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

FINNLAND*

1. General

In Finland, there has so far been no need for a separate cybercrime law. Cyber- offences are regulated widespread in different chapters (28, 34, 35, 36 and 38) of the Penal code (PC). [1] The protection of both information- and administration system have been given an independent position as an object of legal protection by placing all information- and communication crimes under chapter 38 in the PC.[2] The last mentioned chapter on information crimes regulates *interference with communications* (5-7 §), *interference in a computer system* (7a-b §), *computer break-in* (8- 8a §), *offence involving an illicit device for accessing protected Services* (8b §) and *Data protection offence* (9 §). The legislative technique shows, that the idea has both been to edit existing regulations to reflect new developments and also to create new provisions. In the year 2007, Finland amended a number of the PC's provisions on cyber offences to match up to the Council of Europe Convention on Cybercrime (CCC).

The PC does not give one clear definition of a cybercrime. In Finland a cybercrime is generally understood as a crime that has as object, tool or place of offence the computer system.[3] It could also be said that *'an information technology crime is an offence that is directed against, utilizes, or set against the data processing system with its devices, and that the commission and/or procedural handling of which requires specific knowledge of information technology*'.[4] The object of the crime is usually defined *data* (for example in the provision of interference in a computer system) or *information* (computer break-in). The criminal conduct (*actus reus*) has no typical definition, both description of act and consequence is used (like in the offence of computer fraud), or *intention* (unauthorized use). The general part of the PC makes no difference between cybercrimes and traditional crimes, meaning that the general part of the criminal law (like questions on criminal liability) applies to cybercrimes in its all extent. The most pure cybercrimes (crimes that can't be committed without the computer system) are regulated under the PC's chapter 38 as *data offences*.

---

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

[1] An unofficial translation of the Finnish Penal Code (1889/39) is accessible at the website of Ministry of Justice: http://www.finlex.fi/pdf/saadkaan/E8890039.PDF. The provisions in the chapters mentioned above are Unauthorized use (28:7), Criminal mischeaf (34:1), endangerment of data processing (34:9 a), possession of a data system offence device (34:9b), Criminal damage (35:1) and Computer fraud (36:1.2).

[2] See the Government bill 94/1993, pp. 133.

[3] See Lehtimaja, Lauri: *Eurooppalaisesta atk- rikospolitiikasta* [European computercrime policy].Teoksessa rikosoikeudellisia kirjoitelmia VI Rikosoikeuden juhlavuonna 1989 (toim. Raimo Lahti), Vammala, Suomalaisen Lakimiesyhdistyksen julkaisuja 1989, pp. 260.

[4] See Pihlajamäki, Antti: The protection of data processing under criminal law, an English summary (pp. 285-290) in the doctoral thesis *Tietojenkäsittelyrauhan rikosoikeudellinen suoja, Datarikoksia koskeva sääntely Suomen rikoslaissa*. Gummerus, Jyväskylä 2004. The definition on cybercrime, see the English summary on pp. 286. In Finland it is foremost Pihlajamäki who has written about cybercrimes- he also wrote about the Finnish cybercrime offences in an earlier report of AIDP: see Pihlajamäki, Antti: *Computer Crimes and Other Crimes against information Technology in Finland*, Revue Internale de Droit Pénal (1993), Toulouse, Eres: Computer crime and other crimes against information technology, pp. 275-289.

The certain vagueness of the definitions on cybercrime in law could partly be explained by the high rate of the technological progress, which is so fast, that it is impossible to follow this pace of development by statutory provisions. This has led to provisions of quite general nature with forward looking statements, such as "*comparable to those in any other way*". Generic expressions of penal provisions are though problematic with respect to the principle of legality and especially to its component, the requirement of accuracy.[5] The principle of legality is to be more discussed in part three (3).

Although the general part of the PC applies to cybercrimes, it is though clear, that cybercrimes differ from traditional crimes in many ways: they are committed in an environment that is different from traditional crimes (the so called virtual sphere, therefore the exact definition of the place where the offence was committed often causes confusion) with different 'tools' (information technology) than traditional crimes. The effect of the crime might also be widespread (extending to more than one state) and the effect is usually real-timed. The object of the cybercrime is information and knowledge, which also differ from the object of a traditional crime (like possessions). The cybercrimes are more easily to commit anonymously than traditional crimes[6], which also means that they are more difficult to control. These crimes often result in only electronic evidence. In order to foresee the new coming appearance forms of cybercrimes it is necessary to have knowledge of different forms of all possible future technological development. This places new challenges for both the legislative and the executing force. In Finland, there has actually not been discussion about whether or not cybercrimes should be regulated separately from the PC.

On the other hand, there are also reasonable explications why the general part of the criminal law applies on cybercrimes like all traditional crimes: cybercrimes resemble traditional crimes in many ways. Criminal liability for cybercrime is not limited to particular groups of perpetrators or victims. Almost anybody with knowledge of information technology can commit a cybercrime. The law does not provide sanctions especially for targeting cyber criminals.[7] Provisions on corporate criminal liability apply to most of cyber offences: corporate liability is not applied, if the provision does not explicit say so.[8] Also attempts to the majority of cybercrimes are punishable.[9]

In Finland the requirements for criminal liability are presented in three steps. Firstly, the act must fulfill the definitional elements prescribed by the law (lack of any of these is a ground for precluding liability). Secondly, the act must be wrongful (a justification ground precludes liability). Thirdly, the actor has to show the required culpability (if there

[5] TM 2004:14, pp. 11-12 (a work-group-report by the computer network work group 2004:14, pp. 12- 14). The report can be accessed in Finnish at the webpage of Ministry of Justice: http://www.om.fi/20145.htm

[6] Lehtimaja, Lauri: *Tietokonerikollisuuteen liittyviä oikeudellisia ilmiöitä* [Phenomenons related to computer- crimes], Helsinki, Defensor Legis 1983, pp. 56.

[7] Here could be noticed, that a foreign who has been found guilty of an offence carrying a maximum sentence of imprisonment for a year or more, can be deported from Finland (Ailiens Act (2004/301) 149 §). For example interference in a computer system (PC 38:7a) has a maximum sentence of two years.

[8] The provisions on corporate criminal liability apply to computer break-in, aggravated computer break-in, interference in a computer system and aggravated interference in a computer system (PC 38:12).

[9] Interference with communications (PC 5-7 §), interference in a computer system (PC 7a-b §) and computer break-in (PC 8- 8a §) and copyright offence (PC 49:1).

exists an excusing ground the liability is precluded).[10] The criminal liability for cybercrimes relies on intentional acts. Unless otherwise provided, an act referred to in the Penal Code is punishable only as an intentional act (PC 3:5.2). The PC states, that a perpetrator has intentionally caused the consequence described in the statutory definition if the causing of the consequence was the perpetrator's purpose or he or she had considered the consequence as a certain or quite probable result of his or her actions. A consequence has also been intentionally caused if the perpetrator has considered it as certainly connected with the consequence that he or she has aimed for (PC 3:6). The lowest degree on intention is enough: i.e. it is a question of *probability- intent*. An overweighing probability (over 50 %) is enough to estimate the act intentional.[11]

2. The Finnish substantial provisions

The first cybercrime offences were introduces into the Finnish PC in the year 1991. Some provisions were added in the year 1995 that was followed by a couple of separate amendments, so that the Finnish provisions conformed to the 1989 Recommendation of the Council of Europe.[12] In the year 2007, Finland amended a number of the PC's provisions on cyber offences to match up to the CCC. The CCC on cybercrime is the most comprehensive instrument that addresses cybercrime.[13]

The following presentation of some of the Finnish substantial provisions on cybercrimes follows the CCC's structuration, in the order of (i) Offences against the confidentiality, integrity and availability of computer data and systems (title 1), Computer-related offences (title 2), Content-related offences (title 3), Offences related to infringements of copyright and related rights (title 4). Another option how to compartmentalize cybercrimes could have been the one created by Antti Pihlajamäki, who divided the IT- crimes into data- and information crimes. Data crimes included offences which could be committed through the manipulation of stored computer data: unauthorized access, computer espionage, unauthorized use, computer-related forgery, computer-related fraud, means of payment fraud, damage to data, and data processing endangerment. The common feature of these data crimes were that they every data crime disturbed at least of the elements (confidentiality, integrity, availability) of the data processing peace (*pax computationis*).[14] The presentation is though more easily to follow when the provisions are connected to the articles of CCC.

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

Illegal access (CCC, article 2) is criminalized as *Computer break-in* (PC 38:8). The provision is as introduced:

---

[10] See Lappi-Seppälä, Tapio, pp. 217 in *Criminal Law Theory in Transition: Finnish and Comparative Perspectives.* Edited by Raimo Lahti and Kimmo Nuotio. Finnish Lawyers' publishing company, Helsinki 1992.

[11] About Finnish intent in Nordic connection: see Matikkala, Jussi: *Nordic Intent* in Kimmo Nuotio (ed.,. Festschrift in honour of Raimo Lahti, Edited by Kimmo Nuotio, Helsinki, Forum Iuris 2007, pp. 221- 234. The definition of intent has recently been a central topic in the Supreme court's case KKO:2012:66. In Finland it is illegal to intentionally buy sexual services from subjects to pairing or human traffic. In the Supreme court's case the intention behind such an act was issued.

[12] Pihlajamäki 2004, pp. 286.

[13] On analysis of the Convention on Cybercrime, see Csonka, Peter: 'The council of Europe's convention on cybercrime and other European initiatives' in Revue Internale de Droit Pénal, *Cybercrime* (vol. 77), Ramonville Sainte Agne, Eres, pp. 482- 489.

[14] Pihlajamäki 2004, pp. 285- 286.

> (1) A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most one year.
>
> (2) Also a person who, without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system referred to in subsection 1, shall be sentenced for a computer break-in.
>
> (3) An attempt is punishable.
>
> (4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

If the information captured by computer break-in is later used, this is regarded as an offence under unauthorized use (PC 28:7-9)[15] or criminal damage (PC 35:1-3). Data interference (CCC, article 4) is criminalized as *criminal damage* (PC 35:1.2). The provision of criminal damage states, that a person who, in order to cause damage to another, unlawfully destroys, defaces, conceals or hides data recorded on an information device or other recording shall be sentenced for criminal damage (also an attempt is punishable).

Usually criminalization that protect the confidentially of information requires, that the information is protected: for example the applicability of the offence breaking into a computer system (PC 38:8.1) requires, that the protection of the computer system has been broken down. [16] Without this intention, the applicable provision could be another one, for example unauthorized use (PC 28:7).[17] This also means that there are usually no requirements for ICT users to protect themselves with antivirus software.[18] When it comes to computer viruses it can be noticed, that the person who receives and opens an adverse annex, is not be held responsible for negligence or reckless behavior, due to the fact that the malware messages are carefully formulated.[19]

System interference (CCC, article 5) is criminalized as *interference in a computer system*. The Finnish provision is designed to protect information systems from virus and denial-of-service attacks (PC 38:7a). The provision states, that a person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of a computer system or causes serious interference in it shall be sentenced, unless an equally or more severe punishment is decreed elsewhere in law for it, for interference in a computer system to a fine or to imprisonment for at most two years. Also

---

[15] The provision of unauthorized use states, that A person who without authorization uses the movable property or the non-movable machine or equipment of another shall be sentenced for unauthorized use to a fine or to imprisonment for at most one year. Also an attempt is punishable.

[16] Rautio, Ilkka: RL 38 luku tieto- ja viestintärikokset, pp. 1028, teoksessa Lappi- Seppälä, T. ym., *Rikosoikeus- oikeuden perusteokset* [the basic works on criminal law](3. painos, 2008).

[17] A person who without authorization uses the movable property or the non-movable machine or equipment of another shall be sentenced for unauthorized use to a fine or to imprisonment for at most one year. Also an attempt is punishable.

[18] In order to get practical information on the cybercrime legislation the writer has interviewed by email head inspector Kajantie from the Finnish National Bureau of Investigation (KRP). When hereinafter referred to this interview, it's cited 'email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi'.

[19] This information is accessible in Finnish at the webpage of the Police: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/4E2E3CA9B18035C8C22579E80046AC48?opendocument).

an attempt is punishable. The provision supplements the offence of interference with communications (PC 38:5-7). According to the last mentioned provision, a person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for *interference with communications* to a fine or to imprisonment for at most two years. Also an attempt is punishable.

The object of the attack is the activity of the computer *system* (and not the data itself). The section also requires that the act is unlawful and intentional, done in the purpose of damaging or harming the system (increased intent and unlawfulness). The computer system has also to be inhibited or disrupted by the attack.[20] The attack can be put into force by entering, transferring, damaging or altering data. One way on entering data without damaging it, is to overload the system. The most common way to violate this offence is to transfer the system with a computer virus that destroys or alters data.[21] According to a quite recent national survey, several corporations working in Finland lack the knowledge of that their computer system has been the target of an attack.[22]

Misuse of devices, such as programs for computer break-in, passwords or computer viruses (CCC, article 6) is criminalized as *Endangerment of data processing* (PC 34:9a):

> A person who, in order to impede or cause harm to data processing or the functioning or security of a data system or telecommunications system,
>
> (1) imports, manufactures, sells or otherwise disseminates or makes available
>
> (a) a device or computer program or set of programming instructions designed or altered to endanger or cause harm to data processing or the functioning of a data system or telecommunications system or to break or disable the technical security of electronic communications or the security of a data system, or
>
> (b) a password, access code or other corresponding information, or
>
> (2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph
>
> (1), shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for *endangerment of data processing* to a fine or to imprisonment for at most two years.

The Finnish provision covers all the devices mentioned in CCC's article 6.

2. Computer-related offences

Computer-related forgery (CCC, article 7), i.o.w. forgery of digitally stored data, is criminalized under the Penal code's Forgery offence (33:1, definitions see 36:6). The basic classification of the crime forgery states, that *a person who prepares a false document or other item or falsifies such a document or item in order for it to be used as misleading evidence or uses a false or falsified item as misleading evidence shall be sentenced for forgery to a fine*

---

[20] See the Government bill 153/2006, pp. 65. The attack is no more considered as unlawful if the object of the attack gives permission to the attack.

[21] Rautio 2008, pp. 1043. An attack against IT system can also be regarded as interference with communications (38:5). According to Kajantie, the both provisions applied to attacks against IT systems are well formulated and functioning good (email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi).

[22] National Research Institute of Legal Policy, the article is accessible in Finnish language: http://www.optula.om.fi/Etusivu/Julkaisut/1302672838628.

or imprisonment for at most two years. Also an attempt is punishable. The aim of the provision is to protect the authenticity of items. [23]

Forgery can be put into effect in three different ways: by producing a new document, by falsifying an already existing document or by using either of these. Traditionally a signature proves the authenticity of a document. When it comes to digitally stored data, the signature is usually replaced with an identification seal. Usually if the file is changed, the identity of the object also changes and the object loses its value as evidence.[24]

Digitally stored data in programming language can be used as misleading evidence. Data consists of information that gives a meaning to the content of it (facts, information, concepts, programs by witch the data performs its functions). A recording is an entity formed by the data with the information. Only this entity is protected as evidence.[25] The Supreme court of Finland has newly stated (judgment KKO:2012:54) that the mobile IMEI- code (International Mobile Equipment Identity) could be the subject of forgery[26], if it is converted to another code (for example with a Flasher Box – device) and used as a evidence in legally significant connections.[27]

Computer-related fraud (CCC, article 8), meaning manipulation of digitally stored data, is criminalized as *computer fraud* under PC's 36 chapter, section 1 (2). The provision is as introduced:

> (1) A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud to a fine or to imprisonment for at most two years.
> (2) *Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud.*
> (3) An attempt is punishable.

The elements of the crime computer fraud can be divided in to three characteristics: intention, act and consequence. The offence has to be committed in the intention of gaining or causing harm. The act can be committed in two different ways: either by entering false information in the processing devise (for example using another person's username and password) or by manipulating the digitally stored data. The offence requires that there must be causality between the act and the consequence. The consequence has to be both distortion of the result of the data processing (the computer could for example delete data from the register or combine information wrong) and causing

---

[23] The law defines an item as a document and its facsimile, a mark, a stamp, license plate, audio or video recording, a recording produced by a plotter, calculator or other comparable technical device and a recording that is suitable for data processing, if it is used or can be used as legally relevant evidence of rights, duties or facts. An item is false if, when used as evidence, it is conducive to giving a misleading conception of its origin or of the identity of the person who issued it. An item is falsified if its contents have been unlawfully altered in respect of a datum that has probative relevance. The provision does not apply on so called harmless forgeries (the Government Bill 66/1988, pp. 112).
[24] Rautio 2008, pp. 890.
[25] Rautio 2008, pp 889- 890.
[26] The supreme court of Finland, judgment KKO:2012:54, the grounds of the decision, see point 13 and 16.
[27] Also computers work with IMEI- codes.

economic loss (the injured party does not need to be in direct connection with the data processing system or its exploitation, it's also possible that the damage is caused to the customer of the service provider).[28]

Computer fraud as an already fulfilled crime can also in fact also mean the preparation of another crime such as forgery (PC 33:1), although the provision of forgery does not require that the preparation of a false document has been done in the purpose of deceiving and benefiting from it.[29]

3. Content-related offences

Criminalization and possession of certain virtual images

Offences related to child pornography (CCC, article 9) are criminalized as *Distribution of sexually obscene pictures (*PC *17:18), Aggravated distribution of sexually obscene pictures depicting children (*PC *17:8a) and Possession of sexually obscene pictures depicting children (*PC *17:19).* The provision of distribution of sexually obscene pictures (PC 17:18) is as introduced:

> (1) A person who manufactures, offers for sale or for rent, exports, imports to or through Finland or otherwise distributes sexually obscene pictures or visual recordings depicting
>
> (1) children,
>
> (2) violence or
>
> (3) bestiality
>
> shall be sentenced for *distribution of sexually obscene pictures* to a fine or imprisonment for at most two years.
>
> (2) An attempt is punishable.
>
> (3) The provisions in section 17, subsection 2[30] apply also to the pictures and visual recordings referred to in this section.
>
> (4) A person under 18 years of age and a person whose age cannot be determined but who can be justifiably assumed to be under 18 years of age is regarded as a child.

Creation of child pornography can be done with[31] or without physical contact with the child. Sexual abuse of a child without corporeal sexual contact with the child can happen through internet by web-camera.[32] The internet is also

---

[28] Asko Lehtonen: *IT-law*, the article is accessible in Finnish language at the webpage of University of Vaasa: http://www.uwasa.fi/talousoikeus/opiskelu/verkkojulkaisut/

[29] See The Legal Affairs Committee 4/2009, pp. 5.

[30] Distribution of depictions of violence (PC 17:17) states, that (1) A person who offers for sale or for rent, distributes or to that end manufactures or imports films or other motion pictures or recordings containing such films or motion pictures depicting brutal violence shall be sentenced for distribution of depictions of violence to a fine or to imprisonment for at most two years. (2) The provision in subsection 1 does not apply if the depiction of violence is to be deemed justifiable because of the informative nature or manifest artistic value of the film or recording. Also if the contents of the film or recording have been screened by censors and certified for presentation according to the Act on the Censorship of Pictorial Recordings (775/2000), the provision in subsection 1 does not apply. If the producer or importer of the recording has evidently had the intention of submitting the recording to such censorship before offering it for sale or for rent or conveying it, the production or import is not punishable under subsection 1.

[31] Is quite common, that in especially physical sexual crimes against children, the offender videotapes or takes pictures of the criminal act (crime-related perversion). Later the offender might spread these pictures on the internet.

[32] If the offender makes the child undress in front of the web-camera or for example draw a picture of genitals, it is a question of sexual abuse (PC 20:6), see the Government bill 282/2010.

one of the latest tools for pornographers to spread their so called art.[33] Child pornography can also be spread only in artistic intention by a visual artist, which was the situation in CASE OF KARTTUNEN v. FINLAND, 10.5.2011). The case dealt with the limits of an artist's freedom of speech.[34] Although the appellant's only purpose was to provide a general discussion about how easy it is nowadays to access child pornography by presenting an exhibition of child pornography, the freedom of speech could not be accepted on the ground of being necessary in a democratic society. The judgment of ECHR in this case was inadmissible.

The national criminalization of possession of sexually obscene pictures depicting children aims to protect the child from offences of sexual character.[35] Also a person acquires by contractual means access to a picture representing child pornography can be held guilty of possession sexually obscene pictures depicting children (even then, when the person does not physically take over the data).[36] The criminalization permits the possession of sexually obscene pictures depicting children when there exists a legitimate reason (such as scientific research).[37]

4. Offences related to infringements of copyright and related rights[38]

Violation of copyright in the virtual sphere

The digitalization and creation of internet has made it more difficult to control violations of copyright in the virtual sphere. No national state regulation system is able to tackle with the infringements of copyright on the web, since the web does not recognize boundaries of states.[39] The Copyright Act (1961/404) aims for technology neutrality.[40] There exists no separate regulation for digital environment or products (for example quotation and citation on the web), with the exception of a few sections on computer programs.[41] The same rules apply on analog and digital content. [42]

---

[33] See Khaled Mohey Ahmed: Who does what to children, where, why and how? in *'Computer Crimes, Cyber- Terrorism, Child Pornography and Financial Crimes'* (Ed. Spinellis, Dionysios), Revue Internale de Droit Pénal, Athens, Eres 2004, pp. 202.

[34] The judgment is accessible in English at the website of the ECHR: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22885630%22],%22itemid%22:[%22001-104816%22]}

[35] See the Constitutional Law Committee 23/1997 and the Government bill 6/1997.

[36] See the Government bill 282/2010.

[37] See the Government bill 6/1997.

[38] For a basic and up-to-date representation in English language about the Finnish intellectual property law, see Niklas Bruun: Intellectual Property Law in Finland, in the work *Introduction to Finnish Law and Legal Culture* (Ed. Nuotio, Kimmo- Melander, Sakari – Huomo-Kettunen, Merita), Helsinki, Forum Iuris 2012, pp. 169-186.

[39] *Median maailma* [world of media], the webpage in Finnish is accessible: http://www2.edu.fi/medianmaailma/saannosto/ongelmia_verkkomediassa.html

[40] The Finnish Copyright Act (1961/404) is accessible in English at the webpage of Ministry of Justice, see http://www.finlex.fi/fi/laki/kaannokset/1961/en19610404.pdf

[41] The general rule is that anyone may make single copies for his private use of a work that has been made public (the copies thus made may not be used for other purposes). It is important to notice that this general rule does not apply to a computer-readable computer program or to the making of a computer-readable copy of a computer-readable database (See The Copyright Act, section 12).

[42] Raito, Mikko: *Tekijänoikeudet tietoverkossa ja verkkojulkaisemisessa* [Copyright in the information network and the network publication], Kopiosto 2008. The publication by the Finnish Copyright society KOPIOSTO is accessible in Finnish at the webpage of KOPIOSTO:

Preparatory Colloquium Verona (Italy), November 2012
Finnland

The Finnish copyright law does not provide any provisions on using copyright protected material by linking. A special question that concerns copyright in the virtual sphere is linking, that can traditionally be put into effect on three levels 1) a *standard hyperlink* to the homepage (does not require authorization), 2) a so called *deep link* to another page than the front page (a so called gray zone) and 3) a so called *framework-link*, linking the page to be linked into the own website, in other words, linking in a new environment (requires always authorization).[43] The deep *links* can sometimes make a real problem, because the user does not necessarily notice the owner of the web material, possible disclaimers or the ads placed on the web page.[44] A topical question about linking is also the question of silent approval to conventional internet use.[45]

The PC's chapter 49 regulates violations of incorporeal rights. The provision of copyright offence (49:1) is as introduced:

(1) A person who for profit and in violation of the Copyright Act (404/1961) and in a manner conducive to causing considerable detriment or damage to the person holding a right, violates the right of another to

(1) a literary or artistic work,

(2) the performance of a literary or artistic work or of national heritage,

(3) a record or other device on which sound has been recorded,

(4) a film or other device on which moving images have been recorded,

(5) a television or radio broadcast,

(6) a register, table, program or another similar work referred to in the Copyright Act and containing the compilation of a considerable amount of information, or a database the compilation, verification or presentation of which has required considerable effort, or

(7) a photograph shall be sentenced for a *copyright offence* to a fine or to imprisonment for at most two years. (2) Also a person who for profit and in a manner conducive to causing considerable detriment or damage to the person holding a right, imports for the purpose of dissemination among the public or for transport through Finland to a third state a sample or a copy produced abroad of a work or photograph, a record, film or other device on which sound or moving pictures have been recorded or a register, table, program or another similar work containing the compilation of a considerable amount of information, or a database the compilation, verification or presentation of which has required considerable effort, as referred to in subsection 1, while knowing that it has been produced or copied in circumstances under which said production or copying would in Finland be punishable under subsection 1 or under section 56a of the Copyright Act, shall be sentenced for a copyright offence.

---

http://www.tiedekustantajat.fi/stl-files/raito.pdf

[43] It is possible to direct linking by copyright clauses. It is also important to notice that the storage of data or passing on and keeping available for the public (for example animations) on webpage is never a question of private use, and therefore permission of the copyright holder is always required. See Raito 2008.

[44] Tekijänoikeustoimikunnan mietintö. Tekijänoikeudet tietoyhteiskunnassa. Komiteanmietintö 2002:5 [Copyright Commission report. Copyright in the Information Society. Committee Report 2002:5], pp. 23
http://www.minedu.fi/export/sites/default/OPM/Julkaisut/2002/liitteet/tekijanoikeus/yleisperustelut.pdf?lang=fi

[45] See the report by Commission for copyright 2012/2: Ratkaisuja digiajan haasteisiin [solutions to the challenges by digital media], pp. 101,105. The report is accessible on the webpage of Ministry of Education and Culture: http://www.minedu.fi/export/sites/default/OPM/Julkaisut/2012/liitteet/OKMtr2.pdf?lang=en . See also Pihlajarinne, Taina: Internetvälittäjä ja tekijänoikeuden loukkaus [internet intercessor and copyright infringement],Vantaa, Lakimiesliiton kustannus 2012.

(3) Also a person who uses a computer network or computer system to violate the right of another to the objects of protection referred to in subsection 1 so that the act is conducive to causing considerable detriment or damage to the holder of the right that has been violated, shall be sentenced for a copyright offence.

In Finland, like probably in all other countries too, the main objects of illegal circulation on the internet are music, computer games- and programs, including movies. The Finnish copyright Act that dates back to the year 1961 (it was also in the 1960s when the computers came to Finland) is at the moment quite difficult to understand, also for lawyers.[46] The old Act and the legality principle can collide and cause difficult interpretation problems (could here be a place for the application of the legal doctrine *mistake of law*?).[47]

Crimes related to virtual identities of users

The Constitution (731/1991) guarantees everyone's right to self-determination.[48] In Finland, identity theft is not currently criminal offence though the practice of identity theft has become increasingly common.[49] The legality principle hinders to interpret the offence of theft in an extending way to also cover the theft of another person's identity. A person's identity is not a movable property that can be stolen from the possession of another (PC 28:1). Identity theft has no essential element of offence described in law. Therefore, identity theft is now sanctioned on other grounds- depending on the special circumstances of the case- like fraud (PC 36:1).

Violation of IT privacy takes in practice form of identity misuse in different variations. To put up a Facebook profile in another person's name is legal, if the act clearly does not fill in the descriptions of *defamation offence* (PC 24:9) or *dissemination of information violating personal privacy* (PC 24:8). A fake profile can though also be used in the preparation of a more serious crime, for example in the case of unauthorized acquisition of information in the victim's circle of friends. One problem with identity thefts are, that the applicability of the essential elements of the offence described in the provision are quite high. The essential elements of defamation offences are not easily filled, and they are not either easy to investigate (due to the low maximum penalty it is not possible to use coercive measures in the investigation, the investigation of possible defamations on public discussion forums are the most likely to be objects of investigation).[50]

Crimes related to virtual identities of users can exist of various kinds: it can be a so called fake profile, the misuse of someone else's email address or username, or a dating ad for another person in the purpose of bullying. Of the last mentioned, the ECHR has passed a judgment concerning Finland (CASE OF K.U. v. FINLAND, 2.12.2008) concerning the right to respect for private life (article 8 of European Convention on Human Rights**)**. The background to this case lay in the problematic questions of identity- theft. An unknown person or persons had placed an advertisement on a dating site on the internet in the name of 12 year old boy, without the boy's knowledge. The

[46] The Copyright Act has gone through several amendments since the year 1961. This has partly led to a legislative technique that includes a great number of references from section to another.

[47] If the perpetrator errs in regarding his or her act as lawful, he or she is exempt from criminal liability if the mistake is to be deemed manifestly excusable due to the particular obtuseness of the contents of the law (PC 4:2).

[48] The Finnish Constitution (1999/731) is accessible in English at the webpage of Ministry of Justice, see http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf

[49] In general identity theft also increasingly focuses on companies, See the webpage of Helsinki region Chamber of Commerce http://www.helsinki.chamber.fi/?1011_m=3753&s=2 (information accessible only in Finnish).

[50] email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi

advertisement mentioned the boy's age and year of birth, and it gave a detailed description of his physical characteristics. The advertisement also provided the boy's contact information: a link to the web page with a picture of the boy and a telephone number. In the advertisement, it was claimed that the boy was looking for an intimate relationship with another boy. [51] The case ended up to ECHR, due to Finland's legislation situation at that time: the law made it impossible to clear up the case or prosecute the offender.

Putting up a fake profile in another person's name is mainly to be considered as a *defamation offence* (PC 24:9), *copyright offence* (PC 49:1) or *data protection offence* (PC 38:9).

The misuse of someone else's email address or username mostly fills the essential elements of the offence *computer break-in* (PC 38:9) or *message interception* (PC 38:3). It can also be a question of *defamation* (PC 24:9), *dissemination of information violating personal privacy* (PC 24:8) or *interference with communications* (PC 38:5).

Making a dating ad in another person's name is most easily seen as a *defamation offence* (PC 24:9). It can also be seen as *dissemination of information violating personal privacy* (PC 24:8) or *data protection offence* (PC 38:9).[52]

Damaging the property of virtual personalities: virtual theft

The Penal Code's provision of theft states, that a person who appropriates movable property from the possession of another shall be sentenced for *theft* to a fine or to imprisonment for at most one year and six months. Also an attempt is punishable (PC 28:1)

In the year 2011 the court dealt with the question of damaging virtual personalities and their belongings. The Court of Appeal gave a judgment that virtual theft in 'Habbo Hotel' could not be punished as theft. The accused had stolen another person's virtual hotel account and thereby stolen virtual furniture worth 465 euros. Kouvola court of Appeal held that the accused could not be sentenced for theft because of the law and legal interpretation of it (the legality principle).[53]

3. Problems with respect to the principle of legality[54]

In addition to the criminal law reform in Finland (1970-2003) a greater emphasis was laid on constitutional and human rights.[55]According to Lahti, "*the legality principle is not the only basic right which is relevant for Finnish criminal law and its reform. Many of the basic principles which were behind the reform work can be classified as fundamental rights after the constitutional reform*". In these basic principles can be found, both moral and political

[51] The case can also be found in English at the ministry of justice's webpage http://www.finlex.fi/fi/oikeus/eurooppa/feit/2008/20084408?search[type]=pika&search[pika]=internet

[52] Article '*Nettirikosten pohdintaa'* [Reflections on internet crimes], the article is accessible in Finnish at the Police's webpage http://www.poliisi.fi/poliisi/helsinki/home.nsf/files/Nettirikosten%20pohdintaa/$file/Nettirikosten%20pohdintaa.pdf

[53] The case of Kouvola court of Appeal KouHO:2011:3, is accessible in Finnish at the webpage http://www.oikeus.fi/54105.htm

[54] For a basic and up-to-date representation in English language on the Finnish legality principle, see Melander, Sakari: The Foundations of Criminal Law Thinking, in the work *Introduction to Finnish Law and Legal Culture* (Ed. Nuotio, Kimmo- Melander, Sakari – Huomo-Kettunen, Merita), Helsinki, Forum Iuris 2012, pp. 242-244.

[55] See Lahti, Raimo: Towards internationalization and Europeanization of criminal policy and criminal justice- challenges to comparative research, in *Current problems of the penal law and criminology* (Ed. Emil. W. Ptywaczewski), Warzawa, Wolters Kluwer Polska Sp. z.o.o. 2012, pp. 373.

arguments.[56] A functional criminal law could be found when the forum is open for different types of legal, political and moral arguments: the outcome should not be rejected with arguments entirely based on the legality principle.[57] Although the principle of legality is one of the most fundamental principles of Finnish criminal law[58], it should not hinder the discovery of functional cybercrime legislation. On the other hand, the legality principle should also be strictly followed in the legislation process.

In Finland, like in most countries, the legality principle is seen to consist of five sub principles: 1) *nullum crimen sine lege scripta* (criminal law must be prescribed law), 2) *nullum crimen sine lege certa* (the offence must be exactly defined and thereby also foreseeable), 3) *nullum crimen sine lege praevia* (criminal law shall not be regulated or applied retrospective to the disadvantage of the accused) and 4) *nullum crimen sine lege scripta*: the prohibition of interpretation of regulations by analogy. The case-law of the European court of Human rights accepts this classification.[59]

It could be assumed that in every country, the rate of 'cyber technological progress' is so fast, that it is impossible to follow this pace of development by statutory provisions. The legality principle and its requirement on sufficiently accurate criminal provisions are difficult to combine with this. In Finland, this rapid speed of technological development has been answered with a tendency to prescribe laws of general nature with forward looking statements, such as "*comparable to those in any other way*". Generic expressions of penal provisions are, as mentioned earlier, problematic with respect to the principle of legality and its component, *lex certa*.[60] The principle of *lex scripta* might also be problematic in situations, where the law does not give an exact, covering definition on a subject (for example definitions on racist and hate speech lack at the moment[61]). The problems with the principle of legality and cybercrimes could be assumed to be quite universal between countries who have adopted a similar or identical definition on the legality principle.

4. Civil and administrative sanctions

The non-criminal means of combatting offensive websites

In Finland the operator can be held legally responsible for websites containing illegal and racist material. The operator can be held responsible for this kind of material if the operator doesn't on its own initiative *remove* clearly

[56] Lahti, 2012, pp. 374.

[57] About the Finnish legality principle, see Lahti, Raimo: *The rule of law and Finnish criminal Law reform*, 37 Acta Juridica Hungarica (1997), Budapest, Akademiai Kiado, pp. 251-258. The citation ibid., pp. 258.

[58] The Constitution of Finland provides a provision on the principle of legality in criminal cases (8§), according to which no one shall be found guilty of a criminal offence or be sentenced to a punishment on the basis of a deed, which has not been determined punishable by an Act at the time of its commission. The penalty imposed for an offence shall not be more severe than that provided by an Act at the time of commission of the offence. The principle of legality is also to be found in the Penal Code (3:1),that states: a person may be found guilty of an offence only on the basis of an act that has been specifically criminalized in law at the time of its commission. The punishment and other sanction under criminal law shall be based on law.

[59] See Lahti 2012, pp. 373.

[60] See footnote 5.

[61] Hannula, Ilari – Neuvonen, Riku: *Internetin keskustelupalstan ylläpitäjän vastuu rasistisesta aineistosta* [The internet forums administrator's responsibility for racist material]. Lakimies 3/2011, pp. 532.

illegal material, or if the operator doesn't obey the courts order to remove the material.[62] The operator might also be legally responsibility as abettor or perpetrator if the operator knowingly allows the usage of the website for racist releases.[63]

Websites can also be *closed down* on content basis. This concerns child porn. In a quite recent case laid down by the Highest Administrative Court of Finland (KHO:2010:53)[64] the police had placed A's webpage containing child porn on a *blocking list*[65] that *in concreto* meant that it was impossible to access the webpage. A blocking list restricts the senders and the receiver's freedom of speech and the right to communicate.[66] Blocking of webpages is – to follow the strict phrasing in law - directed to foreign webpages containing child porn.[67] Here could maybe be questioned amongst all: how was it possible that a Finnish webpage was placed on a blocking list that was meant for foreign webpages? By following the principle of legality in the strictest sense, this would not have been possible.

5. The legitimate use of ICT and internet

Constitutional limits to criminalize certain conduct

The Finnish criminalization principles set constitutional limits to criminalize certain conduct. *The legality principle* is one of the so called criminalization principles in Finland. Other criminalization principles are *the principle of inviolably of human dignit*y, the principle of the protected interest (behind every criminalization must be a legitimate protected interest), *the principle of ultima ratio* (criminal law can be used only as a last resort) and the *principle of social cost evaluation* (criminalization is allowed only if it costs more benefits than harms to the society). Each principle is put into proportion to the fundamental rights and EU law.[68] The area of criminalization should be kept concise. The

[62] See Act on the Exercise of Freedom of Expression in Mass Media (2003/460) 18 §, the Act is accessible in English at the webpage of Ministry of Justice: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf) and Act on provision of information society services (2002/458) 16 §, the Act is accessible in English at the webpage of Ministry of Justice: http://www.finlex.fi/fi/laki/kaannokset/2002/en20020458.pdf). The first mentioned Act (Chapter 5, section 17: Release of identifying information for a network message) is adjusted and the adjustment will take force in the year 2014 (about the adjustment in Finnish, see
http://www.finlex.fi/fi/laki/alkup/2011/20110856).

[63] Hannula- Neuvonen 2011, pp. 546.

[64] The case concerned the right to appeal about the decision the police had made to place a Finnish website on a blocking list. The right to appeal was granted although the preparatory work on the Act forbids the appeal (Neuvonen, Riku: KHO 2010:53 – *Keskusrikospoliisi ja lapsipornosivun poistaminen* [The Finnish National Bureau of Investigation and the removal of a child porn website] Lakimies 7–8/2010, pp. 1381. The case is accessible in Finnish at the Ministry of Justice website http://www.finlex.fi/fi/oikeus/kho/vuosikirjat/2010/201002023?search%5Btype%5D=pika&search%5Bpika%5D=KHO%3A2010%3A53%20.

[65] Laki lapsipornografian levittämisen estotoimista (2006/1068) 4 §[The Act of combatting the distribution of child pornography (2006/1068) 4 §]

[66] Neuvonen 2010, pp. 1378.

[67] Neuvonen 2010, pp. 1380.

[68] See Melander, Sakari: Abstract: A theory of criminalization- legal constraints to criminal legislation, pp. 507- 509, in the work *Kriminalisointiteoria- rangaistavaksi säätämisen oikeudelliset rajoitukset* [A theory of criminalization- legal constraints to criminal legislation] Suomalaisen Lakimiesyhdistyksen julkaisuja 2008.

Constitution sets up limits to the criminalization of certain conduct. In order to limit a constitutional right (for example the freedom of speech), the restriction has to be based on parliamentary law (1). The restriction has also to be well-defined and laid down in a sufficiently precise manner (2). The limitation has to be based on an acceptability requirement: there has to be an acceptable social need for the limitation (3). The restriction is not allowed to extend to the core of the fundamental right (4). Also the requirement of proportionality has to be followed: the restriction has to be necessary for achieving the aim and in right proportion to the object of legal protection and to the social interest (5). When a constitutional right is restricted, there is also a duty to ensure that adequate systems of process of law are established (6). A restriction can never be in conflict with Finland's international human rights obligations (7).[69] In Finland there has been a tendency to react desist on criminalization on preparation of offences.[70] As long as ICT and internet is used in a legitimate way (without offending the criminalization principles), there is no need or possibility to criminalize the use of it.

6. Criminalization and its limits

About granting access to certain data

The Supreme court of Finland has given a prejudice in the question of granting access to *data* (music, movies and computer software) protected by copyright law (KKO:2010:47). The offenders had maintained a *Finreactor* file on the internet, where registered network users could share and download copyright-protected files for free without the permission of the copyright holders. The files were shared by so called description- or torrent files (and not directly). According to the Supreme Court, the network operators and the network users were working by co-operation, together intentionally violating the rights of the copyright holders and causing the last mentioned large-scale economic loss.[71] In another judgment (KKO 2010:48) concerning the same *Finreactor* case, the Supreme Court stated that also an individual network user who had transferred data to network was held guilty of copyright infringement.[72]

In Finland the webmasters/administrators have been held responsible for *racist and other hate scribbling* on their internet pages since June 2011.[73] Also administrators who keep *child pornography* on their webpage can be held

[69] See Constitutional law committee 25/1994, pp. 4-5.

[70] In Finland, only preparation of serious offences, are punishable by international agreements (for example drug- and terrorist crimes). It is so far legal to plan a crime, for example a robbery. A proposition to criminalize the preparation of some serious criminal offences has been given this year (17/2012), the proposition is accessible in Finnish language at http://www.hare.vn.fi/mJulKaisujenSelailu.asp?h_iId=17871&ju_iId=4739. About the expanding liability for preparation and participation of offences, see especially: Lahti, Raimo - Sahavirta, Ritva: *The expanding forms of preparation and participation. Finland* (National report). Revue Internale de Droit Pénal, 2007, 78:3-4, CD Rom annexe, 101-115 (2008).

[71] The case is accessible in Finnish at the webpage of Ministry of Justice: http://www.finlex.fi/fi/oikeus/kko/kko/2010/20100047?search[type]=pika&search[pika]=KKO%3A2010%3A47

[72] The case is accessible in Finnish at the webpage of Ministry of Justice: http://www.finlex.fi/fi/oikeus/kko/kko/2010/20100048?search[type]=pika&search[pika]=KKO%3A2010%3A48

[73] A person who spreads statements or other information among the public where a certain national, ethnic, racial or religious group or a comparable population group is threatened, defamed or insulted shall be sentenced for *ethnic agitation* to a fine or to imprisonment for at most two years (PC 11:10).

responsible for the content.[74] The present legislation does not encourage the service providers to inform the police force about a suspected malpractice: the service provider might be held criminally responsible for the suspected malpractice.[75] The service provider is obliged to hand over- on the request of the police force – all passwords and other necessary information for retention.[76]

The acquisition or possession of data system offence device

The Finnish Penal Code criminalizes Possession of a data system offence device (34:9b). According to the provision:

> A person who in order to cause impediment or damage to data processing or to the operation or security of a data or communications system has possession of a device, computer program or set of programming instructions referred to in section 9a, paragraph (1a)[77] or a password, access code or other corresponding information referred to in subparagraph b[78], shall be sentenced for *possession of a data system offence device* to a fine or to imprisonment for at most six months.

The criminalization does not apply on programming instructions.[79]

7. Data retention

Accordingly to the Data Retention **(**Directive 2006/24/EC), Finland has made amendments to the Coercive Measures Act (541/2007). Data preservation is an important tool in the investigation of cybercrimes under the CCC.[80]

In Finland there are no laws or regulations obliging internet service providers to store users' history of internet use. When it comes to the storage of data, only registration and telephony data is stored. Registration data includes data on internet access, i.e. to whom an ip- address was allocated at a certain moment.[81] There are no laws or regulations limiting the encryption of files and messages on the internet.

The Coercive Measures Act regulates data preservation (4:4) and obliges internet service providers to store internet users' personal data under certain circumstances, for a respite, up to three months (maximum).[82] If there is a reason

---

[74] Distribution of sexually obscene pictures (PC 17:18).

[75] Pihlajarinne 2012, pp. 160. See also part 4 on 'Civil and administrative sanctions'.

[76] The Coercive Measures Act 4: 4 a (11.5.2007/541).

[77] 'a device or computer program or set of programming instructions designed or altered to endanger or cause harm to data processing or the functioning of a data system or telecommunications system or to break or
disable the technical security of electronic communications or the security of a data system' (CC 34:9a, paragraph 1 a of the offence Endangerment of data processing).

[78] 'a password, access code or other corresponding information'(CC 34:9a, paragraph 1 b of the offence Endangerment of data processing).

[79] See the Government Bill 153/2006.

[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML . According to Kajantie: "*Finland has implemented the data retention directive (2006/24/EC), although in a way that does not entirely meet the idea behind the directive. The very reason for the directive was the fact that telcos and ISP's are moving towards flat rate invoicing from traffic based invoicing. Therefore they do not have a need to log traffic data anymore as they used to in the past. Finland has taken a slightly different approach: telcos are required to log only the data that they handle for the business*" (email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi).

[81] email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi.

[82] The Coercive Measures Act 4:4 c (541/2007). If the investigation requires, the respite may be extended for up to three months at a time.

to believe that data, which may be relevant to the investigation of the crime under investigation, will be lost or modified, the arresting officer may be entitled to impose it, in whose possession or control of data is (not, however, the alleged offender), to keep it unchanged.[83] This also applies to information transferred through the information system and the information of the data's origin, destination, route and timing of communications, as well as the size, duration, quality, and other similar factors (*traffic data*). If more than one service provider has been involved in conveying the information, pre-trial investigation authority has the right to get the service providers to identify the relevant traffic data.

As a general rule, traffic data (on real time or stored) can be accessed only for investigation or prevention of serious crime. A district court decides about the accessibility to the data (based on the evidence provided by the police officer leading the investigation.[84] The *suspect* can never be obliged to help out in clearing his own quilt (*right to not incriminate oneself*), for example by disclosing used passwords.[85]

In Finland there are no laws or regulations obliging an internet service provider to register users prior to providing services. If a service is free, no registration is required. In practice the operators do require registering of customer, mostly for billing purposes. According to Kajantie from the Finnish National Bureau of Investigation (KRP), there is basically no way to identify a criminal afterwards when it comes to free WLAN networks. This is a problem.

8. Internationalization

Legal instruments that have influenced Finnish legislation are foremost;

(i) the report *Computer -related Crime analysis of Legal Policy*, made by OECD (The organization for Economic co-operation and Development) in the year 1986

(ii) Recommendation No. R (89) 9on computer crime related penalties, given by the Select Committee of Experts on Computer-related Crime (PC-R-CC) in the year 1989[86]

(iii) the CCC given by the Committee of Experts on Crimes in cyber-space, signed in Budapest 23.11.2001 (came into force in 1.7.2004)

(iv) the Proposal to EU- directive on attacks against information systems (which would also overturn the council's framework decision 2005/222/YOS)[87]

The regulation of the scope of application of the Finnish law (double criminality) equals with the CC's article 22 on jurisdiction. Finland has made no reservation to this article.

The premise is, that Finnish criminal law applies to an offence committed in Finland (1 §). Finnish law applies to an offence committed outside of Finland that has been directed at Finland (3 §).[88] If the offender publishes on the

[83] The order shall provide upon request a certificate (4:4b.1). The investigating authority does not have the right to be informed of the message traffic information or other data stored in the content (4:4b.3).

[84] email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi.

[85] The Constitution of Finland (1991/731) 21 §, The Criminal Investigation Act (1987/449) 7.2 §, the Government Bill 82/1995, pp. 70, the case law by ECHR (self-incrimination) and international agreements.

[86] See the Government bill 94/1993.

[87] Information about this is accessible in Finnish language at the webpage of Ministry of Justice (updated 6.6.2012): http://www.om.fi/Etusivu/Valmisteilla/Lakihankkeet/Rikosoikeus/1290610003201

internet something illegal that is aimed for the Finnish audience, it is probably a question that the Finnish authorities have competence in.[89] Finnish law also applies to an offence committed outside of Finland that has been directed at a Finnish citizen, a Finnish corporation, foundation or other legal entity, or a foreigner permanently resident in Finland if, under Finnish law, the act may be punishable by imprisonment for more than six months (5 §).

If data has been entered to the internet abroad for example in the purpose of harming a Finnish corporation's computer system, the domestic law applies (*interference in a computer system)* if the requirement of double criminality applies. According to this, if the offence has been committed in the territory of a foreign State, the application of Finnish law may be based on sections 5, 6[90] and 8 only if the offence is punishable also under the law of the place of commission and a sentence could have been passed for it also by a court of that foreign State. In this event, no sanction that is more severe than what is provided by the law of the place of commission shall be imposed in Finland. According to section 8 mentioned above, the Finnish law applies to an offence committed outside of Finland which, under Finnish law, may be punishable by imprisonment for more than six months, if the State in whose territory the offence was committed has requested that charges be brought in a Finnish court or that the offender be extradited because of the offence, but the extradition request has not been granted.

It is though important to keep in mind that the requirement of double criminality does not always apply: if the offence has been committed outside Finland (PC 1:1 does not apply), the requirement of double criminality is not examined.
It is also often difficult to exactly define the place of where the cybercrime offence was committed. In Finland, there is no clear view on the question where a cybercrime is committed: it could be either where the service provider is situated[91], or there were the act took place. According to Lehtonen, most cybercrimes are committed where the primary action is performed: this applies on so called data vandalism (destruction of another's computer file, database, and web pages, or sending a computer virus that causes harm),

---

[88] An offence is deemed to have been directed at Finland (1) if it is an offence of treason or high treason, (2) if the act has otherwise seriously violated or endangered the national, military or economic rights or interests of Finland, or (3) if it has been directed at a Finnish authority (PC 1:3).

[89] See Hannula- Neuvonen 2011, pp. 540.

[90] Offence committed by a Finn 6 § (1) Finnish law applies to an offence committed outside of Finland by a Finnish citizen. If the offence was committed in territory not belonging to any State, a precondition for the imposition of punishment is that, under Finnish law, the act is punishable by imprisonment for more than six months.(2) A person who was a Finnish citizen at the time of the offence or is a Finnish citizen at the beginning of the court proceedings is deemed to be a Finnish citizen. (3) The following are deemed equivalent to a Finnish citizen: (1) a person who was permanently resident in Finland at the time of the offence or is permanently resident in Finland at the beginning of the court proceedings, and (2) a person who was apprehended in Finland and who at the beginning of the court proceedings is a citizen of Denmark, Iceland, Norway or Sweden or at that time is permanently resident in one of those countries.

[91] Lehtonen, Asko: *Straffrättslig jurisdiktion över internetbrott* [criminal jurisdiction over cybercrime]an internet publication that is accessible at the webpage of University of Vaasa: http://lipas.uwasa.fi/ktt/talousoikeus/it/i-brott/ibrott_toc_swe.htm .The same publication is a part of a book in Swedish language: Lehtonen, Asko: Straffrättslig jurisdiktion över internetbrott, i verket: IT och juristutbildning. Red. Wahlgren, Peter. Nordisk årsbok i rättsinformatik 2000. Stockholm 2001.

falsification of documents, and copyright infringement by making illegal copies or making them available to the public, hacking and unlawful use of another's computer.[92]
The CCC provides a negotiation obligation on questions concerning the interpretation and application of the CCC (article 45). Finland has now in June 2012 furthermore approved a new law on prevention and resolution of jurisdiction conflicts in the criminal procedure, the law regulates as well pre-trial investigation and the transfer of the prosecution proceedings between Finland and other EU Member States.[93] The negotiation mechanism is based on the European Framework decision 2009/948/YOS.

9. Participation of the country in discussions about the harmonization of cybercrime legislation

Because the cybercrimes does not respect the borders of countries, the harmonization of legislation plays an essential role (under or the absence of criminalization might lead to international criminality moving to countries where the penalties are week or non-existent).[94]

There has been discussion about possible updates or amendments to the cybercrime convention, due to the rapidly changing IT- environment.[95] In order to achieve an optimal update, there is a need for a comparative research like this AIDP's work, which provides information on the shared phenomena cybercrime. Like Lahti has formulated it: *"There is much more need for comparison of legal orders due to the emergence of European criminal law and international criminal law and due to the interaction between European and global legal regulations and the national legal orders*".[96]

10. Future developments

The majority of cybercrimes violates "*Pax Computationis*" (information technology peace).[97]

Some cybercrimes also have other objects of legal protection.[98] The development of information technology determinates which specific legal interests are deemed to be in need of protection by criminal law.

Sometimes new phenomenon in society, which would be in need of legal protection, but for which there has not yet been legislated a provision, can't be punished because of the legality principle. Maybe some phenomenon can be predicted earlier: in the year 1999 it was already predicted that imported or manufactured products and programs especially made for the purpose of committing cybercrimes, could be in need of legal protection.[99] Seven years later

---

[92] Lehtonen, Asko: *Tietotekniikkaoikeus* [IT-law]. The internet publication is accessible in word- format in Finnish language at the webpage of University of Vaasa: http://lipas.uwasa.fi/ktt/talousoikeus/it/i-brott/ibrott_kap4_swe.htm#kap4_2

[93] The law is accessible in Finnish at the webpage of Ministry of Justice: http://www.finlex.fi/fi/laki/ajantasa/2012/20120295 . See also the Government bill 21/2012 and the report by committee of Legal Affairs 5/2012.

[94] See Lehtimaja 1989, pp. 260.

[95] See Sieber, Ulrich: *International cooperation against terrorist use of the internet*. International review of Penal law: Cybercrime (vol. 77), Ramonville Sainte Agne, Eres, pp. 447.

[96] See Lahti 2012, pp. 365.

[97] Information technology peace can be described with the definitions confidentiality, integrity and availability. See the Government bill 4/1999, pp. 4. See also the handbook on information technology crimes of UN, the decisions on information technology crimes of OECD, European Council and Finnish Government.

[98] For example the provision of unauthorized use (CC 28:7) protects the exclusive right to use the information system (Pihlajamäki 2004, pp. 240- 241).

[99] See the Government bill 94/1999.

the provision of criminal computer mischief (PC 34:9a) was changed to equal with the development (951/1999). As a durable or good solution to the fast technological development can't either be the constant modification of the criminal law. If the law changes to frequently, nobody knows is his or her act criminal or not. Criminal law has to be foreseeable.

Today's new phenomenons in Finland are especially identity thefts and targeted attacks against data networks. The object of identity theft is automated identifiable information (names, passwords, email addresses, network services, credit data etc.) that can be misused for gaining economic profit or harm-making to the real identity holder. The majority of data captures are made with harmful software through email or a USB- flash drive. The object of the attack is information of great value and that has been carefully protected. The identity is usually captured by malicious computer programs and borrowed for a short time. The fight against identity thefts is complicated by the fact that the Criminal code does not criminalize identity capture. Especially the legal interest of personal data is in need of further protection by criminal law. [100]

Another problem that has to do with the rapid technological change is that the criminalization does not always correspond to the present time. When it comes to computer viruses, the problem is not anymore the distribution of a computer virus: the real problem is the usage of the virus. According to Kajantie, the most serious damage is being caused with information acquisition that is made by a remote-controlled malware program. At first, an offender distributes a malware program (PC 34:9a). Secondly another person comes and uses the malware program for information acquisition and collects important data. The whole process certainly violates the victim's fundamental rights, but the action does not fit in in any essential element of a crime.[101] In this way the rapid technological process creates new legal interests that are in need of legal protection.

[100] Information in Finnish on identity thefts, accessible on the Police's webpage: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/4E2E3CA9B18035C8C22579E80046AC48

[101] email 4.9.2012: sari.kajantie@poliisi.fi -> liisa.makela@helsinki.fi. See also see Sieber, Ulrich: International cooperation against terrorist use of the internet, in Revue Internale de Droit Pénal: Cybercrime (vol. 77), Ramonville Sainte Agne, Eres, pp. especially about 433 about perpetrators who attack other computers indirectly via third party computers from country A, B to C.