Preparatory Colloquium
Helsinki (Finland), 10-12 June 2013.
Section IV : International Criminal Law

AIDP FINLAND: NATIONAL REPORT ON SECTION 4*

Karri TOLTTILA[1]

1. **General: cybercrimes in Finland**

The Finnish Criminal Code (CC) does not give one single clear definition of a cybercrime. The provisions on cyber offences are widely dispersed in different chapters (28, 34, 35, 36 and 38) of the Criminal Code (CC).[2] The protection of both the information system and the administration system has been given an independent position as an object of legal protection by placing all information and communication crimes in chapter 38 in the CC.[3] This last mentioned chapter on information crimes regulates the following offences: interference with communications (CC 38:5-7), interference in a computer system (7a-b §), computer break-in (8-8a §), offence involving an illicit device for accessing protected services (8b §) and data protection offence (9 §). The legislative technique shows that the idea has both been to revise existing crime definitions in order to reflect new developments and also to create new provisions. In the year 2007, Finland amended a number of the provisions of the CC on cyber offences in order to harmonize them with the Council of Europe Convention on Cybercrime in connection with the process for the ratification of the Convection.

A cybercrime is generally understood as a crime that has a computer system as its object, tool or place of offence.[4] 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".[5] The object of the crime is usually defined as being *data* (for example in the provision of interference in a computer system) or *information* (computer break-in). The criminal conduct (*actus reus*) has no typical definition. The description of both the act and the consequence is normally used (as in the offence of computer fraud). As a rule, a computer crime is punishable only as an *intentional* act (see also CC 3:5.2).

The cybercrime offences can be regarded as having a transnational element to the extent that they are defined in a way to be harmonized with international or European law obligations binding on Finland, especially the Convention on Cybercrime. The definitions of cybercrime offences or the general rules on commission or participation do not contain jurisdictional elements such as the place of commission of the offence. Jurisdictional rules are regulated in the general part of CC, more precisely in its chapter 1 (see below 2).

Corporate criminal liability was introduced in Finland in 1995. It is applicable when such liability is provided specifically for the offence in question, for example for computer fraud (CC 36:1.2) and information offences (CC 38:5-8a). If Finnish law applies to the offence according to the jurisdictional principles, Finnish law applies also to the determination of corporate liability (CC 1:9).

---

* 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.M., Doctoral Student at the University of Helsinki (Finland). Chapters 1–2 and 4-5 of the report are based on draft work done by LL.M. *Liisa Mäkelä*, Doctoral Student at the University of Helsinki. Liisa Mäkelä is also the author or co-author of the Finnish national reports on sections 1 and 2 of the preparatory colloquia for the AIDP 19th International Congress on Information Society and Criminal Justice.

[2] An unofficial translation of the Finnish Criminal Code (1889/39) is accessible at the website of Ministry of Justice: http://www.finlex.fi/laki/kaannokset/1889/en18890039.pdf. The provisions in the chapters mentioned above are the following: unauthorized use (28:7), criminal mischief (34:1), endangerment of data processing (34:9 a), possession of a data system offence device (34:9b), criminal damage (35:1) and computer fraud (36:1.2).

[3] See Government Bill 94/1993, p. 133.

[4] This is the position in Finnish legal doctrine; see Lehtimaja, Lauri: Eurooppalaisesta atk-rikospolitiikasta [European computer-crime policy]. In: Rikosoikeudellisia kirjoitelmia VI (ed. Raimo Lahti), Suomalainen Lakimiesyhdistys 1989, p. 260.

[5] Citation from Pihlajamäki, Antti: The Protection of Data Processing under Criminal Law, an English summary (pp. 285-290, 286) in his doctoral thesis, Tietojenkäsittelyrauhan rikosoikeudellinen suoja, Datarikoksia koskeva sääntely Suomen rikoslaissa, Suomalainen Lakimiesyhdistys 2004. Pihlajamäki has also written about cybercrimes in an earlier Finnish national report for AIDP: see Pihlajamäki, Antti: Computer Crimes and Other Crimes against Information Technology in Finland, Revue Internationale de Droit Pénal (1993), pp. 275-289.

2. Jurisdictional issues

2.1 Place of commission

In Finland, an offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent. If the offence remains an attempt, it is deemed to have been committed also where, had the offence been completed, the consequence contained in the statutory definition of the offence either would probably have become apparent or would in the opinion of the perpetrator have become apparent. An offence by an inciter and abettor is deemed to have been committed both where the act of complicity was committed and where the offence by the offender is deemed to have been committed. If there is no certainty as to the place of commission, but there is justified reason to believe that the offence was committed in the territory of Finland, said offence is deemed to have been committed in Finland. (See CC 1:10.)

Cybercrimes can be committed anywhere: the only requirement is an internet connection.[6] It is often difficult to define precisely the place where the cybercrime offence was committed. In Finland, there is no clear view on the question where a cybercrime is committed: it could be either where the service provider is situated[7] or there were the act took place. According to Asko Lehtonen, who is a specialist in the field of IT-law, most cybercrimes are committed where the primary action is performed: this applies to so-called data vandalism (destruction of another's computer file, database, and web pages, or sending a computer virus that causes harm), falsification of documents, and copyright infringement by making illegal copies or making them available to the public, hacking and unlawful use of another's computer.[8]

If damage has been caused to data or information on a server, the territory where the server is situated determines the place of the crime effect. Also the provision on computer fraud (CC 36:1.2)[9] requires that the consequence of the offence has to be both distortion of the result of the data processing and the causing of economic loss. If computer fraud is committed from a foreign state and directed at a Finnish company, also the effect or consequence of the offence emerges in Finland. A defamation offence (CC 24:9) can be committed by sending an email from one country to another. The country where the email arrives determines the place of crime effect.[10]

2.2 The scope of application (jurisdiction) of Finnish criminal law

The scope of application of the criminal law of Finland is regulated in chapter 1 of the CC, which was fully amended in 1996.[11] The scope of application of Finnish criminal law is wide, and the principles concerning the connection to Finland include the following: the territorial principle (CC 1:1), the flag principle (CC 1:2), the protective principle (CC 1:3), the passive personality principle (CC 1:5), the active personality principle (CC 1:6), the universality principle (CC 1:7) as well as the principle of vicarious administration of criminal justice or the representation principle (CC 1:8). Accordingly, Finnish criminal law applies not only to an offence committed in Finland (1:1), but also to an offence committed by a Finn (1:6) or an offence committed outside of Finland that has been directed at Finland (1:3).[12] Finnish criminal law also applies to an offence committed outside of Finland that has been directed at a Finnish citizen, a Finnish corporation, foundation or other legal entity, or a foreigner permanently resident in Finland if, under Finnish law, the act may be punishable by imprisonment for more than six months (1:5).

2.3 Cybercrimes as universal crimes?

For international crimes, such as terrorism and drug-related offences, the scope of their application is defined as universal, which means that the national criminal law is applicable universally (CC 1:7 and the related Decree): Finnish law applies to an offence committed outside of Finland where the punishability of the act, regardless of the law of the place of commission, is based on an

---

[6] Clough, Jonathan: The Council of Europe Convention on Cybercrime: Defining 'Crime' In a Digital World. Criminal Law Forum 2012, pp. 363-391, 370.

[7] Lehtonen, Asko: Straffrättslig jurisdiktion över internetbrott. In: IT och juristutbildning. Red. Wahlgren, Peter. Nordisk årsbok i rättsinformatik 2000. Stockholm 2001 (also accessible at the website of the University of Vaasa).

[8] Lehtonen, Asko: Tietotekniikkaoikeus [IT-law]. The internet publication is accessible in Finnish at the website of the University of Vaasa.

[9] CC 36:1 in extenso: (1) A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud to a fine or to imprisonment for at most two years. (2) *Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud.* (3) An attempt is punishable.

[10] Lehtonen, Asko: Straffrättslig jurisdiktion över internetbrott. In: IT och juristutbildning. Red. Wahlgren, Peter. Nordisk årsbok i rättsinformatik 2000. Stockholm 2001.

[11] As to the draft proposal for the reform of the Finnish provisions on criminal jurisdiction, see chapter IX – with the articles by Per Ole Träskman, A. H. J. Swart, Iain Cameron and Karin Cornils – in: Criminal Law Theory in Transition; Strafrechtstheorie im Umbruch (eds. Raimo Lahti & Kimmo Nuotio), Finnish Lawyers' Publishing Company 1992, pp. 511-586.

[12] An offence is deemed to have been directed at Finland (1) if it is an offence of treason or high treason, (2) if the act has otherwise seriously violated or endangered the national, military or economic rights or interests of Finland, or (3) if it has been directed at a Finnish authority (CC 1:3.2).

international agreement binding on Finland or on another statute or regulation internationally binding on Finland (so-called *international offences*). Further provisions on the application of the section are issued by Decree.

According to Minna Kimpimäki, who is a specialist in issues of universal jurisdiction,[13] Finland's universal jurisdiction does not play a significant role when it comes to questions related to cybercrime and jurisdictional issues. The Decree on the application of chapter 1, section 7 of CC does not contain any provisions on actual cybercrimes. It is still possible that some universal crimes mentioned in the Decree could be committed by using a computer network, such as drug-related offences and the financing of terrorism. Also different forms of sabotage can be directed at information networks dealing with air traffic or maritime transport. Different forms of participation in crimes, categorized as universal crimes – and especially incitement– could be fulfilled through the use of a computer network. In Finland there has been a cautious tendency in criminal policy towards the criminalization of preparation of and participation in offences.[14]

Finnish legislation has defined universal jurisdiction widely. In practice, universal jurisdiction has been applied very seldom, actually in only one case.[15] This means that it is not very likely that a cybercrime, even when committed as a universal crime, would fall under Finnish jurisdiction in a case which has no connection to Finland. Bringing charges requires an indictment order by the Prosecutor General of Finland.

It is more important to define the place where cybercrime is committed than to assess whether or not a specific cybercrime would be a universal offence under Finnish jurisdiction.[16]

It should also be noted that the representation principle may be applicable instead of the universality principle. Accordingly, Finnish criminal law applies to an offence committed outside of Finland which, under Finnish law, may be punishable by imprisonment for more than six months, if the State in whose territory the offence was committed has requested that charges be brought in a Finnish court or that the offender be extradited because of the offence, but the extradition request has not been granted (CC 1:8).

2.4 The requirement of double criminality

The main rule in the provision on the requirement of double criminality (CC 1:11.1) states the following: If the offence has been committed in the territory of a foreign State, the application of Finnish law may be based on sections 1:5 (passive personality principle), 1:6 (active personality principle)[17] and 1:8 (representation principle) only if the offence is punishable also under the law of the place of commission and a sentence could have been passed for it also by a court of that foreign State. In this event, no sanction that is more severe than what is provided by the law of the place of commission may be imposed in Finland.

2.5 Some examples of jurisdiction over certain cybercrime offences

In 1997, the Committee of Ministers of the Council of Europe adopted a Recommendation on hate speech. The European Court of Human Rights has later in its case law developed further this definition of hate speech. The Additional Protocol to the Convention on Cybercrime, adopted by the Committee of Ministers on 11 July 2002, requires member states to criminalize acts of a racist or xenophobic nature via networks, racist and xenophobic threats and insults and dissemination of such material, denial of the Holocaust and other genocide. The basic Finnish definition for hate speech can be derived from the provision on *ethnic agitation* (CC 11:10), which was amended in 2011 and has the following contents:

> A person who makes available to the public or otherwise spreads amongst the public or keeps available for the public information, in the form of an opinion, message, statement or other information, by which a certain group is threatened, defamed or insulted on the basis of its race, skin colour, ancestry, national or ethnic origin, religion, belief, sexual orientation or disability or any other ground comparable to these, shall be sentenced for *ethnic agitation* to a fine or to imprisonment for at most two years.[18]

---

[13] Minna Kimpimäki is working as assistant professor at the University of Lapland, Faculty of Law. She prepared her doctoral thesis on The Principle of Universality in International Criminal Law, in Finnish Universaaliperiaate kansainvälisessä rikosoikeudessa, Suomalainen Lakimiesyhdistys 2005 (Summary in English). The information from Kimpimäki in this article is based on an interview conducted on 10 December 2012.

[14] In regards to the expanding liability for preparation and participation of offences, see especially: Lahti, Raimo & Sahavirta, Ritva: The expanding forms of preparation and participation**.** Finland (National report). Revue Internationale de Droit Pénal, 2007, 78:3-4, CD Rom annexe, pp. 101-115 (2008).

[15] See Kimpimäki, Minna: Genocide in Rwanda, Is It Really Finland's Concern? International Criminal Law Review 1/2011, pp. 155-176.

[16] Minna Kimpimäki 10 December 2012

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

[18] Free translation by Liisa Mäkelä.

To spread illegal web-content is an abstract endangerment offence, meaning that the essential elements of the offence do not require a separate consequence.[19] The provision is easily and usually connected with another offence, such as defamation (CC 24:9-10), coercion (CC 25:8), public incitement to an offence (CC 17:1), breach of the sanctity of religion (CC 17:10), or even incitement to war (CC 12:2).[20] Some of these offences that can be connected with hate speech are so-called international offences, based on an international agreement binding on Finland or on another statute or regulation internationally binding on Finland (CC 1:7); see above 2.3.

According to the Finnish State Prosecutor Mika Illman**,** who is an expert in questions of ethnic agitation, ethnic agitation is classified as an offence where the scene of the crime plays the determinative role. The place where the unlawful statement has been drawn up (the place of writing) and the place where the offender made the decision to make the statement public, could be seen as the most relevant scene of the crime. It is also possible to pay attention to what was the "audience group" which the offender had targeted. If the statement is written in the Finnish language, it can easily be seen to be aimed at a Finnish audience. In practice the offender mostly composes and makes the material public from a home-computer, meaning that the offender's hometown is to be regarded as the scene of the crime. Since possession of racist material is not punishable, the place where the racist material has been submitted to the audience is conclusive for the determination of the crime scene. This could also be a place other than the place of writing: if the statement is published online on the internet, the location of the editorial web publication can be seen as the most reasoned scene of crime.[21]

Public incitement to an offence is a crime which requires the causing of a certain danger, meaning that there are several possible places of the commission of the crime (CC 17:1). The crime can be seen to be committed where the message had been written (a), where the message had been made public (b) or where the danger as an essential element of the crime had been caused (c).[22]

The Helsinki Court of Appeal has given a judgment[23] on the question of what was the scene of the crime in a case involving internet-based ethnic agitation and how the requirement of double criminality should be solved in relation to the prosecution, when the server that was used for the circulation of unlawful statement was located abroad. The respondent had made his statements available from his home computer to a server maintained by an Australian party on an American server. The defendant claimed that the prosecutor had not even argued that the requirement of double criminality would have been met, and that the prosecution should be ruled inadmissible or disallowed. The Helsinki Court of Appeal examined the prosecution and found the defendant guilty as charged. The Court emphasized that the key role in the assessment of the crime scene has to be given to the offender's aim of spreading the statements to the audience. The language that the statements had been written in has a central role. It is generally known that the Finnish language is mainly used in Finland. Therefore, if the statements are spread on the internet in Finnish, the statements have been readable all over the country (Finland). This leads to the conclusion that the dissemination has taken place in Finland. Since Finland could be located as a place of commission of the offence, there was no need to examine the requirement of double criminality.

Also another judgment, given by the Finnish Supreme Court (case KKO 2005:27 on the Lotteries Act), shows that the geographical location of the server that maintains a web page does not have a crucial role in determining the scene of the crime and the competence of the Finnish authorities. The location of the server is most relevant in cases where the server is situated in a country that does not deliver traffic data to the Finnish authorities for the investigation of hate crimes. In these cases the crimes sometimes remain unsolved.[24]

2.6 National rules on settlements of jurisdiction conflicts

The Convention on Cybercrime provides a negotiation obligation in respect of questions concerning the interpretation and application of the convention (article 45). In June 2012 Finland has approved a new Act on the prevention and resolution of jurisdiction conflicts in criminal procedure. The new law also regulates pre-trial investigation and the transfer of prosecution between Finland and other EU Member States. The negotiation mechanism is based on European Framework decision 2009/948/YOS. There exists as yet no practice on the last-mentioned negotiation mechanism.

[19] In Finland, since the amendment of CC 10:11 in 2011, also webmasters may be held responsible for hate messages posted on their internet pages. After the 2011 amendment, the description of the criminal act includes "keeps available information" as a modus operandi.
[20] Office of the Prosecutor General: Rangaistavan vihapuheen levittäminen Internetissä [Criminal dissemination of hate speech on the Internet], Draft 12042012 (2012) accessible in Finnish language at the National Police website (www.poliisi.fi).
[21] This information is based on an interview with Mika Illman conducted on 14 November 2012. Mika Illman prepared his doctoral thesis on incitement to racial hatred. See (in Swedish) Illman, Mika: Hets mot folkgrupp, Suomalainen Lakimiesyhdistys 2005; Abstract in English. See also Illman, Mika: Uudistunut säännös kiihottamisesta kansanryhmää vastaan [New provision on ethnic agitation], Oikeus 2012 (41):2.
[22] Mika Illman 14 November 2012.
[23] Helsinki Court of Appeal 22 September 2009 nr 2370 (R 08/1382; no longer subject to appeal).
[24] Mika Illman 14 November 2012

3. Cooperation in criminal matters

The most important multilateral conventions in Finland are the Council of Europe's European Convention on Mutual Assistance in Criminal Matters (the 1959 Convention) and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (the MLA 2000 Convention) as well as the Protocol thereto concluded in 2001.

Criminal aid in legal matters is regulated by the Act on International Legal Assistance in Criminal Matters (1994/4) and the Decree on International Legal Assistance in Criminal Matters (1994/13).

The act goes a long way to meet the international agreements that Finland has ratified. The aim is to provide legal aid to the widest possible extent, also covering non-agreement situations.

In Finland the Ministry of Justice functions as the Central Authority. A request may also be sent directly to a competent Finnish authority. The National Bureau of Investigation (NBI) retains a major role in mutual assistance in Finland. Mutual assistance between the Nordic countries functions traditionally through direct contacts.[25]

A request to a foreign jurisdiction is to be sent in accordance with the applicable convention or agreement, or in the absence of such, in a manner required by that jurisdiction. The 1959 Convention provides that requests concerning service of documents and/or taking of evidence be sent to the Central Authority (usually the Ministry of Justice) which will then channel the request to the competent authority for execution.

Along with the entry into force of the MLA 2000 Convention, service of documents by mail and direct contacts between the locally competent authorities have become prevalent.

The Finnish police have a major role in requesting and giving legal aid in criminal matters, because the police are the director of pre-trial investigations in Finland, an arrangement which is exceptional in Europe. In many cases the police deal with requests without the participation of the prosecution, the court or the Ministry of Justice.[26] The Ministry of Justice serves as the Central Authority in questions of legal aid. A foreign request for legal aid is executed by the Finnish authority in whose jurisdiction the question belongs (for example, the police take care of pre-trial hearings, and the court conducts examinations of witnesses during the trial). As a rule, the request is sent from the NBI for enforcement to the local police. However, for example, telephone interviews can be enforced by the NBI. According to the Act on International Legal Assistance in Criminal Matters (14 §), it is usually the authority which is responsible for the execution which also has the power to decide on refusal of legal aid. As a general rule, however, legal assistance is always possible when the corresponding measure in a similar situation would be possible in Finland.

A foreign authority can also ask for the right to be present during the police hearings. In addition, a foreign authority may also be authorized to be present during a search of the premises, or to assist in the interception of telecommunications in a foreign language. Practical preparations, however, must always be left to the Finnish State authorities, so that this is done in accordance with the Finnish Criminal Investigations Act. Fulfilling the request procedure is, therefore, done in accordance with Finnish law. It is important to notice that if the use of coercive measures should be needed, also the requirement of double criminality has to be fulfilled. For example, remote surveillance information can be obtained from Finland only if it would be allowed in a similar Finnish case. Coercion measures such as interception of telecommunications in Finland must always be authorized by a Finnish district court. Finnish national law also allows extraterritorial investigations as regulated in the national Coercive Measures Act and in the 1959 Convention and the MLA 2000 Convention.

The Finnish police do not have competence of its own to investigate cybercrimes abroad without the permission of, and legal aid from, the country's authorities where the crime is suspected to have been committed. The NBI is in charge of questions on executive assistance and legal aid.

4. International cooperation in criminal investigation and crime detection

4.1 Self service, joint investigations and exchange of information

Self service, by the means of obtaining evidence in another state without asking permission, is not permitted by Finnish legislation. However, the establishment of a *joint investigation team* (JIT) means that it is possible to come close to self service. A JIT can be established on an agreement basis between two or more EU member states in order to investigate a particular crime or a larger crime entity. Within a JIT it is possible to directly exchange information without separate requests for legal assistance.[27] The establishment of a JIT enables investigations within the framework of the agreement; for example, separate requests on legal aid for searches or police interrogations (which are the most common ones in Finland) are then not needed.

Finland, as a EU member state, is a party to international agreements that enable information exchange on Passenger Name Records (PNR) and DNA data. These agreements are implemented into national law by laws and decrees. In Finland, DNA samples

[25] As to Nordic cooperation in general, see in more detail Tolttila, Karri: The Nordic Arrest Warrant: What Makes for Even Higher Mutual Trust? New Journal of European Criminal Law, vol. 2, 2011/04, pp. 368-377.
[26] Evaluation Report on Finland on Mutual Legal Assistance and Urgent Requests for the Tracing and Restraint of Property (2010), accessible also in English at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/polju/en/EJN346.pdf
[27] JIT makes direct information change possible without assistance by the NBI or the Ministry of Justice.

are used in both crimes against life and crimes against property.[28] The grounds for taking DNA samples are regulated in the Coercive Measures Act and the Police Act. According to the Coercive Measures Act (5:11; 646/2003), the police has the right to take a DNA sample from a person who is suspected on probable reasons for a crime for which the maximum penalty is more than six months imprisonment, and in the case of driving while intoxicated (CC 23:3) and unlawful use of narcotics (CC 50:2a). If the suspect is later found not to be guilty, the DNA samples must be destroyed.

In 2009, Finland started wide-scaled collaboration on DNA exchange with the Netherlands. The information exchange takes place each night. The collaboration expanded with new collaborating countries, such as Germany, Austria, Spain, Slovenia and Luxemburg. In 2011, the collaboration encompassed all EU countries. Previously Finland had exchanged information only with Estonia on the basis of an agreement. According to an agreement between Finland and the USA, it has been possible since August 2012 to exchange DNA information, fingerprint information and also other information on serious crimes and terrorist crimes between the countries.

Finland has been a member of INTERPOL since the year 1928. INTERPOL's communication channel is ready for information exchange on a 24/7 basis, and it also allows direct access to some international databases. The National Bureau of Investigation is working as Europol's national unit in Finland. Finland has three liaison persons at Europol, two from the police and one from the customs. Finland's representative in EUROJUST is a prosecutor assisted by a police liaison from the Finnish National Bureau of Investigation.

4.2 Illegal information on the web (notice and take down)

Directive 2000/31/EC lays down a rule according to which a service provider can avoid civil responsibility for damage by instantly taking down illegal material from its service on been given notice of such material (*the notice and take down -rule*). In Finland, a service provider can be held legally responsible for websites containing illegal and racist material. The operator can be held responsible for this kind of material if the operator doesn't on its own initiative remove clearly illegal material after having received notice of its illegal contents, or if the operator doesn't obey the court order to remove the material. This kind of conclusion can be made on the basis of the statement given by the Legislative Committee of Parliament when it examined the Government Bill on the reform of the provision on ethnic agitation (CC 11:10).[29]

5. Future developments and human rights concerns

Cybercrimes can be committed anywhere; the only requirement is an internet connection.[30] Cybercrime offences are a matter that a state cannot regulate on its own. Because cybercrimes do not respect the borders of countries, the harmonization of legislation plays an essential role in the fight against cybercrimes. Under-criminalization or the absence of criminalization might lead to international criminality moving to countries where the penalties are weak or non-existent.[31] Harmonization is extremely important for cooperation in criminal matters.[32] Optimal harmonization includes that all countries assert jurisdiction over cybercrimes to the widest possible extent. In this way there are no safe havens for cybercrimes or places where criminal cooperation is impossible.[33]

It may be mentioned that evidentiary hearings via video screen have been possible in national criminal cases in Finland since October 2003 (Criminal Procedure Act 1997/689, amendment 360/2003).[34]

Transnational cases are regulated by law,[35] general principles of law and acts by the EU or international agreement. If the person to be heard is not within Finland's borders or at a place to which Finnish legislative power extends, it is necessary to ask for international legal aid in order to hear the person. Finland can also be the one which offers legal aid to another country by organizing a video conference.

Rapid technological development is an asset to criminal investigations using information technology, such as interception of telecommunications. These investigations violate the suspect's fundamental rights, particularly the freedom of expression and the right to privacy, and a reasonable balance should be found between these rights and interests.

Finland ratified the European Convention on Human Rights in 1989 and this came into force in respect of Finland the following next year. Besides Article 6 of the convention, the principle of the *right to a fair trial* is guaranteed by the Finnish Constitution (section

[28] All EU countries decide by themselves the grounds for taking DNA samples from suspects and convicted persons.
[29] Committee report 39/2010, p. 3 (Government Bill 317/2010). See also Hannula, Ilari & Neuvonen, Riku: Internetin keskustelupalstan ylläpitäjän vastuu rasistisesta aineistosta [Liability of the site administrator for racist material posted on an Internet discussion forum], Lakimies 3/2011, pp. 527-548, 544. Cf. above 2.5.
[30] Clough, Criminal Law Forum 2012, p. 370.
[31] See Lehtimaja 1989 (note 4), p. 260.
[32] Clough 2012, p.365.
[33] Clough 2012, p. 370.
[34] An unofficial translation of the Criminal Procedure Act is accessible at the web site of the Ministry of Justice: http://www.finlex.fi/fi/laki/kaannokset/1997/en19970689.pdf
[35] According to the Code of Judicial Procedure (17:11a), separate provisions apply to the admission of evidence abroad.

21).[36] Finland does not follow any exclusionary rule doctrine that would require the Finnish court to reject certain evidence, such as evidence that has been illegally obtained. According to the Code of Judicial Procedure (1734/4), the court evaluates all evidence on a free basis, in a search for the material truth (17:2: the principle of free evaluation of evidence). It has, however, long been clear that evidence obtained clearly and grossly against international human rights standards, such as a confession obtained by torture (article 3), violating the right to a fair trial, is inadmissible, whether the proof was obtained by Finland or another state. Evidence obtained by the police against the law (such as through illegal interception[37]) is inadmissible if it makes the whole proceeding unfair (in the sense of article 6 of the convention). A judgment cannot be primarily or entirely based on illegally obtained evidence.[38] The Supreme Court of Finland has in a recent precedent stated that evidence obtained in violation of the privilege against self-incrimination is forbidden (KKO 2012:45). At the moment a proposal to reform the Code of Judicial Procedure is pending. A new section is proposed (17:25) that would be formulated as follows:

> The court may not use evidence that is obtained by torture. The Court also has to leave unexploited illegally obtained evidence, if there are strong reasons for this, taking into account the nature of the issue, the method of acquisition of the evidence related to the seriousness of the infringement, the importance of the method of acquisition in respect of the reliability of the evidence, the importance of the evidence to the decision and other conditions.[39]

[36] An unofficial translation of the Finnish Constitution is accessible in English at http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf
[37] Also, if the court has granted permission for interception/monitoring of telecommunications, the evidence acquired in this way may be used only for the same purpose for which the court had earlier given permission.
[38] See for example *Case of Ramanauskas v. Lithuania* 5 February 2008. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-84935#{%22itemid%22:[%22001-84935%22]}
[39] Free translation by Liisa Mäkelä.