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

Nils REKKE *

Questionnaire, Section 4, AIDP (Sweden) *

(B) Jurisdictional issues

(1)(a) To locate the place of the commission of a crime in cyberspace one has to apply the regular Swedish rules on jurisdiction, see the answer under 1b). There have been discussions in Sweden concerning the problems to determine where a cybercrime is supposed to be committed. In this context the opportunity to introduce specific rules concerning cybercrimes have been discussed. No such rules have, however, been worked out. The action is normally deemed to have been committed at the place where the computer that was used to bring to pass the relevant operation is located. The action is, at the same time, normally deemed to have been completed at all places where the internet-communication can be received and the information can be read or observed. As mentioned under 1b) a crime is considered to be committed where the criminal action took place as well as the place where the crime was completed.

(b) The questions under b) are relevant, hard to answer and interesting. Since Swedish jurisdiction rules are extensive and in many cases give Sweden the right to prosecute, though there are international aspects, it might be the case that these issues not always causes problems for Swedish law enforcement agencies . According to Swedish law, Sweden has, inter alia, jurisdiction over crimes committed in Sweden and over crimes that not for certain are committed in Sweden but where there are grounds to believe that the crime was committed in Sweden. A crime is considered to be committed where the criminal action took place but at the same time at the place where the crime was completed, or, when it comes to attempts, where the crime would have been completed. As soon as any part of the action took place in Sweden the action is as a whole considered being committed in Sweden. If a crime is committed outside Sweden, Sweden has jurisdiction, inter alia, when the perpetrator is a Swedish citizen or, somewhat simplified, if the perpetrator is a Swedish resident. To have jurisdiction in these cases the double criminality requirement has to be fulfilled. If the penalty for a specific crime under Swedish law can be no less than four years of imprisonment, the requirement of double criminality does not have to be observed.

(2) If one cannot determine the locus delicti for certain but there are grounds to believe that the cybercrime was committed in Sweden, Sweden has jurisdiction. If there are no such grounds, Sweden may have jurisdiction, inter alia if the perpetrator is a Swedish citizen or a resident in Sweden. However, in these cases the double criminality requirement must be fulfilled, and it is necessary to determine in what country or at least in which alternative countries the cybercrime was committed. If the specific crime, however, under Swedish law is considered to be so grave that the penalty can be no less than four years of imprisonment, Sweden has jurisdiction even if one cannot determine the locus delicti.

(3) No specific jurisdictional rules apply to cybercrimes like hate speech via internet, hacking, attacks on computer systems etc. One has to figure out where the crime was committed, or at least, have grounds to believe that part of it was committed in Sweden.

(4) Swedish national law does not provide rules on the prevention or settlement of conflicts of jurisdiction, apart from general regulations that judgements of other states must be respected and, as a main rule, may be an obstacle for proceedings in Sweden.

* Legislative counsellor, Ministry of Justice

Revue électronique de l'AIDP / Electronic Review of the IAPL / Revista electrónica de la AIDP
(ISSN - 1993-2995), 2014, RH-14:1

(5) For the moment it is hard to believe that cybercrime can do without jurisdictional principles in the Swedish criminal justice system. *If* national criminal law was applicable universally, the Swedish position would probably be that this has to be conditional on the basis of a treaty, in order to respect the territory of other countries.

(C) Substantive criminal law and sanctions

It is impossible to state what cybercrime offences that are to be considered to have a transnational dimension. A lot cybercrime offences do, maybe the majority.

To some extent definitions of cybercrime offences do contain jurisdictional elements. It is hard to say to what extent, though. No legal definition of cyber crime exists with respect to jurisdictional elements.

To some extent general part rules on commission, conspiracy or any other form of participation of course contain jurisdictional elements, but impossible to say to what extent.

Cybercrime offences can definitely not be regulated by a state on its own, since they, by nature, can be said to have a transnational dimension. Cooperation in this matter is therefore necessary.

Under Swedish law a corporation can be obliged to pay a corporate fine. In practice at least, the application of corporate fines requires that the company is active in Sweden (i.e. seat or branch)

(D) Cooperation in criminal matters

(2)(a) Sweden do provide for the interception of telecommunication, if:

- someone is reasonably suspected for a crime,
- the interception is of high importance for the investigation, and
- the investigation concerns a crime for which the penalty can be no less than two years of imprisonment (including an attempt or a preparatory act to commit such a crime) or if one can predict that the penalty will be more than two years of imprisonment.

(b) If a provider or a satellite is located outside the borders of Sweden, Sweden cannot wilfully go on with the interception, but has to ask for mutual legal assistance.

(c) Swedish national law provides for mutual legal assistance concerning interception of telecommunication and has concluded international conventions on it.

(3) General grounds for refusal do totally apply concerning internet searches and other means to look into computers and networks located elsewhere.

(4) In situations where the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised, the action would probably under Swedish law be considered as completed in the latter state (and committed there as well), and therefore the double criminality requirement would cause no problem.

(5) Investigative measures that do not require coercive measures may be performed without mutual legal assistance, i.e. by informal contacts (under the conditions that such contacts are allowed under the law of the other state). If coercive measures are needed, rules of mutual legal assistance must be observed.

(6) Self-service might be permitted, concerning public information. As to protected information, see under (4).

(7) There is no Swedish legislation that applies to searches to be performed on the publicly accessible web, or in computers located outside the country.

(8and 9) Sweden is a party to Passenger Name Record (PNR) according to Directive 2004/82/EG. The transmission of data (electronically) from the transport companies to the police is regulated in Law 2006:444. The register may be used only for the control of passengers over the Swedish border. The data should be deleted within 24 hours. Sweden does have an on call unit that is staffed on a 24/7 basis to exchange data.

(9) No regulations as to closing a website. The holder of an electronic board is obliged to delete illegal information such as child pornography and, if not doing so, may face criminal responsibility.

(10) In theory, such an international system would be appropriate. However, it is doubtful whether it would be possible or not; practical problems will arise – legal definitions, different views on the extent of criminalisation, geographical safe havens.

(11) Within the framework of the Prüm-decision, law enforcement agencies of other Member states may have direct access to the Swedish DNA database and the database containing finger prints.

(12) Sweden is a full member of Interpol, Europol and Eurojust.

(E) Human rights concerns

The right of everyone to hold opinions without interference, the right to freedom of expression, the freedom to seek, receive, and impart information and ideas of all kind and the rights concerning the respect for privacy are human rights and constitutional norms that are applicable in the context of criminal investigations using information technology. For the determination of the applicable human rights rules it might, to some extent, be relevant where the investigations are considered to have been conducted. When it comes to fundamental human rights, though, this issue is not relevant, since such human rights are considered inviolable.

If the information has been transmitted to the other state by a Swedish public authority, Sweden would probably, at least to some extent, be accountable for the misuse of the information. It is not known whether a similar case has occurred in practise.

(F) Future developments

If the legal systems and standard are at the same level and there is a common trust between the parties, such extended powers may be allowed. The classical mutual legal assistance might be cumbersome and slow. There have been discussions in that direction in the Nordic States.

There is no legal impediment under the law of Sweden to court hearings via the screen in transnational cases. The impediment concerns the other country involved, thus if the other country agrees to the procedure.