Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

SWEDEN*

(B) Legislative Practices and Legal Concepts

(1) Swedish criminal laws related to cyber-crimes are not contained in a unified title or code. They are to be found in the Swedish Criminal Code (*SCC*, *brottsbalken*) in various places. The crime *data intrusion* are, for example, to be found in the fourth chapter of the SCC, concerning *crimes against freedom and liberty* and the crime *computer fraud* are placed in the ninth chapter of the SCC, concerning *fraud and other types of misconduct*.

(2) The impact of judicial decisions in the formulation of criminal law related to cyber-crimes cannot be said to be so great. Of course, the judges and courts have to apply the laws set by the legislative body in specific cases and interpret the laws, but not more than that. Since it is about criminal law the scope to extend the application of the law is rather restricted, as well.

(3) Sweden has not yet used the technique *recasting* when it comes to cyber-crimes.

(C) The Specific Cybercrime Offenses

(1) In Swedish law cybercrime offenses must be intentional, but they do not require a specific intent.

(2) There are no negligent offenses in the field of cybercrime offenses.

(3) See the answer under 2.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

In Swedish law the serious hindering, without right, of the functioning of a computer and electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program *is* a criminal offense (*data intrusion*, 4 chap. 9 c § SCC*).*

b. Requirement of infringement of security measures?

It is *not* a requirement in Swedish criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access.

2. Data and system interference

a. Object – protection of system/hardware/data?

Swedish criminal law does *not* specifically define “computer” or ”electronic data”. In Swedish law, a lot that goes under the definition of ”cyber-crime” is criminalized by one particular article in the Swedish Criminal Code (*4 chap. 9 c § brottsbalken*). According to this article a person should be convicted of *data intrusion* (*dataintrång*) if he unlawfully gives himself access to *data intended for automated processing* or if he unlawfully modifies, deletes, blocks or in a registry adds such data. The same applies to a person who unlawfully by a similar action is seriously interfering with or hindering the use of such data. Since the object is *data intended for automated processing*, programs and software fall under the scope of the article.

---

* 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.

b. Act – destruction/alteration/rendering inaccessible?

i. Swedish penal law *does* penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program. See the description of the article on data intrusion under 2a above.

ii. Swedish penal law *does* penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and information, at least as long as the transmission is not made by radio waves, since there is a principle in Swedish law that anyone has the right to freely pick up radio waves in the air.

3. Data Forgery

a. Object – authenticity

For the moment Swedish penal law *does* – to some extent – define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes if the act implies a risk that the data is to be taken for authentic. The article in the Swedish Criminal Code concerning forgery (*14 chap. 1 § brottsbalken*) is however constructed with tangible objects in scope. It is not totally clear to what extent a conduct consisting in manipulation of digitally stored data falls under the scope of the article, though the Swedish Supreme Court in some cases has applied the article in such a context (e.g. NJA 2009 p. 111). In 2005 the Swedish Governement appointed a committee to look into this matter. In 2007 the inquiry – "The Inquiry on IT- forgery" (*It-förfalskningsutredningen*) made a proposition for an amended version of the article on forgery in the Swedish Criminal Code aiming at making it applicable to electronic documents as well. The proposition is currently being prepared by the Swedish Government Offices.

b. Act – alteration/deletion?

See the answer under 3a above.

4. Misuse of Devices

a. Object – type of device?

Swedish criminal law *does*, to some extent, criminalize the development of a hacker's "tool kit" or any part of it for the unauthorized access to computer or electronic systems or transmissions, according to provisions on preparatory acts (e.g. preparation of data intrusion).

b. Act – public distribution/transfer to another person?

i. Swedish criminal law *does*, to some extent, penalize the unauthorized use of the hacker's tools listed above under a, likewise according to provisions on preparatory acts.

ii. Swedish criminal law *does* penalize the public distribution and transfer to other parties of hacked electronic information, if the act is considered as a preparatory act or as complicity in crime.

c. Possession?

Swedish law does *not* criminalize the mere possession of a hacker's "tool kit" or any part of it as such, but the Swedish provisions on preparatory acts cover a lot of different acts, such as the production, procurement and storing

of tools that specifically can be used to commit crimes with. Therefore possession has in most cases been preceded by a criminalized action or have the tools been possessed with the intent to commit a crime.

(b) Privacy

1-3

Processing personal or private data by use of ICT is regulated in Law on personal data (1998:204). The main rule is that processing is permitted only by regulations in law or with the consent of that person. There is a general prohibition against processing data concerning race, political views and religious belief. There are also restrictions as to other sensitive areas such as data on health or criminal records. Violation of the law 1998:204 – intentionally or by grave negligence – may result in penal sanctions (fine or prison up to six months).

4. Identity theft

a. Object

i. Swedish criminal law does *not* penalize identify theft as such, but such a conduct will probably, in most cases, form part of a crime such as fraud or forgery.

ii. Swedish criminal law does *not* proscribe specific forms of identity theft.

b. Subject

Swedish criminal law does not contain penal responsibility connected to a person's digital personality etc.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Swedish penal law *does* criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography. According to the article on child pornography offence in the SCC (16 chap. 10 a §) it is criminalized 1) to depict a child in a pornographic picture, 2) to disseminate, assign, make available, show or in any other way make such a picture of a child available for someone else, 3) to purchase or offer such a picture of a child, 4) to arrange contacts between a buyer and a seller of such pictures of children or in any other way promote trade of such pictures of children, or 5) to possess such a picture of a child or look at such a picture that the perpetrator has prepared himself access to. The article on child pornography offence is applicable no matter in what way the perpetrator disseminated, made available the child pornography etc., thus it is applicable if he used the internet to do so.

ii. It is an offense in Swedish law to make contact with a child with a sexual purpose (SCC 6 chap. 10 a §). It is likewise a crime to transmit, make available, export and intentionally access child pornography on the Internet – see the description of the article on child pornography offence under 1a *i* above. Child pornography posted on computer systems can be deleted and any materials or equipment used in the commission of a child pornography offense can likewise be forfeited. Swedish law criminalize knowingly accessing child pornography on the internet, transmitting child pornography on the internet, exporting child pornography on the internet and generally possessing child pornography, no matter in what purpose – see the description of the article on child pornography offence under 1a *i* above.

iii. The online solicitation of children for sexual purposes via social networking websites and chat rooms is criminalized in Swedish law – if not as an attempt to commit any form of sex crime against the child, according to the specific article on contact with children with a sexual purpose.

iv. There is no legal definition of child pornography in the SCC. Nevertheless, the meaning of child pornography in Swedish law is close to that contained in international instruments, such as the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

v. Prostitution and the appearance in pornography are *not* punishable under Swedish criminal law.

vi. Swedish criminal law *does* criminalize "virtual child" pornography. The article on child pornography offence even covers realistic drawings of children involved in sexual acts. The Swedish Supreme Court (*Högsta domstolen*) has however come to the conclusion that the possession of drawings of imaginary characters (in the specific case Japanese manga), when it is clear that the drawings do not depict real children, according to the principles on freedom of speech and freedom of information, is not criminal (decision on 15th of June 2012, case B 990-11).

vii. Under Swedish criminal law, to be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties are not to be applied to persons inadvertently accessing sites containing child pornography.

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

When it comes to conducts such as the creation and use of true anonymity sending and receiving material on the ICT, cyber-bullying, cyber-stalking and cyber-grooming there are no specific provisions in Swedish law concerning such *cyber*-conducts. If the act as such, i.e. the stalking, bullying etc., is punishable as for example defamation or molestation, it would be punishable committed with the use of ICT as well.

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use. **No such other regulation known.**

(d) ICT Related Violations of Property, Including Intellectual Property

Swedish law does *not specifically* proscribe and penalize fraud, infringement of Intellectual Property IP rights and industrial espionage perpetrated through the use of the ICT.

(e) Criminalization of Acts Committed in the Virtual World

As described above under 1 a *vi* Swedish criminal law penalize virtual child pornography. When it comes to other offences it might be considered as defamation or sexual harassment, under the regular provisions on defamation and sexual harassment, even though committed in the virtual world.

(f) Non-Compliance Offenses

Service providers are under a duty to retain and store various type of information and to give access to cyber systems to install devices needed for real-time collection of traffic data and interception of content data. The breach

of the duty to cooperate can result in an order to take corrective actions at the risk of liquidated damages and can, ultimately, have the effect that the service provider no longer is permitted to carry on his business.

(D) Complementary optional information concerning law and practice (including statistics)

- Cybercrimes are *not* included *as such* in the collection of data on crime in Sweden.
- There is *no* website in Sweden that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes.
- Victimization surveys in Sweden *do*, to some extent, include questions on cyber-crimes. For example questions about fraud on the Internet have been posed.
- Law enforcement and prosecution in Sweden *do* have a computer crimes unit.
- The subject of cybercrime *is* included in the continuing education of judges, prosecutors and police in Sweden.