Mr. Jarmo Koistinen,
LL.D, Detective Superintendent
National Bureau of Investigation, Finland

Ms. Liisa Mäkelä
LL.M., Doctoral student
University Of Helsinki, Faculty of Law

Preparation of the 19th International Congress of Penal Law Section 2, Special Part (Finnish Report)*

1. General remarks

The first cybercrime offences were introduced into the Finnish Penal Code (PC) in 1991. Some provisions were added in 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. In 2007 Finland amended a number of the PC's provisions on cyber offences to match up to the Convention on Cybercrime (CCC). The CCC on cybercrime is the most comprehensive international instrument that addresses cybercrime.

The Finnish 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.[1] 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'*.[2]

There has so far been no need for a separate cybercrime law in Finland. Cybercrime offences are regulated widespread in different chapters (28, 34, 35, 36 and 38) of the Penal code (PC).[3] Nevertheless, Chapter 38 of the PC is primarily devoted to data and communication offences, i.e. crimes that cannot be committed without the computer system. 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.[4]

Chapter 38 contains following conducts which are established as criminal offences: Section 1 - *Secrecy offence* (578/1995), Section 2 - *Secrecy violation* (5 78/1995), Section 3 - *Message intercep-*

[1] 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.

[2] 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.

[3] An unofficial translation of the Finnish Penal Code (1889/39) into English is accessible at the website of Ministry of Justice: http://www.finlex.fi/pdf/saadkaan/E8890039.PDF. In this Report in appropriate places will be referred to the unofficial translations in the data base "Finlex". When reading these translations one must keep in mind that no all the translations are updated. The text of the Penal Code is also not updated, i.e. the latest amendments cannot be identified in the translation.

[4] See the Government bill (HE 94/1993), pp. 133.

* 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.

tion (531/2000), Section 4 - *Aggravated message interception* (578/1995), Section 5 – *Interference with communications* (578/1995), Section 6 - *Aggravated interference with communications* (578/1995), Section 7 - *Petty interference with communications* (578/1995), Section 7 a – *Interference in a computer system* (540/2007), Section 7 b – *Aggravated interference in a computer system* (540/2007), Section 8 - *Computer break-in* (578/1995), Section 8a – *Aggravated computer break-in* (540/2007) Section 8b — *Offence involving an illicit device for accessing protected services* (540/2007 and 1118/2001), Section 9 - *Data protection offence* (525/1999).

As already mentioned, Chapter 38 doesn't cover all the conducts to be defined as cybercrime offences. The provisions of *Unauthorised use* (PC 28:7–9) or *Criminal damage* (PC 35:1–3) may be applied in case information captured by computer break-in is later used. In case a person unlawfully interferes in the operation of production, supply or communications channels so that serious danger is caused to power supply, public health care, defence, administration of the law or another corresponding important societal function shall be sentenced for *Criminal mischief* (34:1.2). Misuse of devices, such as programs for computer break-in, passwords or computer viruses (CCC, Article 6) is criminalised as *Endangerment of data processing* (PC 34:9a). Computer-related forgery (CCC, Article 7), i.e. forgery of digitally stored data is criminalised under the PC's *Forgery offence* (33:1–3). Computer-related fraud (CCC, Article 8), meaning manipulation of digitally stored data, is criminalized as *Computer fraud* (PC 36:1.2). Content-related offences, such as related to child pornography (CCC, Article 9) are criminalised 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).

2. Case law and cybercrime offences

A judicial precedent is recognised in the Finnish law system as a source of law.[5] Nevertheless, under the Finnish legal system a judicial precedent is not binding. Courts of appeal and even district courts may depart from earlier decisions made by the Supreme Court, for example when the social circumstances have considerably changed. In practice, however, precedents of the Supreme Court are followed in cases arising after the precedent has been created and involving a similar point of law. The most important function of the Supreme Court is to rule on important points of law in cases which are significant for the entire legal order, guiding thereby the administration of justice in future cases. These precedents are usually created in cases for which the applicable Acts of Parliament and Decrees do not provide a clear solution for a question of law or in which there is room for interpretation. Approximately 150 such precedents are decided each year.[6]

[5] Officially, there are two general sources of law in Finland: written law (enactments) and established custom (customary law). In this connection the term *laki* (written law) encompasses constitutional law, statutes, and government Decrees and similar non-statutory instruments. Nowadays certain rules and regulations directly applicable throughout the European Union have also come to form part of this category of sources. Customary law, in its turn, constitutes a source of law where there are no written enactments and, as an additional requirement, the custom in question is not unreasonable. These legitimate sources of law are classed as mandatory in the sense that they must be taken as a basis in the performance of official functions on pain of dereliction of duty. Decisions of the Supreme Court and the *travaux préparatoires* attached to statutes (committee proposals, government Bills and records of parliamentary proceedings) which explain the legislators' intention are deemed to constitute weakly binding sources of law. General principles of law mainly fall into this category. Decisions of the European Court of Justice also fall into this category. Decisions of the Supreme Court, in particular, are taken as a basis for jurisprudential interpretations. All other legal bases to which it is generally recognized as acceptable to look for guidance when seeking the best possible outcome constitute permissible sources of law. These are, *inter alia*, jurisprudence, comparative arguments and practical reasons.

[6] http://www.kko.fi/29537.htm

The majority of cyber crimes violates "*Pax Computationis*" (information technology peace).[7] Some cyber crimes also have other objects of legal protection.[8] The development of information technology determinates which specific legal interests are deemed to be in need of protection by criminal law. Finnish legislative technique shows that the idea has both been to edit existing regulations to reflect new developments and also to create new provisions.

When considering reforms of the provisions that regulate cybercrime offences, it has to be noted that Finnish criminalization principles set constitutional limits to criminalize certain conduct.[9] Due to the rapid technological change penalized acts by the PC do not always correspond to the present time. The rate of technological progress is so fast, that it is impossible to follow this pace of development by statutory provisions. The legality principle[10] 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 problematic with respect to the principle of legality and its component, *lex certa*. 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[11]). 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.

The Finnish Statistics doesn't give a consistent picture of the frequency of cybercrime. Some estimates can be done by analysing the number of the cases regulated by Chapter 38 of the PC. The amount of those cases (regulated by Chapter 38) in the first court instance has not been very big.[12] The number of precedents concerning the interpretation of legal matters in cybercrime in the Supreme Court is naturally smaller. Therefore it can be said that the impact of judicial decisions on the formulation of criminal law related to cybercrimes is so far not significant or it is even very small. On the other hand, some recent precedents given by the Supreme Court of Finland have given tools

---

[7] Information technology peace can be described with the definitions confidentiality, integrity and availability. See the Government bill (HE 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.

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

[9] *The legality principle* is one of the so called criminalization principles in Finland. Other criminalization principles are *the principle of inviolably of human dignity*, 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. 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.

[10] 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 (See Lahti 2012, pp. 373).

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

[12] The amount of cases: 39 cases (2005), 27 cases (2006), 24 cases (2007), 21 cases (2008), 22 cases (2009), 27 cases (2010). See Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. ISSN=1798-6680. Helsinki: Tilastokeskus [viitattu: 14.12.2012]. Saantitapa: http://www.stat.fi/til/syyttr/tau.html

for the interpretation of statutes. For example, 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, if it is converted to another code (for example with a Flasher Box – device) and used as a evidence in legally significant connections (The supreme court of Finland, judgment KKO:2012:54, the grounds of the decision, see point 13 and 16. Also computers work with IMEI codes).

3. Finnish requirements for criminal liability concerning cybercrimes

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 exists an excusing ground the liability is precluded).[13]

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.[14]

Two offences to be classified as cyber crimes can also be committed negligently: Negligent endangerment (PC 34:7.1) and Data protection offence (PC 38:9). Negligent endangerment (PC 34:7.1) regulates a situation when a person who intentionally or negligently commits an act referred to in section 1, section 2 or section 4 of the Chapter 34.

> Section 1 of the Chapter 34 regulates ***Criminal mischief*** (578/1995):
> (1) A person who
> (1) starts a fire,
> (2) explodes something, or
> (3) causes a flood or another natural disaster,
> so that the act is conducive to causing general danger to life or health or general danger or very severe economic loss, shall be sentenced for *criminal mischief* to imprisonment for at least four months and at most four years.
> (2) Also a person who damages or destroys property or unlawfully interferes in the operation of production, supply or communications channels, so that serious danger is caused to power supply, public health care, defence, administration of the law or another corresponding important societal function shall be sentenced for criminal mischief.

[13] 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.

[14] 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.

(3) An attempt is punishable.

Chapter 38
Section 9 - Data protection offence (525/1999)
A person who intentionally or grossly negligently
(1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of data, sensitive data, identification codes or the processing of personal data for specific purposes, or violates a specific provision on the processing of personal data, (480/2001)
(2) by giving false or misleading information prevents or attempts to prevent a data subject from using his or her right of inspection, or
(3) conveys personal data to states outside the European Union or the European Economic Area in violation of chapter 5 of the Personal Data Act,
and thereby violates the privacy of the data subject or causes him or her other damage or significant inconvenience, shall be sentenced for a *data protection offence* to a fine or to imprisonment for at most one year.

4. The Finnish substantial provisions protecting integrity and functionality of the IT system

4.1 Interference in a computer system

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 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.

Chapter 38
Section 7 a – *Interference in a computer system (540/2007)*
(1) 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.
(2) An attempt is punishable.

Section 7 b – *Aggravated interference in a computer system* (540/2007)

(1) If in the interference in a computer system
(1) particularly significant detriment or economic loss is caused or
(2) the offence is committed in a particularly methodical manner
and the interference in a computer system is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference in a computer system* to imprisonment for at least four months and at most four years.
(2) An attempt is punishable.

Section 5 – *Interference with communications* (578/1995)
(1) 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.
(2) An attempt is punishable. (540/2007)

Section 6 - *Aggravated interference with communications* (578/1995)
(1) If in the interference with communications
(1) the offender commits the offence by making use of his or her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his or her other special position of trust,
(2) the offence prevents or interferes with the radio transmission of distress signals or such other telecommunications or radio transmissions that are made in order to protect human life
and the interference with communications is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference with communications* to imprisonment for at least four months and at most four years.
(2) An attempt is punishable. (540/2007)
[The Cable Transmission Act has been repealed by the Television and Radio Act 744/1998]

Section 7 - *Petty interference with communications* (578/1995)
(1) If the interference with communications, in view of its nature or extent or the other circumstances of the offence, is of minor significance when assessed as a whole, the offender shall be sentenced for *petty interference with communications* to a fine.
(2) An attempt is punishable. (540/2007)

4.2 Computer break-in

There is no requirement in the Finnish Penal Code that the hack of the computer system should be conducted by using one or more software to defeat security measures. When considering requirements for computer break-in it is enough for criminal liability that a person uses an access code that does not belong to him or her or by otherwise breaks a protection and unlawfully hacks into a com-

puter system. It is not relevant from the point of view of offence how the security measures are defeated.[15]

Chapter 38
Section 8 - *Computer break-in* (578/1995)
(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.

4.3 Message interception

The unauthorized interception of the transmission is regulated by PC 38: 3–4.

Chapter 38
Section 3 - *Message interception* (531/2000)
(1) A person who unlawfully
(1) opens a letter or another closed communication addressed to another or hacks into the contents of an electronic or other technically recorded message which is protected from outsiders, or
(2) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable telemessage transmitted by telecommunications or on the transmission or reception of such a message
shall be sentenced for *message interception* to a fine or to imprisonment for at most one year.
(2) An attempt is punishable.

Section 4 - *Aggravated message interception* (578/1995)
(1) If in the message interception
(1) the offender commits the offence by making use of his or her position in the service of a telecommunications company, as referred in the Act on the Protection of Electronic Messages (516/2004) or his or her other special position of trust, (517/2004)
(2) the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically, or

[15] Pihlajamäki 2004, p. 124.

(3) the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated message interception* to imprisonment for at most three years.
(2) An attempt is punishable.

4.4 Data forgery

In the Finnish PC there are no special statutes regulating data forgery. Authenticity as an object and alteration/deletion as a criminal act are regulated general forgery provisions. 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 33:6).

Chapter 33 - Forgery offences
Section 1 - *Forgery* (769/1990)
(1) 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 or imprisonment for at most two years.
(2) An attempt is punishable. (514/2003)

Section 2 - *Aggravated forgery* (769/1990)
(1) If in the forgery
(1) the item that is the object of the offence is an archival document stored by an authority or a general register kept by an authority and such a document or register is important from a general point of view, or the item otherwise has a particularly significant probative value, or
(2) the offender uses technical equipment procured for the commission of forgery offences or otherwise acts in a particularly methodical manner and the forgery is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated forgery to imprisonment for at least four months and at most four years.
(2) An attempt is punishable. (514/2003)

Section 3 - *Petty forgery* (769/1990)
If the forgery, when assessed as a whole, with due consideration to the nature of the item or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for petty forgery to a fine.

Section 6 - *Definitions* (769/1990)
(1) For the purposes of this Code, *item* refers to 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.
(2) 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.
(3) An item is *falsified* if its contents have been unlawfully altered in respect of a datum that has probative relevance.

4.5 Endangerment of data processing and an offence involving an illicit device for accessing protected services

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). The Finnish provision covers all the devices mentioned in CCC's article 6. Unauthorized use of the hacker's tools is included in the provision PC 34:9a.

> **Chapter 34**
> **Section 9a – *Endangerment of data processing* (540/2007)**
> 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.

Offence involving an illicit device for accessing protected is regulated in PC 38:8b.

> **Chapter 38**
> **Section 8b — *Offence involving an illicit device for accessing protected services*** (540/270 and 1118/2001)
>
> A person who, in violation of the prohibition laid down in section 3 of the Act on the Prohibition of Illicit Devices for Accessing Protected Services (1117/2001), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces, imports, offers for sale, rents out or distributes illicit devices for accessing protected services, or advertises, installs or maintains the same, shall be sentenced, unless a more severe or equally severe penalty for the act is provided elsewhere in the law, for an *offence involving an illicit device for accessing protected services* to a fine or to imprisonment for at most one year.

4.6. Possession of a data system offence device

Possession of a data system offence device is criminalised in PC 34:9b.

Chapter 34
Section 9 b – *Possession of a data system offence device (540/2007)*
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) or a password, access code or other corresponding information referred to in subparagraph b, shall be sentenced for *possession of a data system offence device* to a fine or to imprisonment for at most six months.

5. The Finnish substantial provisions protecting secrecy of private data

5.1 Legal regulation of secrecy of private data

Secrecy of private data is regulated by *Personal Data Act* (523/1999).[16] The objectives of the Act are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice (Personal Data Act 1.1 §). The Act applies to the automatic processing of personal data. It applies also to other processing of personal data where the data constitute or are intended to constitute a personal data file or a part thereof (2 §).

According to Section 3 of the Act *personal data* means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. Furthermore *processing of personal data* means the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data. *Personal data file* means a set of personal data, connected by a common use and processed fully or partially automatically or sorted into a card index, directory or other manually accessible form so that the data pertaining to a given person can be retrieved easily and at reasonable cost.

According to the Section 10 of the *Personal Data Act* the controller (a person, corporation, institution or foundation, or a number of them, for the use of whom a personal data file is set up and who is entitled to determine the use of the file, or who has been designated as a controller by an Act) shall draw up a *description of the personal data file*. The description of the personal data file must indicate (1) the name and address of the controller and, where necessary, those of the representative of the controller; (2) the purpose of the processing of the personal data; (3) a description of the group or groups of data subjects and the data or data groups relating to them; (4) the regular destinations of disclosed data and whether data are transferred to countries outside the European Union or the European Economic Area; and (5) a description of the principles in accordance to which the data file has been secured.

The controller shall keep the description of the file available to anyone. This obligation may be derogated from, if necessary for the protection of national security, defence or public order and security, for the prevention or investigation of crime, or for a supervision task relating to taxation or public finances.

According to the Section 11 the processing of sensitive data is prohibited. Personal data are deemed to be sensitive, if they relate to or are intended to relate to (1) race or ethnic origin; (2) the social,

[16] See the unofficial translation into English: http://finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf.

political or religious affiliation or trade-union membership of a person; (3) a criminal act, punishment or other criminal sanction; (4) the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person; (5) the sexual preferences or sex life of a person; or (6) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.

The Section 24 of the Act regulates information on the processing of data. When collecting personal data, the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. This information shall be provided at the time of collection and recording of the data or, if the data are obtained from elsewhere than the data subject and intended for disclosure, at the latest at the time of first disclosure of the data.

Acts violating the provisions of the *Personal Data Act* are penalised by the PC 38:9.

> ***Penal Code Chapter 38***
> ***Section 9 - Data protection offence*** (525/1999)
> A person who intentionally or grossly negligently
> (1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of data, sensitive data, identification codes or the processing of personal data for specific purposes, or violates a specific provision on the processing of personal data, (480/2001)
> (2) by giving false or misleading information prevents or attempts to prevent a data subject from using his or her right of inspection, or
> (3) conveys personal data to states outside the European Union or the European Economic Area in violation of chapter 5 of the Personal Data Act,
> and thereby violates the privacy of the data subject or causes him or her other damage or significant inconvenience, shall be sentenced for a *data protection offence* to a fine or to imprisonment for at most one year.

The illegal transfer and distribution of private data is not defined by the PC of Finland. The acts are included in the definition of processing of personal data. The Illegal use, transfer and/or distribution of private data is primarily treated as data protection offence (PC 38:9).

5.2 Justification of processing private data

Conditions under which processing of private personal data is allowed are defined by the Section 8 of *Personal Data Act.*

> Personal data shall be processed (Section 8 of the Personal Data Act) only if:
> (1) the data subject has unambiguously consented to the same;
> (2) the data subject has given an assignment for the same, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
> (3) processing is necessary, in an individual case, in order to protect the vital interests of the data subject;
> (4) processing is based on the provisions of an Act or it is necessary for compliance

> with a task or obligation to which the controller is bound by virtue of an Act or an order issued
> on the basis of an Act;
> (5) there is a relevant connection between the data subject and the operations of the controller, based on the data subject being a client or member of, or in the service of, the controller or on a comparable relationship between the two (*connection requirement*);
> (6) the data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping,
> (7) processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;
> (8) the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the controller or a third party receiving the data; or (9) the Data Protection Board has issued a permission for the same, as provided in section 43(1).

5.3 Violation of professional confidentiality

Professional confidentiality can be assessed from the point of view of authorities, health care professionals, advocates and priests.

When considering the authorities non-disclosure of the secret information by the authorities is regulated by the Chapter 6 Section 23 of the *Act on the Openness of Government Activities* (621/1999)[17].

> Chapter 6 Section 23 of the *Act on the Openness of Government Activities*: Non-disclosure and prohibition of use
>
> (1) A person in the service of an authority and an elected official shall not disclose the secret content of a document, nor information which would be secret if contained in the document, nor any other information obtained in the service of the authority, where covered by a duty of non-disclosure provided in an Act. The provision on non-disclosure shall apply also after the service or the performance of the task on behalf of the authority has ceased.
> (2) The provision in paragraph (1) applies also where trainees or other temporary personnel, persons commissioned by the authority or persons in the service of such persons have acquired secret information by virtue of an Act or a permission based on an Act, unless otherwise provided in the Act or laid down in the permission. A party, his/her representative or counsel shall not disclose to third parties secret information obtained by virtue of party status and concerning other persons than the party himself.
> (3) A person referred to above in paragraph (1) or (2) shall not use secret information for personal benefit or the benefit of another, nor for the detriment of another. However, a party, his/her representative and counsel may use information concerning a person other than the party himself/herself, where the matter concerns the right, interest or obligation on which the access of the party to the information is based.

[17] See the unofficial translation into English: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990621.pdf.

Chapter 3 Section 17 of the *Health Care Professionals Act* (559/1994)[18] regulates that no health care professional may reveal without permission to a third party any secret concerning an individual or a family that he or she has learned on the basis of his or her position or tasks. The obligation to maintain secrecy shall continue after their professional activity has ended.

From the point of view of patients the *Act on the Status and Rights of Patients* (785/1992)[19] regulates patients' rights in the field of collecting personal information.

> **Section 13 (653/2000)**
> ***Confidentiality of information in patient documents***
>
> The information contained by patient documents shall be confidential.
>
> Health care professionals or other persons working in a health care unit or carrying out its tasks shall not give information contained by patient documents to outsiders without a written consent by the patient. If a patient is not capable of assessing the significance of the consent, information may be given by his/her legal representative's written consent. In this Act outsiders refer to persons other than those who participate in the care of the patient or in carrying out jobs related to it in the health care unit in question or by its order. The secrecy obligation remains in force after termination of the employment relationship or the job.

The 2nd paragraph notwithstanding:

1. information included in patient documents may be given if there are express provisions on giving it or on the right of access to it in the law;
2. information necessary for the arranging of examination and treatment of the patient may be given to another health care unit or health care professional, and a summary of the treatment provided may be given to the health care unit or the health care professional that referred the patient for treatment and to a physician possibly appointed to be responsible for the care of the patient in accordance with the patient's or his/her legal representative's orally given consent or consent that is otherwise obvious from the context; and
3. information necessary for arranging and providing the examination and care of a patient may be given to another Finnish or foreign health care unit or health care professional, if the patient, owing to mental health disturbance, mental handicap or for comparable reason is not capable of assessing the significance of the consent and he/she has no legal representative, or if the patient cannot give the consent because of unconsciousness or for comparable reason;
4. information about the identity and state of health of a patient may be given to a family member of the patient or to other person close to the patient, if the patient is receiving treatment because of unconsciousness or for other comparable reason, unless there is reason to believe that the patient would forbid this; and
5. information on the health and medical care of a deceased person provided when the person was still living may be given upon a justified written application to anyone who needs the information in order to find out his/her vital interests or rights, to the extent the information is necessary for that purpose; the acquiring party may not use or forward the information for some other purpose.

[18] See the unofficial translation into English - http://finlex.fi/fi/laki/kaannokset/1994/en19940559.pdf.
[19] See the unofficial translation into English - http://finlex.fi/fi/laki/kaannokset/1992/en19920785.pdf

According to Section 5c of the *Advocates Act* (496/1958)[20] an advocate or his assistant shall not, without due permission, disclose the secrets of an individual or family or business or professional secrets which have come to his knowledge in the course of his professional activity. Breach of the obligation of confidentiality provided for under paragraph 1 above shall be punishable in accordance with chapter 38, section 1 or 2 (Secrecy offence) of the Penal Code, unless the law otherwise provides for more severe punishment for the act.

Breaching of the professional confidentiality may become actual, for example, in case of reporting an offence. Nevertheless, there is no general requirement in the Finnish legislation to report a crime to the authorities. On the other hand, PC 15:10 includes a provision which sets criminal liability for failure to report a serious offence to the authorities or the endangered person when there is still time to prevent the offence.

In the provision offences being as objects of such omission are following crimes: imminent genocide, preparation of genocide, crime against humanity, aggravated crime against humanity, war crime, aggravated war crime, torture, breach of the prohibition of chemical weapons, breach of the prohibition of biological weapons, compromising of the sovereignty of Finland, treason, aggravated treason, espionage, aggravated espionage, high treason, aggravated high treason, rape, aggravated rape, aggravated sexual abuse of a child, murder, manslaughter, killing, aggravated assault, robbery, aggravated robbery, trafficking in persons, aggravated trafficking in persons, hostage taking, aggravated criminal mischief, aggravated endangerment of health, nuclear device offence, hijacking, an offence committed with terrorist intent referred to in chapter 34a, section 1, subsection 1(3), aggravated impairment of the environment or aggravated narcotics offence.

Chapter 15 of the PC

Section 10 - *Failure to report a serious offence* (563/1998)

(1) A person who knows of imminent genocide, preparation of genocide, crime against humanity, aggravated crime against humanity, war crime, aggravated war crime, torture, breach of the prohibition of chemical weapons, breach of the prohibition of biological weapons, compromising of the sovereignty of Finland, treason, aggravated treason, espionage, aggravated espionage, high treason, aggravated high treason, rape, aggravated rape, aggravated sexual abuse of a child, murder, manslaughter, killing, aggravated assault, robbery, aggravated robbery, trafficking in persons, aggravated trafficking in persons, hostage taking, aggravated criminal mischief, aggravated endangerment of health, nuclear device offence, hijacking, an offence committed with terrorist intent referred to in chapter 34a, section 1, subsection 1(3), aggravated impairment of the environment or aggravated narcotics offence, and fails to report it to the authorities or the endangered person when there is still in time to prevent the offence, shall be sentenced, if the offence or a punishable attempt thereof is committed, for a failure to report a serious offence to a fine or to imprisonment for at most six months. (212/2008)

(2) However, a person shall not be sentenced for a failure to report a serious offence, if, in order to prevent the offence, he or she would have had to denounce a spouse, a sibling, a direct ascendant or descendant, a person living in the same household or a person who is close owing to another comparable personal relationship.

[20] See the unofficial translation into English - http://www.finlex.fi/fi/laki/kaannokset/1958/en19580496.pdf

When preparing abovementioned provision it was suggested add to the provision that a perpetrator of the failure cannot be a person, who is according to law obliged to keep confidentiality (for example priests, clinicians, lawyers etc.).[21] Anyway, this was not accepted by the law committee of the Parliament.[22] In that sense the legal state of the issue is not totally clear.

For example, according to Chapter 5 Section 2 of the *Church Law* (1054/1993)[23] a priest in case of being informed in confession about preparation of a crime has to advice a person to report a crime to the authorities or to a person who is in danger. If a person making a confession doesn't do it, the priest has to tell about it cautiously to the authorities without revealing any names or identifying information.

Provisions of the PC to be applied to breaching of confidentiality obligations:

> **Chapter 38 - Data and communications offences** (578/1995)
> **Section 1 - *Secrecy offence*** (578/1995)
> A person who in violation of a secrecy duty provided by an Act or Decree or specifically ordered by an authority pursuant to an Act
> (1) discloses information which should be kept secret and which he or she has learnt by virtue of his or her position or task or in the performance of a duty, or
> (2) makes use of such a secret for the gain of himself or herself or another
> shall be sentenced, unless the act is punishable under chapter 40, section 5, for a *secrecy offence* to a fine or to imprisonment for at most one year.

> **Chapter 40 Section 5 - *Breach and negligent breach of official secrecy*** (604/2002)
> (1) If a public official intentionally, while in service or thereafter, unlawfully
> (1) discloses a document or information which pursuant to the Act on the Openness of Government Activities (621/1999) or another Act is to be kept secret of not disclosed, or
> (2) makes use of the document or information referred to in paragraph (1) to the benefit of himself or herself or to the loss of another,
> he or she shall be sentenced, unless a more severe penalty for the act has been laid down elsewhere, for *breach of official secrecy* to a fine or to imprisonment for at most two years. A public official may also be sentenced to dismissal if the offence demonstrates that he or she is manifestly unfit for his or her duties.
> (2) If a public official commits the offence referred to in subsection 1 through negligence, and the act, in view of its harmful and damaging effects and the other relevant circumstances, is not of minor significance, he or she shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for *negligent breach of official secrecy* to a fine or to imprisonment for at most six months.

[21] Government bill (HE 6/1997).
[22] Committee report (LaVM 3/1998).
[23] A translation into English is not available in the data base "Finlex".

5.4 Illegal processing of personal and private data

General rules on the processing of personal data are regulated by the *Personal Data Act*. By *personal data is* meant any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. By *processing of personal data* is meant the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data (*Personal Data Act* 1:3).

Personal Data Act
Chapter 2 — ***General rules on the processing of personal data***
Section 5 — ***Duty of care***
The controller shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject's private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an Act. Anyone operating on the behalf of the controller, in the form of an independent trade or business, is subject to the same duty of care.

Section 6 — ***Defined purpose of processing***
It must be appropriate and justified to process personal data in the operations of the controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or their organisation into a personal data file. The purpose of the processing shall be defined so that those operations of the controller in which the personal data are being processed are made clear.

Section 7 — ***Exclusivity of purpose***
Personal data must not be used or otherwise processed in a manner incompatible with the purposes referred to in section 6. Later processing for purposes of historical, scientific or
statistical research is not deemed incompatible with the original purposes.

Section 8 — ***General prerequisites for processing***
(1) Personal data shall be processed only if:
(1) the data subject has unambiguously consented to the same;
(2) the data subject has given an assignment for the same, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the
request of the data subject before entering into a contract;
(3) processing is necessary, in an individual case, in order to protect the vital interests of the data subject;
(4) processing is based on the provisions of an Act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of an Act or an order issued
on the basis of an Act;
(5) there is a relevant connection between the data subject and the operations of the

controller, based on the data subject being a client or member of, or in the service of, the
controller or on a comparable relationship between the two (*connection requirement*);
(6) the data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping,
(7) processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;
(8) the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard
the rights and interests of the controller or a third party receiving the data; or
(9) the Data Protection Board has issued a permission for the same, as provided in section 43(1).
Personal data may be disclosed on the basis of paragraph (1)(5) only if such disclosure is a regular feature of the operations concerned and if the purpose for which the data is disclosed is not incompatible with the purposes of the processing and if it can be assumed that the data subject is aware of such disclosure.
Chapter 3 contains provisions on the processing of sensitive personal data and personal identity numbers. Chapter 4 contains provisions on the processing of personal data for special
purposes. The provisions on access to official documents apply to access to information in the personal data files of the authorities and to other disclosure of. personal data therein.

Section 9 — ***Principles relating to data quality***
(1) The personal data processed must be necessary for the declared purpose of the processing (*necessity requirement*).
(2) The controller shall see to that no erroneous, incomplete or obsolete data are processed (*accuracy requirement*). This duty of the controller shall be assessed in the light of the purpose of the personal data and the effect of the processing on the protection of the privacy of the data subject.

Section 10 — ***Description of file***
(1) The controller shall draw up a description of the personal data file, indicating:
(1) the name and address of the controller and, where necessary, those of the representative of the controller;
(2) the purpose of the processing of the personal data;
(3) a description of the group or groups of data subjects and the data or data groups relating to them;
(4) the regular destinations of disclosed data and whether data are transferred to countries outside the European Union or the European Economic Area; and
(5) a description of the principles in accordance to which the data file has been secured.
(2) The controller shall keep the description of the file available to anyone. This obligation may be derogated from, if necessary for the protection of national security, defence or public order and security, for the prevention or investigation of crime, or for a supervision task relating to taxation or public finances.

Applicable penal provisions concerning illegal processing of personal data are defined by the Personal Data Act as follows. Illegal processing covers illegal collection, use, retention and transfer of

personal data. From the point of illegality it doesn't make a difference whether the personal and private data are used, transferred etc. for police or law enforcement purposes.

Personal Data Act (523/1999)
Chapter 10

Section 48 — *Penal provisions*
(1) The penalty for a personal data offence is provided in chapter 38, section 9 of the Penal Code (39/1889) and for breaking into a personal data file in chapter 38, section 8 of the Penal Code.
The penalty for a violation of the secrecy obligation referred to in section 33 is provided in chapter 38, section 1 or 2 of the Penal Code, unless the act is punishable under chapter 40, section 5 of the Penal Code or a more severe penalty is provided in another Act.
(2) A person who intentionally or grossly negligently and contrary to the provisions in this Act:
(1) fails to comply with the provisions on the definition of the purpose of the processing of the personal data, the drawing up of the description of the file, the information on data processing, the rectification of the file, the right of the data subject to prohibit the processing of data or the notification of the Data Protection Ombudsman;
(2) provides false or misleading data to a data protection authority in a matter concerning a personal data file;
(3) breaks the rules or regulations on the protection and destruction of personal data files; or
(4) breaks a final order issued by the Data Protection Board on the basis of section 43(3), thus compromising the protection of the privacy of the data subject or his/her rights, shall be sentenced for a *personal data violation* to a fine, provided that a more severe penalty is not provided in another Act.

Chapter 38 of the PC
Section 9 - *Data protection offence* (525/1999)

A person who intentionally or grossly negligently
(1) processes personal data in violation of the provisions of the Personal Data Act (523/1999) on the exclusivity of purpose, the general prerequisites for processing, the necessity and integrity of data, sensitive data, identification codes or the processing of personal data for specific purposes, or violates a specific provision on the processing of personal data, (480/2001)
(2) by giving false or misleading information prevents or attempts to prevent a data subject from using his or her right of inspection, or
(3) conveys personal data to states outside the European Union or the European Economic Area in violation of chapter 5 of the Personal Data Act,
and thereby violates the privacy of the data subject or causes him or her other damage or significant inconvenience, shall be sentenced for a *data protection offence* to a fine or to imprisonment for at most one year.

Chapter 38 of the PC
Section 8 - *Computer break-in* (578/1995)

> (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.

In Finland, identity theft is not currently criminal offence though the practice of identity theft has become increasingly common. 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).

There are no specific forms of phishing in PC. Phishing is primarily treated as a fraud (PC 36:1–2). A person's digital personality is usually protected. If somebody illegally obtains access to it, the act may be treated as *computer break-in* (PC 38:8).

6. Protection against ICT Related illegal content

6.1 Child pornography

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).*

> **Chapter 17**
> **Section 18 - *Distribution of sexually obscene pictures*** (650/2004)
> (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 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.

Section 18a - *Aggravated distribution of sexually obscene pictures depicting children*
(650/2004)
(1) If, in the distribution of a sexually obscene picture depicting children
(1) the child is particularly young,
(2) the picture also depicts severe violence or particularly humiliating treatment of the child,
(3) the offence is committed in a particularly methodical manner or
(4) the offence has been committed within the framework of a criminal organisation referred to in section 1a, subsection 4
and the offence is aggravated also when assessed as whole, the offender shall be sentenced for aggravated distribution of sexually obscene pictures depicting children to imprisonment for at least four months and at most six years.
(2) An attempt is punishable.

Section 19 - Possession of sexually obscene pictures depicting children
(650/2004)
A person who unlawfully has in his or her possession a photograph, video tape, film or other realistic visual recordings depicting a child referred to in section 18, subsection 4 having sexual intercourse or participating in a comparable sexual act or depicting a child in another obviously obscene manner shall be sentenced for possession of sexually obscene pictures depicting children to a fine or imprisonment for at most one year.

Creation of child pornography can be done with 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.[24]

Finland has taken the necessary legislative measures when ratifying Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201). The Convention entered into force 1.10.2011 and following provisions in the Finnish Penal Code entered into force 1.6.2011. The main purpose of the provisions is to fight against child pornography in the cyperspace.

Chapter 20
Section 8b - *Solicitation of children for sexual purposes* (20.5.2011/540)

(1) A person who proposes a meeting or other contact with a child so that on the basis of the contents of the proposal or other circumstances it is obvious that the purpose of a person is to manufacture sexually obscene pictures or visual recordings depicting children referred in chapter 17, section 18, subsection 1 or commit an offence against a child referred in section 6 or 7 of this chapter, the offender shall be sentenced for solicitation of children for sexual purposes to a fine or imprisonment for at most one year.

[24] 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 (HE 282/2010).

(2) In case no more severe punishment is set by other legislation, for solicitation of children for sexual purposes shall be sentenced also the offender who lures a person under 18 years of age to sexual intercourse or other sexual act referred in section 18 a or to participate sexually obscene performances.

(3) An attempt of an offence referred to subsection 2 is punishable.

Chapter 20
Section 8c - *Attending sexually obscene performances involving the participation of children* (20.5.2011/540)

(1) A person who attends sexually obscene performances in which a person under 18 years of age participates, shall be sentenced for attending sexually obscene performances involving the participation of children to a fine or imprisonment for at most two years.
(2) An attempt of an offence is punishable.

Concept of "child pornography" or "pornographic performance" is not adopted in the Finnish criminal code. Instead of pornography is used expression "sexually obscene" which is not explicitly defined in PC. Nevertheless, ratification of the Convention (CETS 201) of the Council of Europe means that Finland has adopted the definition of "child pornography" contained in the Convention.

A problem of secondary victimization is avoided in the Finnish penal law since in Finland prostitution or the appearance in pornography as such is not punishable.

"Virtual child" pornography is criminalised by the amendment (20.5.2011/540) of the provision PC 17:18. In the provision a picture or visual recording depicting children is defined as genuine or life-like. A picture or visual recording is genuine, if it has been produced in a situation in which a child factually was as an object of sexually obscene activities. Correspondingly, a picture or visual recording is lifelike, if it misleadingly reminds a picture or visual recording created by photographing or using other method in a situation in which a child was an object of sexually obscene activities.

The internet is also one of the latest tools for pornographers to spread their so called art.[25] 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.[26]

6.2 Bullying, stalking and grooming in the cyber space

Creation and use of true anonymity sending and/or receiving material on the ICT is not penalised by the Finnish PC. Cyber-bullying is not directly penalized, but to it may be applied, for example, the provision of *defamation* (PC 24:9–10). Cyber-stalking is directly not penalised, but at least theoreti-

[25] 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.
[26] 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]}

cally to it may be applied in certain circumstances, the provision of *violation of a restraining order* (PC 16:9a). Cyber-grooming is not penalised in case of adult people.

7. ICT Related Violations of Property, Including Intellectual Property

7.1 ICT related fraud

Chapter 36 - Fraud and other dishonesty (769/1990)
Section 1 - *Fraud* (769/1990)
(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. (514/2003)
(3) An attempt is punishable.

Section 2 - *Aggravated fraud* (769/1990)
(1) If the fraud
(1) involves the seeking of considerable benefit,
(2) causes considerable or particularly significant loss
(3) is committed by taking advantage of special confidence based on a position of trust or
(4) is committed by taking advantage of a special weakness or other insecure position of another
and the fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated fraud* to imprisonment for at least four months and at most four years.
(2) An attempt is punishable.

7.2. Infringement of Intellectual Property IP rights

Chapter 49 - Violation of certain incorporeal rights (578/1995)
Section 1 - *Copyright offence* (822/2005)
(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.
(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.

Section 2 - *Intellectual property offence* (1281/2009)
A person who in violation of the Trademark Act (7/1964), the Patents Act (550/1967), the Registered Designs Act (221/1971), the Act on the Protection of Semiconductor Topographies (32/1991), the Utility Models Act (800/1991) or the Plant Variety Rights Act (1279/2009) and in a manner conducive to causing considerable financial loss to a person holding a right, breaches
(1) the right to a trademark,
(2) the exclusive right conferred by a patent,
(3) the right to a registered design,
(4) the right to a semiconductor topography,
(5) the right to a utility model, or
(6) a plant variety right
shall be sentenced for an *intellectual property offence* to a fine or to imprisonment for at most two years.

7.3. Industrial espionage

Chapter 30
Section 4 - *Business espionage* (769/1990)
(1) A person who unlawfully obtains information regarding the business secret of another
(1) by entering an area closed to unauthorised persons or accessing an information system protected against unauthorised persons,
(2) by gaining possession of or copying a document or other record, or in another comparable manner, or
(3) by using a special technical device,
with the intention of unlawfully revealing this secret or unjustifiably utilising it shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for *business espionage* to a fine or to imprisonment for at most two years.
(2) An attempt is punishable.

7.4 Other acts committed in the virtual world

There are no special provisions of acts committed in the virtual world. The Finnish courts have recently examined a 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 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).[27]

7.5 Non-Compliance Offences

What is concerning cooperation with law enforcement agencies in the field of cybercrime, the Communication Market Act (393/2003) sets obligations of a telecommunications operator to assist a public authority (Chapter 9, sections 90–99). In case the operator violates the Communication Market Act following sanctions are set by the Act (12:21). There are no provisions in criminal law concerning this matter.

> **Chapter 12 of the Communication Market Act**
>
> **Section 121 - *Conditional fines and temporary orders***
>
> (1) If someone violates this Act or provisions issued under it, and, despite being requested to do so, fails to rectify his actions within a reasonable period of at least one month, the Finnish Communications Regulatory Authority may order him to rectify the error or omission. A conditional fine or a threat of terminating the operations or of having the act done at the defaulter's expense may be imposed as sanctions in support of the obligation.
>
> (2) The provisions on conditional fines, threat of termination and threat of completion laid down in the Act on Conditionally Imposed Fines (1113/1990) shall apply.
>
> (3) If the error or omission represents an immediate and serious threat to public safety, public security or public health or creates serious economic or operational hindrance to other companies or users or to the functioning of communications networks, the Finnish Communications Regulatory Authority may decide on necessary interim measures without waiting for the expiry of the time limit referred to in subsection 1. As an interim measure the Finnish Communications Regulatory Authority may terminate the operations representing a threat or serious hindrance. The Finnish Communications Regulatory Authority may also restrict the use of frequencies or issue orders

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

on a comparable coercive measure. The interim measures may be valid for a maximum period of three months. The Finnish Communications Regulatory Authority may extend the interim measures for a further period of up to three months if the error or omission has not been rectified within the prescribed period. An appeal may be made separately against a decision concerning interim measures in the same manner as against a decision referred to in subsection 1. (363/2011)

8. Complementary optional information concerning law and practice (including statistics)[28]

Statistical data on offences regulated by Chapter 38 of PC is collected and stored in the databases of Statistics Finland. Official Statistics of Finland (OSF)[29]: Prosecutions, sentences and punishments [e-publication] contains statistical data on cyber crimes regulated by Chapter 38.

Other cyber crimes for which provisions of Chapter 38 PC are not applied cannot be identified in the official statistical data. Internal database of the Finnish police (PATJA) makes it possible to classify and collect statistical data also on other crimes to be classified as cyber-crime.

There is no comprehensive Finnish website concentrating on these questions. Anyway, there are warnings in various websites, for example, about scams. Finnish Consumer Agency warns to be careful with internet swindlers: http://www.kuluttajavirasto.fi/en-GB/scams/ The Finnish police has also information on cyber-crime in its website: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/5ABA1CD4B1D3B896C22570FB0057CA71

Victimization surveys don't include systematically questions on cyber-crimes.

One of the most common types of frauds is on-line scam, i.e. fraud. In typical online scams, the customer does not receive a product ordered and paid for in advance. The seller in these cases can no longer be contacted. The same pattern can occur in online auctions as well. In the Police of Central Finland region was made recently an analysis which showed that approximately 55 % of all registered frauds are on-line scams. There are no official studies on this question, but according to some estimates 30 % of all frauds are on-line scams. Anyhow, it is clear that the number of on-line frauds is growing.

One frequent group of computer crimes is malicious software attacking on-line banking transactions. In 2012 approximately 300 attacks were registered by police, and approximately 1000 attempts were revealed.

There are no centralised computer crime units in Finland. Biggest police stations have units which investigate evidence which is in electronic form, i.e. computers. There is a computer crimes unit in the National Bureau of Investigation which is specialised in criminal investigation of cyber-crime. In Finnish Prosecution Service prosecutors specialise in certain types of crime and they are called as key prosecutor of certain type of crime. There are three key prosecutors in the field of cyber-crime.

[28] The answers of this part of Questionnaire are primarily based on the interview of Detective Inspector Timo Piiroinen (20.12.2012). He works as a supervisor of cyber-crime investigation unit in the National Bureau of Finland.
[29] http://www.stat.fi/til/syyttr/tau_en.html

Law schools don’t offer systematically courses on cyber-crime. Cyber-crime is included in the training of police to some extent. It is estimated that the police has more knowledge in this field when comparing to prosecutors and judges.

The following forms and means of cyber-crimes are estimated to occur frequently, infrequently, or have not occurred in Finland.

Forms and Means of Cyber-Crime	**Occur Frequently**	**Occur Infrequently**	**Has not Occurred**
Online identity theft (including phishing and online trafficking in false identity information)	X		
Hacking (illegal intrusion into computer systems; theft of information from computer systems)	X		
Malicious code (worms, viruses, malware and spyware)	X		
Illegal interception of computer data		X	
Online commission of intellectual property crimes	X		
Online trafficking in child pornography	X		
Intentional damage to computer systems or data		X	

In addition, to the above, ransomware occurs frequently in Finland. The ransomware will attempt to extort money from the system's user by forcing them to purchase either a program to decrypt the files it had encrypted, or an unlock code which will remove the locks it had applied. This kind of messages have been sent in the name of police stating that the computer is illegally used and it will be opened if the user pays for example 100 euros.