Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

AIDP FINLAND: NATIONAL REPORT ON SECTION 3*

Helena VIHRIÄLÄ[1]

B. General Questions

The legislation on cyber crimes in Finland has followed the developments in Europe. The Finnish legislation conforms to the 1989 year Recommendation of the Council of Europe and Council of Europe Convention on Cybercrime 2001 as already stated in the previous Finnish reports in sections 1-2 and 4.[2]

There are two procedural laws which apply to the criminal cases. For the criminal procedure there is a separate law (Criminal Procedure Act/689/1977) in addition to the Code of Judicial Procedure, which is a general procedural law applying to all cases handled in general courts. The cyber crimes are not handled in isolation from other crimes and therefore there are no special conceptual definitions within the criminal procedure for cyber crimes.

There are no specific institutions involved in the implementation of information and communication technology (ICT) in the criminal justice. As stated in the Finnish report in section 2, there is a computer crimes unit in the National Bureau of Investigation specialised in cyber crimes and there are some prosecutors who specialise in the field of cyber crimes. In general, judges do not specialise in specific fields.[3]

The criminal justice system (investigation, prosecution, sentencing and prison service) is run by government agencies, i.e. private companies have no part in its implementation.

C. Information and Intelligence. Building information positions for law enforcement

The law enforcement agencies' (the police) main tasks are to secure the rule of law, maintain public order and security, prevent and investigate crimes and submit cases to prosecutors for consideration of charges (Police Act 493/1995, chapter 1 section 1, referred later as "Act 493/1995")[4] In Chapter 3, there are provisions on information gathering activities, which the police are allowed to engage in. The Police can use among others both telecommunications monitoring and telecommunications interception in its preventing work. [5] Other measures are technical monitoring, surveillance, technical surveillance (including interception, technical observa-

---

* 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 LL.D., Judge at Helsinki Court of Appeal.

2 Finnish legislation on data crimes was rather comprehensive and up-to-date already before the implementation of the 2001 Convention. The 2001 year convention has therefore not caused fundamental changes in the scope of punishable behaviour. See Pihlajamäki, Antti: The Protection of Data Processing under Criminal Law, Jyväskylä 2004 p. 289.

3 See UNOCD, Comprehensive Study on Cybercrime, Draft-February 2013 p. 172 (later referred as "UNODC); Courts show minimal levels of specialization for cybecrime, with just 10 per cent of countries reporting specialized judicial services.

4 The new Police Act 872/2011 will enter into force 1.1.2014 (later referred as "Act 872/2011").

5 Act 493/1995 chapter 3 section 31 c (1): Preconditions for telecommunications monitoring: Police officers have, in order to prevent or detect an offence, the right to subject a subscription, telecommunications address or telecommunications terminal equipment a person possesses or that he or she is otherwise assumed to be using to telecommunications monitoring or to temporarily disconnect such a subscription or terminal equipment if the person's statements, threats, behaviour or other circumstances give reasonable cause to suspect that he or she could commit an offence for which the maximum punishment is at least four years' imprisonment or an offence targeting an automatic data processing system and committed using telecommunications terminal equipment, or make him or herself guilty of procuring, threatening a person to be heard in the administration of justice, illegal threatening, a narcotics offence, a punishable attempt of the offences referred to above or preparing an offence to be committed with terrorist intent. Act 493/1995 chapter 3 section 31 d(1): Preconditions for telecommunications interception: Police officers have, in order to prevent or detect an offence, the right to intercept a subscription, telecommunications address or telecommunications terminal equipment a person possesses or that he or she is otherwise assumed to be using if the person' statements, threats or behaviour give reasonable cause to suspect that he or she could make him or herself guilty of an offence committed with terrorist intent and referred to in Chapter 34a, section 1(1)(2-7) or 1(2) of the Criminal Code, preparation of an offence to be committed with terrorist intent, directing of a terrorist group, promoting of the activities of a terrorist group or financing of terrorism, if the information to be gathered can be assumed to be of prime importance in preventing or detecting the offence (unofficial translation from the website of the Ministry of justice, www.finlex.fi, like all other direct quotations later on).

tion and technical tracking), undercover activities and undercover transactions as well as use of human intelligence sources. [6] The coercive measures regulated in the Police Act are similar to the coercive measures regulated in the Coercive Measures Act (449/1987)[7]. The difference between the two acts is that the coercive measures regulated in the Coercive Measures Act can be used when the pre-trial investigation of a crime has started, as a repressive measure. The coercive measures in the Police Act can be used when gathering information for preventive purposes.[8] Most of the coercive measures, both preventive and repressive, have to be decided by court.

The police have the right to obtain information both from a public and a private organization or person and to use human intelligence sources in their preventive and investigative work.[9] Those include DNA-databases and PNR and SWIFT databases. There seems to be a slight difference in the Credit Company Act (12/2007) and in the Insurance Company act (521/2008) as to what purpose they are obliged to provide the police information notwithstanding secrecy aspects. Section 141.2 in the Credit Company Act states that the company has the right to give secret information to the prosecutor and law enforcement agencies (police) to investigate crime. Chapter 30 section 3.8 the Insurance Company Act allows the insurance company to provide secret information to the prosecutor and the investigative authorities both to investigate and prevent crime. The conclusion seems to be that in spite of the wording in the police act (chapter 3, section 36), the police cannot receive secret information from the credit companies before a crime has been committed.[10]

In the Act on Processing of personal Data by the Police (761/2003) chapter 1 section 1 defines the scope of the Act as follows: "(1)This act applies to the automatic and other processing of personal

data needed for the performance of duties as referred to in section 1of the Police Act (493/1995), where the personal data constitutes or is intended to constitute a personal data file or part thereof. The Personal Data Act (523/1999) and the Act on the Openness of Government Activities (621/1999) apply to the processing of personal data, unless otherwise provided in this or any other Act. (2) In addition to what is provided in this Act, international agreements binding on Finland shall also be observed.

Chapter 2 section 4: (1) The Suspect Data System is a permanent, computerized personal data file intended for nationwide use by the police.

(2) The Suspect Data System may contain criminal intelligence, surveillance and observation data, obtained for the performance of duties laid down in section 1(1) of the Police Act, on persons who are, with reason, suspected of: 1) being guilty of or having been guilty of an offence subject to imprisonment; or 2) contributing to or having contributed to an offence subject to imprisonment of more than six months, or to an unlawful use of narcotics. (3) The data that may be recorded in the data system on the identity of persons consists of the full name, date of birth, personal identity code, sex, mother tongue, nationality, marital status, country of birth, municipality of residence at birth, municipality of residence, occupation, address and telephone number or other contact details, information on the person's death, and travel document information in the case of an alien.

(4) The Suspect Data System may only be used with the aid of a technical interface by police personnel appointed to criminal intelligence and surveillance duties." The last part (4) was amended by the law 15.7.2005/529 by adding the possibility to use it by police personnel appointed to crime analysis duties.

Chapter 2 section 6 (1): In addition to the permanent, computerized, nationwide information systems referred to in sections 2-4 and in sections 30 and 31, the police may also keep temporary or manually maintained personal data files for nationwide use.(2) With the exception of the information systems referred to in sections 2-5 and in sections 30 and 31, a police personal data file may also be established:1) for use by more than one police unit; or 2) for use by a police unit.(3) Information necessary for the performance of duties laid down in section 1(1) of the Police Act may only be collected and recorded in police personal data files established for the purpose of performing the duties in question. Information necessary for the performance of duties laid down in section 1(3) of the Police Act may only be recorded in police personal data files established for the purpose of performing the duties in question.

---

6 As of 1.1.2014 the police will have right, if it is likely that the message meant in the telecommunications interception cannot be acquired by the interception, to get the same information from a telecommunications operator or a corporate on the same conditions as the police is allowed to do telecommunications interception (information gathering instead of telecommunications interception). This a seizure type of measure. Act 872/2011, chapter 5 section 6, see also Helminen, Klaus - Fredman, Markku - Kanerva, Janne - Tolvanen, Matti - Viitanen, Marko: Esitutkinta ja pakkokeinot (The Criminal Investigation and Coercive Measures), Helsinki 2012 p.1038-1039 (later referred as "Helminen ym") Another new measure will be a systematic surveillance, which can be used against a person if there is a cause to suspect that he or she would commit an offence (as in surveillance). Systematic surveillance is meant to be use for longer periods of time than the surveillance, Act 872/2011 chapter 5 section 13, see also Helminen ym. p. 1059-1062.

7 The new Coercive measures Act 806/2011 will enter into force 1.1.2014.

8 See Helminen ym. p. 662-663.

9 Act 493/1995 chapter 3 section 36 (1): At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members or the employees of an organization…. Section 36 (2): The police have right to obtain from a telecommunications operator or a corporate or association subscriber, or by using a technical device, the contact information about a subscription that is not listed in a public directory or the data specifying a telecommunications subscriber connection, an e-mail address or other telecommunications address, or telecommunications terminal equipment if, in individual cases, the information is needed to carry out police duties…

10 See also Helminen ym. p. 582, where the conditions to give information seem to be even more strict.

Part (2) above was amended by the law 15.7.2005/529 as follows: For the use by one or more than one police unit a temporal police personal data register, other than mentioned in sections 2-5 and in sections 30 and 31, can be established for criminal analysis to prevent, detect or investigate an offence subject to imprisonment. In this register the police can combine, record and otherwise process data defined in sections 2-4, the data gathered by intelligence, surveillance or observation on a single crime and the data defined in section 14 (2). (translated by the writer). The Government bill [11] states that crime analysis is essential for preventing and investigating crime. It also notes that it has previously been unclear how widely the police can combine, record and process data gathered by intelligence and other police work in crime analysis.

Supreme Police Command has 12 January 2007 published a report on "Community Policing Strategy".[12] The report refers to the Hague Programme 2005 on intelligence-led policing: "it emphasises the significance of information gathering, analysis, threat and risk assessments and information exchange as a basis for effective policing. In the implementation plan of the Hague Programme community policing is held to be of primary importance in this respect, especially in local prevention of terrorism. According to the report, preventing policing can only be founded on accurate, dependable and (as far as possible) open and public information. Information supplied locally, by authorities and other interest groups, and by citizens concerning their environment, are increasingly important resources in terms of the direction and development of policing.[13] In practice, intelligence-led policing in Finland continues chiefly to refer to analysis serving police, customs and border guard cooperation and cooperation in the Baltic region. Up to now the question has been mainly one of operative analysis, although recently also more strategic analysis, which are based on mapping of the operating environment and on impact analysis. These are provided by the national Bureau of Investigation, regional crime analysis centres and provincial analysis units, similarly a small number of local analysis units".[14]

As stated above, the Finnish police use intelligence-led policing at least in local crime preventing. The police have a wide range of coercive measures at their disposal as well as access to various databases. Whether these measures can be called "building information positions", "data mining", or “data matching" is a question of definition.[15] Timo Laine has told that same coercive measures apply to cyber crimes as to all other crimes and they function in general reasonably well. There has, though, sometimes been problems in cases where the crime has been committed in the net. In some cases the crime committed has not been severe enough to allow telecommunications interception, which might have led to situations where the crime could not be properly investigated. Laine has stressed the fact that each agent has the right to use various registers only according to his or her job description. In addition, the agent can use the various registers only if he has a specific reason to do so, mere curiosity is not an acceptable reason. The use of various registers is being controlled.

There are various safeguards (appeal, complaint etc.) against the misuse of the measures.[16]

According to chapter 3 section 33 (Act 493/1995), the police officer…"shall, after the termination of technical surveillance, telecommunications monitoring or telecommunications interception, notify the person at whom the measure had been directed of the measure unless the notification endangers the purpose of the information gathering or the pre-trial investigation".[17]

The Ministry of Interior is obliged to give a report on the use of telecommunications monitoring and –interception to the Parliamentary Ombudsman once a year (Coercive Measures Act Chapter 5 section 15). The Parliamentary Ombudsman supervises among others the police. Thus, anybody who considers that an agent (the police) has acted unlawfully or neglected a duty in the performance of their tasks can file a complaint at the Parliamentary Ombudsman’s office. [18]

According to the Constitution of Finland, section 118, anyone who has suffered a violation of his or her rights or sustained a loss through an unlawful act or omission by a civil servant or other person performing a public task shall have the right to request that the civil servant or other person in charge of a public task be sentenced to a punishment and that the public organisation, official or

other person in charge of a public task be held liable for damages, as provided by an Act. This section has recently been amended and as of 1 January 2014 the injured party may bring a charge for an offence against a civil servant only if the public prosecutor has

11 HE 266/2004 p. 4, 29

12 Ministry of the Interior has 5.4.2006 assigned a committee, whose final report this publication is. In the report there are strategic outlines and objectives of community policing and security cooperation development. The report can be found in English at www.poliisi.fi. (later referred as "Community Policing Strategy").

13 Community Policing Strategy p. 14.

14 Community Policing Strategy p. 15.

15 Superintendent Timo Laine (National Police Board/Crime prevention unit) has told the writer that he does not recognize the expression "building information positions" in this context.

16 More on legal safeguards in Helminen ym. p. 720-730.

17 Act 872/2011, chapter 5 section 58, extends the obligation to notify the person concerned to apply also to undercover activities and also to the new measures of systematic surveillance and the information gathering instead of telecommunications interception with some exceptions. Act 806/2011, chapter 10 section 60, the suspect has to be informed of the use of secret coercive measures after the case has been brought to prosecutor or the pre-trial investigation has been finished. In some cases this notification can be postponed two years at a time and in some exceptional cases not to notify at all. The latter are exceptions from the main ruling. It is up to the court to decide on the exceptions. See also Helminen ym. 1140-1148.

18 Parliamentary Ombudsman Act (197/2002) Chapter 1, oversight of the legality, section 1, subjects of the parliamentary ombudsman’s oversight, section 2, a complaint. See also Helminen ym. p.729-730.

decided not to prosecute.

D. ICT in the criminal investigation

In Chapter 5a in the Coercive Measures Act there are rules on real-time collection of both traffic data and content data in criminal investigation.[19] Telecommunications monitoring and -interception are decided by a judge on an application by the law enforcement authorities. These measures are limited to certain serious crimes and they can be granted for a month at one time. Telecommunications companies are obliged to assist the law enforcement authorities in fulfilling the said coercive measures (Coercive measures Act, chapter 5 a, section 9).[20] There are no coercive measures to oblige the telecommunications companies to do so, but it seems that the telecommunications companies have not failed to help to fulfil the court orders. Telecommunications companies are entitled to get compensation for their financial losses in helping the law enforcement authorities.

The law enforcement agencies have the right to search and seize a thing or a document (Coercive Measures Act Chapter 4 Section 1) including data in a computer or in a similar system. Search and seizure can thus concern data.[21]

In the Coercive Measures Act there is a rule on technical observation (monitoring) (Chapter 5a, Section 4 a), A suspect or a place can be monitored via a technical equipment (the home/a room or space used for permanent living of the suspect is excluded). If the suspect is in the custody of the law enforcement authorities or if equipment is installed in a car of the suspect or other place where the suspect is staying (not the home), a court decision is needed. The enforcement agencies have the right to enter secretly the premises where the equipment is to be installed (translated by the writer).

In criminal investigations, it has been common practice to videotape the interrogations of young persons (under the age of 15) in order to protect them from the harms of a court hearing.[22] In the new law on criminal investigation (Criminal Investigations Act, 805/2011, entry into force 1 January 2014), the law enforcement authorities may videotape all the interrogations partly or totally (chapter 9, section 3 and 4) and they must record the interrogations of the injured party (complainant) and the witnesses who cannot be heard in the court without causing them harm due to their young age or mental incapacity.[23] From the rules it follows that there is a possibility but no obligation to record the interrogations.

E. ICT and evidence

In the Code of Judicial Procedure (chapter 17) there are rules on evidence (concerning all evidence including electronic evidence). The chapter 17 section 2 in the Code of Judicial Procedure states the principle of free judicial evaluation of evidence.[24] This has been understood as the right for the court to use any fact brought to its knowledge in the case as evidence and the freedom to evaluate its importance as proof.[25] In the present legislation there are no rules on admissibility or exclusion of the evidence in criminal matters.

A group of experts has recently laid down a proposal[26] for some changes regarding chapter 17 in the Code of Judicial Procedure. Most of the proposed changes have already been accepted by the precedents of the Supreme Court and hence also in the court practices in general. The decisions of the European Court of Human Rights have had an impact on the Finnish jurisprudence in this area.[27] One example is that evidence gathered by torture cannot be used as evidence. Secondly, there are also restrictions on under which circumstances a piece of evidence obtained unlawfully can be used in court.[28] Thirdly, evidence gathered for example in taxation cannot be used against the suspect in the criminal proceedings if it were to violate the principle of self-incrimination. The proposal suggests that these restrictions be legislated.[29] It has already been ruled (chapter 17, section 11.2[30]) under which circum-

19 Understood as telecommunications interception and telecommunications monitoring as well as technical surveillance, which all can be used also in crime preventing.

20 Communications Market Act 393/2003, section 95: "Obligation of a telecommunications operator to equip its systems for telecommunications interception and monitoring. A telecommunications operator shall equip its communications network and communications service with technical instruments and features that allow the interception of electronic communications and telecommunications monitoring as referred to in the Coercive Criminal Investigation Means Act (450/1987), the Police Act (493/1995), and the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union".

21 Supreme Court 2001:39, 2009:4 and Helminen ym. p. 899-890.

22 Helminen ym. 473. According to the finish law people under the age of 15 cannot be prosecuted.

23 more detailed in Helminen ym. p. 491-496.

24 17:2.1:"After having carefully evaluated all the facts that have been presented, the court shall decide what is to be regarded as the truth in the case".

25 Helminen ym. p. 507

26 Reports and Statements 69/2012 (later referred as "69/2012")

27 Human rights considerations have restricted the principle of free evaluation on evidence. See Pihlajamäki p. 10.

28 Supreme Court 2007:58; The evidence obtained illegally can be used in court if the proceeding as a whole conforms with the principle of fair trial.

29 See 69/2012 p. 47-48.

30 17:1.2: "If the statement given in a pre-trial criminal investigation by a person who has not reached the age of 15 years or a person who is mentally incapacitated has been recorded on a video recording device or on a comparable video and audio recording, the statement may nonetheless be admitted as evidence in court if the defendant is provided with an opportunity to present questions to the person being heard". 69/2012 p. 116 proposes that this possibility to be extended to certain sexual offences.

stances a hearing recorded on video can be accepted as evidence in court.[31] According to the proposal, this ruling should be extended to the injured party of certain sexual offences.[32] In addition, there are rules according to which a person cannot testify[33] and rules according to which a witness can refuse to testify. [34]

Electronic evidence is regarded as written evidence in the same way as documents.[35] There are no specific rules on ICT related evidence, not on its admissibility, discovery, disclosure or evaluation.

F. ICT in the trial stage

According to chapter 17 section 11 b 1): "A document to be presented as evidence shall be delivered to the court in the original unless the court deems it sufficient that it be presented as a copy." In court practices copies are regularly accepted. [36] There are no other special rules on how the evidence in general or ICT related evidence in particular can or must be introduced in the trial: it is possible to use copies of computer files, presentation of digital information on projectors, expert reports etc. [37] As we continue to have paper court records, the evidence also has to be in "concrete" form,. The following statement of evidence presentation especially in the case of electronic evidence is illustrative: "The results of the forensic activities/digital evidence should be presented in a clear matter, without interpretations. They have to be easy to understand by the prosecutors and judges who have usually less technical knowledge".[38]

There are no rules on reconstruction but the reconstruction of events is used in rare cases in criminal investigation. There is no obstacle to use digital or virtual techniques in the reconstruction.[39]

As stated in the report for section 4, evidentiary hearings via video can be used in national criminal cases since 1 October 2003. Cross-border proceedings can also be organised by a video conference according to legal aid conventions. As noted earlier videotaping will be possible in more cases as of 1 January 2014 in criminal investigation. The Finnish courts have in general adequate electronic equipment for the various forms of evidence presentation.

In the public administration there is a tendency towards paperless administrative processes. [40] As an example in the judicial field is a project started by the Ministry of Justice in 2010 (OM 21/31/2007) with the aim to create a common IT-based system for the whole judicial administration. At the moment the different actors use non-compatible IT-systems. After the completion of the project, the files could be delivered electronically from the law enforcement agencies to the courts. The aim is to have a management process that is completely paperless, including an electronic archive. The time frame is still open, but the system is unlikely to be ready before the year 2018.

31 See also Supreme Court 2006:107
32 69/2012 p. 47.
33 Chapter 17 Section 23: The following may not testify:1) a public official or a person elected or appointed to a public function or duty in respect of what he or she is bound to keep in secret in this function: 2)…
34 The Code of Judicial Procedure Chapter 17 Section 20: A person may not refuse to testify. However, the following need not testify against their will: 1) a person who is or has been married or is engaged to one of the parties, 2) a person…
35 69/2012 p. 23
36 69/2012 p. 135: While the copies are technically as good as originals, proposal is been made that a copy of a document can be presented in court unless the court otherwise requires.
37 see UNODC p. 166-167.
38 CyberCrime@IPA Project of the Council of Europe and European Union. Version 9.11.2011 p. 52
39 More on reconstruction in Helminen ym. p. 569-571. The reconstruction of a traffic accident was made by the National Bureau of Investigation in Supreme Court case 1991:23.
40 Chapter I section 1 of the Act on Electronic Services and Communication in the Public Sector (13/2003) states as the objective of the Act the improvement of the smoothness and rapidity of services and communications as well as information security in the administration, in the courts and other judicial organs and in the enforcement authorities by promoting the use of electronic data transmission.