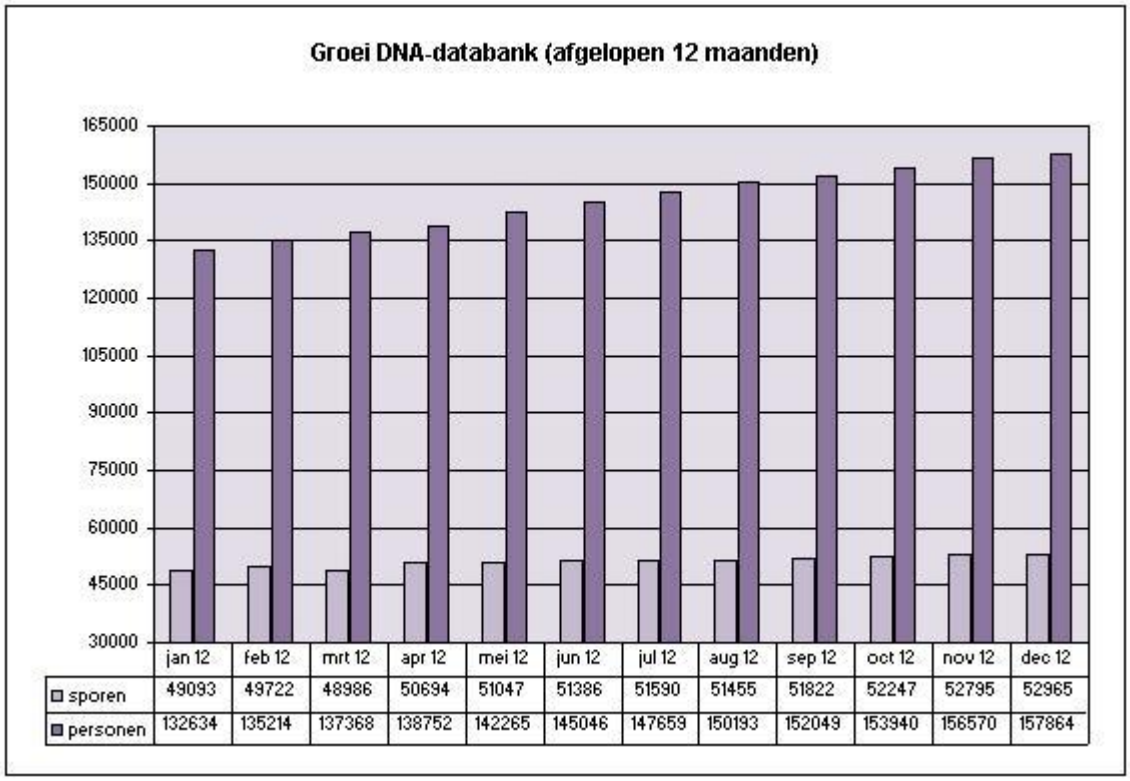
[80] R. Leyen in Blauw, Opsporing, 5 February 2011 – Nr. 3

Growth of the DNA-databank



	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Sporen	21	723	2014	2335	3453	5622	11900	19400	25223	29534	33567	38391	40356	44672	49158	52965
Personen	28	332	649	1011	1403	2260	3725	6441	14747	27056	45635	72881	92324	108793	130067	157864

Growth of the DNA databank in the last 12 months



	jan 12	feb 12	mrt 12	apr 12	mei 12	jun 12	jul 12	aug 12	sep 12	oct 12	nov 12	dec 12
sporen	49093	49722	48986	50694	51047	51386	51590	51455	51822	52247	52795	52965
personen	132634	135214	137368	138752	142265	145046	147659	150193	152049	153940	156570	157864

12. Does your state participate in Interpol/Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions.

Yes, the Netherlands takes part in Europol and Eurojust, which are situated in the Hague. The Netherlands also participates in Interpol. The exchange of information takes place according to the regulations of these organisations.

Chapter 5 Human Rights

E. Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility of your state involved in international cooperations regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human right standards?

Human rights with relevance for the investigations in cybercrime offences are the right to respect for privacy, the right to a free life, and the right to a fair trial. The Cybercrime Convention refers in Article 15 to conditions and safeguards laid down in domestic law, in the European Convention on Human Rights and in the International civil and political rights covenant.

The human right to privacy protects the individual against intrusions which may occur in the fight against cybercrime. The right to privacy is codified in Article 10 of the Dutch Constitution and in Article 8 of the European Convention on Human Rights. In its judgments the ECHR has given a broad definition of private life, namely the physical and psychological integrity of a person.[81] The storing of data relating to the private life of a person amounts to an interference within the meaning of Article 8.[82] The national governments may not interfere in one's private life. Exceptions on this rule may only be in accordance with the law and must be 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[83]

While cybercrimes are committed by individuals and not by states, the human right to privacy does not apply directly. Indirectly, however, it is highly important with regard to the possible impact of cybercrimes. Not the unlawful use of the stored private data by governments is the real danger, as many would believe, but the most threatening is the obtaining of personal data by third parties through hacking or defects in the storage system.

[81] Pretty v. the United Kingdom, n. 2346/02, para.61, ECHR 2002-III.
[82] Leander v. Sweden, 26 March 1987, para.48, Series A no. 116.
[83] Article 8 (2) ECHR.

It seems to me that, in relation to investigations using information technology and large databases, privacy is the human right that is most in danger. However, other human rights have to be mentioned as well. The first one to name is the right to liberty of the person as laid down in Art. 15 subsection 1 of the Dutch Constitution and in Art. 5 of the European Convention on Human Rights. It is often suggested that electronic surveillance, DNA analysis and data matching by government agencies could endanger our freedom in decision making. Another human right that can be named is freedom of expression (Art. 7 of the Dutch Constitution, Art. 10 ECHR), while in relation to criminal investigations email and mobile phone communications are monitored consequently and also the internet is being observed. This could result in a lesser freedom of expression, because people would feel restrained due to all this surveillance.

Another human right that I perceive as relevant for cyber crime investigations is the right to a fair trial as laid down in Art. 6 ECHR. In the Code of Criminal Procedure of the Netherlands there are a lot of new rules concerning for instance searches in computers and computer networks and concealing electronic evidence through the use of encryption. The obligation in laws to require individuals to disclose encryption keys is seen as contrary to the right on a fair trial. In Dutch procedural law the investigation officer may give an order to undo a security measure (Art. 125k par. 1 CCPNL) and may give an order for the decryption of or handing over of a decryption key for encrypted data (Art. 125k, par. 2 CCPNL). These orders cannot be given to a suspect. At the moment this provision does not seem to be contrary to the right on a fair trail. In the letter of the Minister for Justice and Security to the chair of the Parliament of 12th October 2012 that I already mentioned before, the Minister emphasised that research is being done regarding the legal basis for ordering decryption according to Art. 125k CCPNL also to the suspect. The results of this research will be available shortly. At the moment this order can't be given to a suspect.

In the same letter, the Minister states that measures should be introduced to make it possible to penetrate a computer for the wiretapping of confidential communication. According to this letter it is sometimes necessary to install software secretly in the suspects devices to render it possible to encrypt the data or get round the encryption. Looking at these new plans of the Minister, one wonders if this would create tension regarding the admissibility of evidence, and regarding the right to a fair trial.

Article 13 of the Dutch Constitution states that the confidentiality of mail, telephone and telegraph transmissions is inviolable. With regards to transmissions by means of electronic

devices this provision is perceived as too limited. A proposition for an amendment has been drafted. The proposed article is as follows:

Art. 13 (not yet enacted revision) of the Constitution:

1. Everyone is entitled to the privacy of his correspondence and telecommunications.
2. This right may be restricted in cases provided for by statute, if authorized by a court or, in the interest of national safety, by one or more ministers designated by statute.
3. Rules for the protection of the privacy of correspondence and telecommunications are prescribed by statute.

The purpose of the amendment is to extend the scope of the current provision to include all present and future usage of telecommunication. The idea is that an article which does not refer to the method of telecommunication better matches current reality and makes the law future proof. Hence, the proposed article for the Constitution would protect the content of any private telecommunications, notwithstanding the used method or technology.

The Netherlands only work together with other countries in the field of criminal prosecution that respect human rights. Therefore, in case the Dutch authorities receive information from cooperating countries, they will automatically assume that the information has been gathered according to the procedural rules in the providing country and according to human rights standards. Mutual assistance in criminal cases requires mutual trust that the requested information has been retrieved according to the country specific procedural rules and with respect to human rights. Within the European Union this principle of mutual trust is laid down in the so-called Stockholm programme.[84] The Stockholm programme is the road map of the European Union for the cooperation on, inter alia, the field of criminal cooperation. Par 1.2.1 of the Stockholm programme states that mutual trust between the authorities and services in the different member states is the basis for cooperation. All kind of new cooperation measures, as for example the European Arrest Warrant, have their basis in the principle of mutual recognition, which implies mutual trust.

There is no real possibility and opportunity to verify the circumstances under which information is gathered in the providing country. Hence, if the Netherlands receives and uses information from another state, the Dutch State is not accountable if the information was collected in violation with international human right standards.

[84] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF

With regard to fundamental human rights, it is irrelevant where the investigations have been conducted. These fundamental human rights must always be respected. If evidence is gathered in violation with fundamental human rights, this is a procedural defect in the Dutch procedure. In Art. 359a CCPNL the consequences of a procedural defect are given. If a procedural defect is detected, there are tree possibilities. In case of the most flagrant violations the judge may decide that the case is inadmissible. This decision will only be made in very severe cases of human rights violations. The second possibility is that the judge may decide that the information which was gathered wrongfully will not be used as evidence. The third possibility is that the concerning information will be used, but that the punishment will be reduced. The judge will choose for this option if it considers that there has been only a minor violation of human rights.

Chapter 6 Future Developments

> Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions. If not, should the classical rules on mutual assistance be applied (request and answer) and why?

In the Netherlands there is sometimes contact between the police and the judiciary and the accused, victims and witnesses in another country. For example, if a victim asks for compensation for damages. In such cases contact is often needed to inform the respective victim about the right to demand compensation in a Dutch criminal case against the accused. This compensation claim can also be submitted to the court in writing. The presence of the victim at the Court is not required. The aggrieved party may demand compensation by a specific form which has to be sent to the Public Prosecutor, as laid down in Article 51b of the CCPNL. The victim can also submit his claim during the court session. There can be informal contact with the victim about this procedure, for instance by email. The claim cannot be sent by email, though has to be submitted and signed by the aggrieved party using the special form. The victim and other witnesses can be asked to come to the Netherlands for making a statement. However, if a witness refuses to come, the Dutch authorities are out of other options to deal with this. In general, the Dutch judiciary has no instrument to oblige a victim, witness or suspect, who resides in a foreign country, to cooperate, if they do not want to have any contact with the Dutch judiciary and do not want to cooperate with the Netherlands. In these cases it is necessary to sent a letter of request to the authorities where the suspect, victim or witness is living to enforce cooperation.

> Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

There is no legal impediment against court hearings via the screen. The general legal provision which renders it possible to have hearings by means of a videoconference is the law introduced on 1 January 2007. With that law Article 78a CCNL was included in which is laid down that all notices of interrogations incorporated in the Criminal Code or the Criminal

Procedure Code of the Netherlands may take place by means of a videoconference. It is up to the judge to decide on the usage of a videoconference. For making this decision, the judge informs himself about the opinions on the matter of the suspect or his counsel and of the Public Prosecutor.[85]

Court hearings of witnesses via the screen in transnational cases are conducted by the Examining Magistrate of the District Court or of the Court of Appeal. Mutual Legal Requests are often sent to the Netherlands asking for a video conference to hear a witness. The hearing of witnesses by these means of modern technology occurs frequently. According to Art. 552n CCPNL subsection 1 par. A the Public Prosecutor sends a request to hear a witness or an expert by videoconference to the Examining Magistrate. The Examining Magistrate supervises the hearings videoconference in the Netherlands.

At the e-justice site of the European Commission there is an overview of all locations with videoconference facilities in the European Union.[86] At this link there is a list of places in the Netherlands with videoconference equipment.[87] The legal basis of hearings by videoconference of a person who is present in a foreign country is often the Convention of Mutual Assistance in Criminal matters 2000 and the second protocol by this Convention on Mutual Assistance in Criminal matters 2000. The Dutch government has made a declaration when signing the Convention and the Second Protocol concerning the hearing of an accused via a videoconference in the Netherlands. Because of this declaration, the Dutch authorities remain the possibility to refuse a request to hear an accused on this legal basis. The Dutch authorities also use videoconferences for the hearing of witnesses abroad, not only in European countries, but as well in countries such as Australia, the United States and South-Africa.

Although the Dutch government has made a declaration about the hearing of an accused by videoconference in the Netherlands it is possible for the Dutch authorities to ask for a hearing

[85] Art. 78a CCNL

1. Authorization under this Code for hearing, questioning or interrogating persons includes – cases as designated by Order in Council excepted –the hearing, questioning or interrogating by videoconference through a direct image or sound connection between the persons involved.
2. The president of the board, the judge, examining magistrate or official who is in charge of directing the hearing, shall decide whether a videoconference will be used, taking into account the interest of the investigation. Before deciding, the person to be heard or his counsel and in occurring cases the public prosecutor shall be enabled to give their view on the use of videoconference. Further rules in this context may be prescribed by Order in Council.
3. The decision to use videoconference is not subject to separate appeal.

[86] https://e-justice.europa.eu/content_videoconferencing-69-eu-en.do

[87] Unfortunately this list is not complete. For example in 's Hertogenbosch there is the possibility of a videoconference but this city is not in the list

of an accused abroad via videoconference. Other countries often cooperate with these requests. In practice videoconference hearings of accused asked by the Dutch authorities do not occur often.

> Is there any other issue related to information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

In today's society the usage of secured internet sites and email has become common knowledge with regard to governmental services, for example for the submission of tax forms and applications for subsidies. The use of the internet or email could more often be applied in the communication between the Public Prosecutor and the judiciary, and in the official communications between governmental agencies and suspects, victims and witnesses in criminal proceedings. For instance, witnesses and suspects could be summoned to appear in Court by email. Hypothetically, suspects and witnesses would only have to be reached by post as a back-up. This modernising of the means of communication would have great advantages, while digital communication operates faster, and while citizens are themselves more familiar at the moment with this method of communication as with registered post.
If this future development would be realised, it is very important that the safety of the communication is ensured. Documents concerning criminal procedures contain sensitive personal information. Before the digital distribution of these kind of documents in criminal procedures can be realised , it is very important to arrange and guarantee the safety of the system.
In addition, the communication between the judiciary and councillors could take place through a secured and personalised internet website or email. At the Court of Appeal at Den Bosch, preparations are being made for a whole digitalisation of proceedings. In the future, it seems likely that official files will only be distributed digitally to judges and the advocate-general, and no longer in paper. The files which are intended for the bar could also be sent digitally. At the moment this not happens yet in all cases. Especially in cases with extended files the documents are digitalised. At the stage the digitalisation is finalized the usage of paper files during the proceedings in Court could even be omitted.

Final remarks

As stated in the introduction cybercrime is a serious problem for our society. Awareness about the threats and consequences of cybercrime has steadily augmented inside governments and in the media. Fighting cybercrime is not only a concern for the government. Also, for example banks and multi nationals are trying to tackle this problem. In the CPNI, the Centre for protection of the national infrastructure, public and private organisation work together to fight cybercrime.[88] Part of this organisation is the information exchange centre *(Informatieknooppunt*) where information is shared and brought together. This information centre works with the exchange model as illustrated bellow.

Next to this there is the National Cyber Security Centre (NCSC)[89] from the Ministry of Justice. The object of this centre that opened his doors on the 1th of January 2012 is increasing the resilience of Dutch society against cybercrime.

The Public Prosecutors Office gives special attention to the subject. There is a special hotline on cybercrime at which civilians can report cases of child pornography and of radical and

[88] www.cpni.nl

[89] www.ncsc.nl

terroristic statements that have been spotted on the internet. The Public Prosecutors service also started a national hotline on internet fraud. An Electronic Crimes Taskforce has started and also a National Skimming Point. There is a Knowledge and Expertise Centre Cybercrime (*Kennis- en Expertisecentrum*) that gives information advice and training to the Public Prosecutors Office and the police. Within the police a special High Tech Crime Unit of the national police service has been introduced. Also the judiciary has been expanded with a Cybercrime Centre which is located at the court of appeal in The Hague.

In the media there is a lot of attention on the subject. Identity fraud, problems about privacy with digital stored information about persons (for example patients), computer viruses, problems with internet banking, skimming, cyber plague, aspects on cybercrime are almost daily discussed in the media.[90] Commercials are shown on national television pointing out the dangers of the (unsafe) use on the internet. A lot of information is provided to prevent cybercrime. [91] Moreover, on schools attention is paid to the safe use of the internet. After the successful completion of these lessons, they get a diploma "save use of the internet."[92]

What we see in recent years is that a lot of attention is paid on the "real" cybercrime, cybercrime where the internet is used to commit the crime, or where the internet is the object of the crime.

In my opinion the "real" cybercrime gets more and more attention national and internationally. Though, another aspect of the subject is that ICT plays an increasing role in all kind of "old fashion" crimes like fraud, theft, drug trafficking etc. This is a result of the place ICT has in our society as a whole and the way ICT is used between people in general. The social media are more and more important and the use of the internet for communication is booming. While ICT has become very common in our society, criminals as well use these digital ways, for example preparing drugs transactions or robberies. Evidence is more and more not on paper but as data available in a computer. Moreover, in the investigations of the police the social media can play a more important role. The "friends" of a person on facebook (with pictures) give a lot of information of the people he or she is dealing with. Video films of suspects are spread by the public on internet and sometimes this leads to very fasts results.

What I perceive as a problem is that the "normal" police force often still uses old fashion ways of investigating crimes. Requests for a wiretap on a phone and sometimes when a

[90] This link gives an overview: http://www.ru.nl/opleidingen/bachelor/natuur-techniek/informatica/vm/cyber-security/cyber-security-media/
[91] http://www.nederlandveilig.nl/veiliginternetten/
[92] http://diplomaveiliginternet.kennisnet.nl/

smartphone is involved an internet tap. However, a lot of people use ipad's or other tablets or laptops and communication is taking place via a chat using these instruments. Or to say it with a telephone commercial "Who's still calling?".[93] In every day's work of the police the ICT aspect of the preparation or committing of a crime and the possibilities of solving a crime should be more ingrained in daily police practice. Of course there are specialists on cybercrime in high tech units. But this is not enough. My suggestion is that the ICT aspect of crime should be more important in the education and daily practice of all policemen.

These observations are as well applicable for international cooperation. In big cases for example of a botnet (as described in the introduction) or international fraud there is an intensive cooperation between the countries. There is worldwide working together to solve these kinds of cases. The botnet case gives a good example of this worldwide working together. After the police did an investigation on the server the suspect who was an Armenian citizen was arrested on the airport of Jerevan, Armenia. The Dutch authorities asked for this arrest. The Dutch police was already looking for him for weeks and worked together with the Russian and Armenian police to trace him. During the investigations of the Dutch police the suspect tried to get back the control on the botnet and did an attack on his hosting provider with 22.000 infected computers. This attack was tackled by cutting down his server situated in Paris from the internet.[94] The arrested person was convicted in Armenia on 22 May 2012 to a sentence of four years imprisonment.

In these big cases the high tech crime units of the several countries are working together in a proper way. Eurojust and Europol can play an important role in coordinating cooperation. As discussed in chapter four the establishment of Joint Investigation teams is a good tool for the international cooperation in a fast and efficient way.

Though, in the solving of "normal" cases of cross boarder crime for example drug trafficking or human trafficking the working together is often still focusing on wiretaps on phones and surveillance. Cross boarding internet wiretapping is not often asked by the Netherlands or asked from the Netherlands. The international searching and seizing of data and the search of computers is not yet a very common instrument in tackling cross border crime. Police, the Public Prosecutors Office and the investigation judges could use these instruments more, while it is certain that the criminals are changing or have changed their way of communications. A search in the computer of a criminal can give a lot of information,

[93] http://www.youtube.com/watch?v=14RlmlvajGE
[94] http://nos.nl/audio/193901-landelijk-parket-over-aanhouding-verdachte-leider-botnet.html

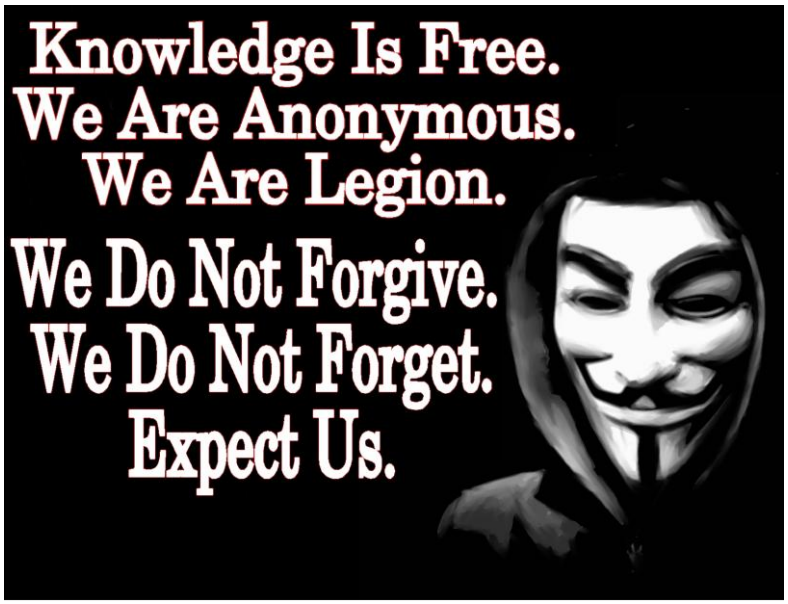
especially when not only the existing files but also the unallocated files with the deleted messages are investigated.
In international cooperation more evolved instruments and the use of digital communications in the cooperation between law enforcement authorities offers substantial gains. Digital communications between law enforcement authorities could result in more efficiency and a speed-up of the cooperation. Paper files and letters sent by post could be replaced by digital files and requests sent by email. While it is not yet possible to intercept communications through for example "skype", this medium could be used to communicate with our counterparts.
The working together worldwide is also very important in order to realise the necessary Notice and Take Down procedures and to remove for example child pornography more definitely from the internet.

The first aspect I wanted to emphasize is the importance of the working together on cybercrime cases. The second – and as important aspect – is the aspect of human rights. There is cybercrime and cybercrime. A person can hack a computer to get money of a bank or secrets of a company, other people are hacking to get information for example from the government or the army. Not because they want to blackmail people, but because they are critical towards the functioning of the policy, the government, or banks or the army. They want to denounce certain things or let the people now "the truth" about events that have taken place. A group like "Anonymous" claims their actions serve the freedom of humanity.[95] According to them hacking is as a tool.[96]
The goal of a hacker may be the gathering of information to expose for example a failure of the government. In Dutch jurisprudence there is a case about hacking the mailbox of Mr. J. de Vries, the state secretary of the Ministry of Defence.[97] The person who was prosecuted was a journalist. He stated that the reason for his action was that he wanted to show that it was easy to hack into the computer of the State Secretary. He wanted to emphasize that the security of the systems was not sufficient. The court convicted the journalist involved. The court considered that the journalist worked together with a person who not only entered the mailbox but also manipulated the system with the effect that the mails were automatically sent

[95] http://www.youtube.com/watch?v=SNLPXvWpP4o.
[96] http://www.youtube.com/watch?v=2K0E8sMDJ9M.
[97] District Court of The Hague 23 November 2009, LNJ BK 4065 (Hacking Mailbox Jack de Vries).

to the hacker. The Court considered that this was unnecessary for the purpose of the journalist.
In cases like this hackers consider themselves sometimes as “revolutionist”. Human rights and especially freedom of speech can be an important issue in cases like this.
The same problem can occur in cases of “notice of take down” order from internet sites. The closing down of sites can in some cases be considered as a form of censorship. In the implementation of orders of another country this may be an issue.

For the future the challenge will remain to intensify international cooperation and cooperate more efficiently to fight all kinds of cybercrime. The struggle against new possibilities for cybercrime and the developments to fight against it by law enforcement authorities world wide will continue. In this struggle the protection of human rights, as the right on privacy and the right on a fair trail, have to be respected. The specific content of these rights with regard to cyber crime offences will have to crystallize more in the judicial practice in the future.



Bibliography

S.W. Brenner and B.J. Koops, "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law* 2004, p. 1-30.

Europol, *'Theat assessment: Internet facilitated Crime'*, iOCTA, Den Haag 7 January 2011, file number 253-264.

Faber, W., Mostert, S. Faber, J. en Vrolijk, N., *'Phishing, kinderporno en Advance-Fee Internet Fraud: hypothesen van cybercrime en haar daders'*, rechearch on behalf of WODC and NICC, August 2010.

Ferreira Pires, L., *'Wat is Cloud computing?'*, in: Computerrecht, tijdschrift voor informatica, telecommunicatie en recht, afl. 3, 2011, p. 104.

S.L. Gellarts en C.M. Jobse, *''Inleiding ICT en recht''*, especially chapter, p. 156-176

Hesseling, R., *'Slachtofferschap van cybercrime'*, : Secondant, nr. 5, October 2010.

M. Hildebrandt en M.E. Koning, "Universele handhavingsjurisdictie in cyberspace? Van computer- naar cybercriminaliteit", *Strafblad* 2012 (3).

Hulst, R.C. van der en Neve, R.J.M., *'High Tech Crime, soorten criminaliteit en hun daders'*, WODC, Den Haag, Boom Juridische Uitgevers: 2008.

Leukfeldt, E.R., Domenie, M.M.L. en Stol, W.Ph., *'Verkenning Cybercrime in Nederland 2009'*, Den Haag, Boom Juridische Uitgevers 2010.

H.W.K. Kaspersen, "Bestrijding van cybercrime en de noodzaak van internationale regelingen", *Justitiële Verkenningen* 2004, p. 58-75

A.H. Klip en A.S. Massa, "*Communicerende grondslagen van extraterritoriale rechtsmacht''* (research on behalf of WODC), p.97-101

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

Koops, B.-J., *'Strafrecht en ICT, Monografieën Recht en Informatietechnologie'*, Den Haag, 2007.

Koops, B.-J., '*Cybercrime legislation in the Netherlands'*, Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes', feb 2010.

Koops, B.-J., *'Tijd voor Computercriminaliteit III'*, in: Nederlands Juristen Blad 2010, p. 1982 e.v.

Koops, B.-J., *'Digitale grondrechten en de Staatscommissie: op zoek naar de kern'*, in: Tijdschrift voor constitutioneel recht, 2011, vol. 2, nr. 2, p.168-185

Koops, B.-J., *'The internet and its opportunities for cybercrime'*, Tilburg Law School Legal Studies Research Paper Series, no. 09/2011

Koops B.J., (ed.), *''Strafrecht en ICT''*, Second edition, SDU publishers, 2007.

Koops B.J. and Brenner S.W. (eds.), *''Cybercrime and Jurisdiction, a global survey''* TMC Asser, 2006.

Luchtman, J.J. M. Transnationale rechtshandhaving in de EU en het ne-bis – in –idem beginsel, SEW, Tijdschrift voor Europees en Economisch recht, June 2011

Nationaal Cyber Security Centrum - Ministerie van Veiligheid en Justitie, *''Cybercrime - van herkenning tot aangifte''*.

Nationaal Coördinator Terrorismebestrijding, *'Jihadisten en het internet'*, Koninklijke De Swart, April 2010.

Oerlemans, J.J., *'Het concept wetsvoorstel versterking bestrijding computercriminaliteit nader bezien'*, in: Tijdschrift voor Internetrecht, nr. 5 oktober 2010, p. 148 e.v.

Oerlemans, J.J. en Koops, B.-J., *'Hoge Raad bewijst een slechte dienst in high tech crimezaak over botnets'*, in: NJB 2011, p. 914 e.v.

Schellekens, M, *''Aansprakelijkheid van Internetaanbieders''* SDU publishers, 2001.
Schermer, B.W., *'High Tech Crime en ambient intelligence'*, in: Computerrecht, tijdschrift voor informatica, telecommunicatie en recht, afl. 6, 2010, p. 283-287.
Wilsem, J. van, '*Digitale en traditionele bedreiging vergeleken, Een studie naar risicofactoren van slachtofferschap'*, in: Tijdschrift voor Criminologie 2010 (52) 1.
Wiemans, F.P.E., 'Onderzoek van gegevens in geautomatiseerde werken', Nijmegen, Wolf Legal Publishers, 2004. (diss.)
Zoontjens, P. *''Fundamentele rechten in een ICT-omgeving*", in Recht en Informatietechnologie - Handboek voor rechtspraktijk en beleid
Zwenne, G.-J., *'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren'*, in: Tijdschrift voor Internetrecht, nr. 1, February 2011.

Justitiële Verkenningen 'Cybercrime', December 2004 (jrg. 30, nr. 8)
Justitiële Verkenningen 'Veiligheid in cyberspace', March 2012 (jrg. 38, nr. 1)
Justitiële Verkenningen, 'Tappen en infiltreren', May 2012 (jrg. 38, nr. 3)
Wetenschappelijk onderzoek en documentatie centrum (WODC) (Scientific Research and Documentation Centre) 'High Tech Crime, soorten criminaliteit en hun daders, 2008 (nr. 264)
WODC report Onderzoek 'Phishing, kinderporno en advance-fee internet fraud', 2010
WODC report Onderzoek en beleid, 'Het gebruik van de telefoon- en internettap in de opsporing, 2012 (nr. 304)

Links on the World Wide Web

www.rijksoverheid.nl/onderwerpen/ict
www.meldpuntcybercrime.nl
www.ncsc.nl (National Cyber Security Centrum)
www.cpni.nl (Centre for Protection of the National Infrastructure)
www.eurojust.eu
www.europol.eu
www.security.nl
www.webwereld.nl
www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (Council of Europe Project on Cybercrime)
www.justice.gov/criminal/cybercrime (Computer Crime & Intellectual Property Section van de US Department of Justice)
www.fbi.gov/cyberinvest/cyberhome.htm (FBI Cyber Investigations)

Articles of the Dutch penal Code

derived from KRIS Kenniscentrum Rechtshulp in Strafzaken (Knowledge Centre Mutual Assistance in Criminal Cases)

Article 45 CCNL

1. An attempt to commit a criminal offence will be punishable if the intention of the perpetrator has manifested itself in the first act of the commission of the offence.

2. In the case of an attempt, the maximum term of the principal penalties imposed for the offence will be reduced by one third.

3. If the criminal offence is one for which the punishment is life imprisonment, a prison sentence of a term not exceeding twenty years will be imposed.

4. The additional punishments for an attempt to commit a criminal offence will be the same as for the completed criminal offence.

Article 46 CCNL

1. The preparation of a criminal offence, on which a term of imprisonment of eight years or more has been imposed according to its statutory description, will be punishable if the perpetrator deliberately acquires, manufactures, imports, forwards, exports or keeps in his possession objects, substances, data carriers, rooms or means of transport which are intended to be used for the commission of this criminal offence.

2. In cases which concern the preparation of a criminal offence, the maximum term of the principal penalties imposed for the criminal offence will be reduced by one half.

3. If the criminal offence is one for which the punishment is life imprisonment, a prison sentence of a term not exceeding fifteen years will be imposed.

4. The additional punishments for the preparation of a criminal offence will be the same as those of the completed criminal offence.

5. Objects are understood to mean all objects and all property rights.

Article 47 CCNL

1. The following persons are liable for punishment as principals in a criminal offence:
   (1) those who commit the criminal offence, either personally or jointly with another or others, or who cause another or others to aid in the commission of the criminal offence;
   (2) those who, by means of gifts, promises, abuse of authority, use of violence, threat or deception or providing opportunity, means or information, intentionally solicit the commission of the criminal offence.
2. With regard to the last category, only those actions intentionally solicited by them, and their consequences, are to be taken into consideration

Article 48 CCNL

The following persons are liable for punishment as accessories to a serious offence:
(1) those who intentionally assist during the commission of the serious offence;
(2) those who intentionally provide opportunity, means or information to aid in the commission of the serious offence.

Article 83a CCNL

A terrorist purpose is understood to mean the intention of instilling profound fear in (part of) a country's population, unlawfully forcing a government or international organisation to do, refrain from doing or tolerate something, or seriously disrupting or destroying the fundamental political, constitutional, economic or social structures of a country or international organisation.

Article 96 CCNL

1. The conspiracy to commit any of the criminal offences specified in Articles 92-95a will be punishable by a prison sentence of a term not exceeding ten years or a fine of the fifth category.

2. The same prison sentence applies to any person who – with the intention of preparing or promoting the criminal offences specified in any of the Articles 92-95a:

1°. seeks to induce another person to commit this criminal offence, cause this criminal offence to be committed, act as a co-perpetrator, be of assistance thereto or provide the opportunity, means or information to this end;
2°. seeks to provide himself or another person with the opportunity, means or information to commit the criminal offence;
3°. has objects available which he knows are intended for the commission of the criminal offence;
4°. is preparing or retaining plans for the commission of the criminal offence, which plans are intended to be communicated to others;
5°. tries to obstruct, hinder or prevent any government measure which seeks to prevent or suppress the commission of the criminal offence.

Article 138ab CCNL

1. A prison sentence of a term not exceeding one year, or a fine of the fourth category, will be imposed on any person – being guilty of unlawful entry with respect to automated information – who deliberately and unlawfully enters or accesses a computer facility or automated information system, or part thereof. Such an entry will be deemed to have occurred if the access to the information is obtained:

a. by breaching security;
b. by a technical intervention;
c. by means of false signals or a false key, or
d. by taking on a false identity.

2. A prison sentence of a term not exceeding four years, or a fine of the fourth category, will be imposed on an unlawful entry into a computer system if the perpetrator – on his own behalf or on behalf of others – subsequently copies, taps or records any stored, processed or transferred data by means of the automated information system to which he unlawfully gained access.

3. A prison sentence of a term not exceeding four years, or a fine of the fourth category, will be imposed if the unlawful entry into a computer system is committed through the intervention of a public telecommunication network, and if the perpetrator subsequently:

a. uses the automated system's processing capacity to illegally obtain profits or advantages for himself or other persons, or
b. gains access to the automated information system of a third party through the intervention of the automated system to which he previously

Article 161sexties CCNL

1. Any person who deliberately destroys, damages, renders unusable, or disrupts the functioning or operation of any automated information system, computer facility or telecommunication facility, or any person who frustrates a safety measure taken with regard to such facility, will be punishable by:

    1°. a prison sentence of a term not exceeding one year or a fine of the fifth category, if this creates an illegal disruption or complication of the storage, processing or transfer of data for public purposes, a disruption in a public telecommunication network, or a disruption in the provision of a public telecommunication service;
    2°. a prison sentence of a term not exceeding six years or a fine of the fifth category, if this creates a general danger to property or the provision of services;
    3°. a prison sentence of a term not exceeding nine years or a fine of the fifth category, if this creates danger to the life of another person;
    4°. a prison sentence of a term not exceeding fifteen years or a fine of the fifth category, if this creates danger to the life of another person and the offence causes the death of another person;

2. A prison sentence not exceeding one year or a fine of the fifth category will be imposed on any person who – with the intention of committing a criminal offence as specified in the first paragraph:

    a. manufactures, sells, acquires, imports, distributes, provides in any other way, or keeps in his possession a technical aid which has been rendered predominantly suitable or designed to commit such a criminal offence, or
    b. sells, acquires, distributes, provides in any other way or keeps in his possession a computer password, access code or similar data by means of which access can be obtained to an automated facility or part thereof.

Article 161septies CCNL

Any person found to be responsible for destroying, damaging or rendering unusable any automated information system or computer facility or telecommunication facility, disrupting the functioning or operation of such facility, or frustrating any safety measure taken with regard to such facility, will be punishable by:

1°. a prison sentence of a term not exceeding six months or a fine of the fourth category, if this creates a disruption or complication of the storage, processing or transfer of data for public purposes, a disruption in a public telecommunication network, or a disruption in the provision of a public telecommunication service, or a general danger to property or the provision of services;
2°. a prison sentence of a term not exceeding one year or a fine of the fourth category, if this creates danger to the life of another person;
3°. a prison sentence of a term not exceeding two years or a fine of the fourth category, if the offence causes the death of another person.

Article 232 CCNL

1. Any person who deliberately forges or falsifies a cash card, credit card or any other card or carrier of identity information available to the public for making or obtaining payments or other goods/services in an automated fashion – such with the intent of deriving benefits from this for himself or other persons – will be punishable by a prison sentence of a term not exceeding six years or a fine of the fifth category.

2. The same sentence will be imposed on any person who deliberately uses the false or forged card as if it were genuine and non-forged, or who deliberately delivers, keeps in possession, receives, acquires, transports, sells or transfers such a card whilst he knows, or could reasonably have been expected to have known, that this card is intended to be used as such.

Article 350a CCNL

1. Any person, who deliberately and illegally alters, erases, renders unusable or inaccessible any data stored, processed or transferred by means of an automated facility or a means of telecommunication, or who adds other data to such existing data, will be punishable by a prison sentence of a term not

exceeding two years or a fine of the fourth category.

2. Any person who commits the offence referred to in the first paragraph after having gained illegal access to an automated facility through the intervention of a public telecommunication network and who causes serious damage to the existing data in the process, will be punishable by a prison sentence of a term not exceeding four years or a fine of the fourth category.

3. Any person who deliberately and illegally makes available or distributes data which are intended to inflict damage on an automated facility, will be punishable by a prison sentence of a term not exceeding four years or a fine of the fifth category.

4. Any person who commits the criminal offence referred to in the third paragraph with the intention of limiting the damage resulting from such data will not be punishable.

Article 350b CCNL

1. Any person found guilty of illegally altering, erasing, rendering unusable or inaccessible data which are stored, processed or transferred by means of an automated facility or by telecommunication, or adding other data to such existing data, will be punishable by a prison sentence or detention period of a term not exceeding one month or a fine of the second category if this creates serious damage to such existing data.

2. Any person found guilty of deliberately and illegally making available or distributing data which are intended to inflict damage on an automated facility, will be punishable by a prison sentence or detention period of a term not exceeding one month or a fine of the second category.

Article 351 CCNL

Any person who deliberately and illegally destroys, damages, renders unusable or inaccessible, or mislays railway works, electricity works, automated or telecommunication facilities, water-retaining or water-discharging works, gas mains, waterworks or any sewer systems in public use, or property or facility used for national defence, will be punishable by a prison sentence of a term not exceeding three years or a fine of the fourth category.