International Organisation of Penal Law

XIXth International Congress of Penal Law

"Information Society and Penal Law"

Rio de Janeiro, Brazil, 31st August to 6th September 2014

Preparatory Colloquium Section 4:

General Rapporteur: André Klip

Natonal rapporteurs – Denmark: *

Jørn Vestergaard[1] & Maria Raabye Füchsel[2]

(A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

(B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

a. By applying the traditional provision under the Penal Code (PC), cf. PC § 6 and § 9 (1) (territoriality principle) and § 9 (2) (ubiquity principle) supplemented by a new cyber-specific provision in § 9 a, see the following specifications.[3]

b. Under the territoriality principle stipulated in PC § 6 and § 9 (2), an offence committed on the internet will be subject to Danish jurisdiction if the perpetrator was located in Denmark when acting, e.g. if someone in Denmark transmits an email containing a virus to a specific recipient in another country and thereby infects the recipient's computer as an attachment is opened, or if a hacker accesses a closed informationsystem in another country. Likewise, if someone from a computer in Denmark sends an email with a defamatory content to a specific recipient in another country, or if someone dissemitates child pornography on the internet by giving others access to the materials whether free of charge or on a pay basis.

c. The ubiquity principle is laid down in PC § 9 (2). When the completion of a criminal act depends on a specific consequence to occur, the lotus delicti could also be regarded as the place where the consequence occurs or where the offender intended it to occur. Under the common ubiquity principle, an offence committed by someone in another country will be subject to Danisk jurisdiction, of the offence violates or is intended to violate an individual in Denmark, if the offender's act concurrently involves some kind of effect in Denmark. See below regarding the cyber-specific provision in § 9 a.[4]

d. When any part of a criminal act is conducted in Denmark, the offence, in full, will be regarded as committed in Denmark, cf. PC § 9 (4).

e. A cybercrime related to pictures, sound or text disseminated from another country but made commonly accessible for an indeterminate group of users by the internet, is regarded as also conducted in Denmark if the material has some kind of specific relation to Denmark, e.g. by being phrased in Danish or concerned with matters related to a specific group of individuals living in Danmark, cf PC § 9 a. This extension of the ubiquity principle covers not only the use of computers but also the use of mobile phones and other types of terminals that can be used to disseminate materials. Thus, the mentioned provision covers transmission of defamatory pictures, email containing virus, child pornography, hate speech, etc., if the materials have a specific relation to Denmark or to individuals living in Denmark, e.g. ethnic minority groups. In order to to

---

[1] Jørn Vestergaard is Professor of Criminal Law, Faculty of Law, University of Copenhagen, jv@jur.ku.dk and http://jura.ku.dk/jv.

[2] Maria Raabye Raabye Füchsel is Research Asststant, Center for International Law and Justice (CILJ), Faculty of Law, University of Copenhagen.

[3] The provisions on jurisdiction in the Penal Code were comprehensively revised and modernised in 2008. The amendments were based on recommendations by an expert committee, see the report: Betænkning 1488, 2007 om dansk straffemyndighed.

[4] This statue was inserted into the Penal Code in 2008 to accommodate the jurisdictional problems related to the ubiquitous nature of oline information.

avoid infinite jurisdiction for any country regarding dissemination of illegal materials on the internet, the ubiquity principle has not be subject to a limitless extension but to a more moderate widening as far as cyber crime is concerned. The argument has been made that if another country chose a model implying infinite jurisdiction for such offences, the consequence would be that upload of materials that are perfectly legal in Denmark could be prosecuted by the other state, even though said person did nothing illegal under Danish law.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

a. See answers above. Location of the exact "physical" place where information and evidence is held is not regarded as necessary under Danish law. Information and evidence are often located on servers by hosts and providers whose location can be rather random in relation to the criminal act.[5]

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

a. See answers above.

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

a. As already mentioned, a specific provision has been inserted into the Penal Code to accommodate for situations in which information (text, pictures, or sound) is legally made available from one country but illegally available in Denmark. PC § 9 a makes it a requirement for the establishment of criminal jurisdiction that the online criminal act has a relation to Denmark, e.g. hate speech has to be directed towards a specific group of persons in Denmark or be in Danish.

b. The traditional jurisdictional principles are also applicable to crimes committed in cyberspace. The general rules on jurisdiction competence are laid down in §§ 6-12 of the Penal Code. In the following, only provisions with a possible relevance in relation to cyber crime are mentioned.

- PC § 6: Danish criminal jurisdiction applies to acts carried out (1) within the Danish state (territoriality principle); (2) on a Danish vessel that is within foreign territory as recognized by public international law, by persons employed by the vessel or traveling as passengers on board; or (3) on board a Danish vessel (ship or aircraft) that is outside any state's territory as recognized by public international law.

- PC § 7 (1): Danish criminal jurisdiction applies to acts that a person with Danish citizenship or a person resident in Denmark has committed in another country, (1) if the act is also penalized by the other state (double criminality requirement, active personality principle); (2)(b) if the act is directed against a Danish national or a person resident in Denmark (combined active and passive personality principle).

- PC § 7 (2): Danish jurisdiction applies to acts carried out outside any state territory recognized by public international law by a Danish national or a person resident in Denmark, if the crime, pursuant to Danish law, is punishable by more than four months imprisonment (active personality principle).

- PC § 7 a: Danish jurisdiction applies to a number of serious offences committed from another country and directed against a Danish national or a person residing in Denmark (passive personality principle). The list of serious offences covers, among others, grave disturbance of railroad safety and other serious violations of physical infrastructures, see PC § 184.

- PC § 8, Danish criminal jurisdiction applies to acts perpetrated outside Danish territory, without considering to which state the perpetrator belongs to: (1) when the act violates the independence security, constitution, or public authorities of Denmark, or an official duty towards the Danish state; (2) when the act violates particular interests that require a specific relation to Denmark; (3) when the act violates a legal obligation that the perpetrator is obliged to observe abroad; (4) when the act violates an official duty towards a Danish vessel; (5) when the act is covered by an international obligation requiring Denmark to institute jurisdiction; or (6) when extradition to a foreign state is denied, and the act fulfills a double criminality requirement and the crime, pursuant to Danish law, is penalized by imprisonment for one year or more.

- PC § 9 (2): A criminal act involving some kind of result is considered to have been committed where the result is realised, or where the perpetrator intended it to become realised (ubiquity principle). Hacking, attacks on computer systems, etc., which target computers in Denmark are both subject to jurisdiction in the country where

[5] See the above mentioned committee report [Betænkning 1488, 2011] part 22.2 and 22.3.

the perpetrator was present at the time of the crime (principle of territoriality) and in Denmark if the offence has a relevant impact here.

- PC § 9 (3): Criminal attempt or participation is considered to have been committed within the Danish state if the perpetrator was present in Denmark when acting, independent of whether the offence is completed or intended to be completed outside the Danish state.

- PC § 9 (4): An offence in its entirety is considered to have been committed within the Danish state when part of the offence has been carried out in Denmark.

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

a. Danish law contains no settlement rules. The decision to either initiate or refrain from prosecuting will be taken by the discretion of the prosecutor. The decision depends on considerations regarding conditions with regard to investigation, adjudication, and execution.

b. When settling conflicts of jurisdiction between the member states of the European Union, member states shall consider the criterions laid down in Eurojust annual report 2003[6] and the obligations laid down in the 2007 Framework Decision on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.[7]

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

a. See the answers above. Under PC § 9 a, jurisdiction regarding cyber drime is based on a moderate ubiquity principle requiring some kind of specific relation to Denmark, e.g. by text being phrased in Danish or concerned with matters related to a specific group of individuals living in Danmark.

(C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

a. Probably all crimes conducted on a computer with connection to cyberspace could have a transnational dimension.

To what extent do definitions of cyber crime offences contain jurisdictional elements?

a. The substantive provisions hold no jurisdictional elements. The jurisdictional rules are stipulated in the above mentioned commin provisions (PC §§ 6-12).

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

a. As previously mentioned, criminal attempt or participation is considered to have been committed within the Danish state if the perpetrator was present in Denmark when acting, independent of whether the offence is completed or intended to be completed outside the Danish state, see PC § 9 (3). Other jurisdictional rules are stipulated in the above mentioned separate provisions (PC §§ 6-12). Elsewise, the general part rules on commission, attempt or participation hold no jurisdictional elements.

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

a. Cybercrime offences are transnational by nature. They might be regulated nationally by isolated domistic legislative initiatives but only with the risk of unnecessary duplicating legislative work, missing important international links and complicating mutual legal assistance procedures. ICT makes it particularly important to enhance international corporation in criminal matters. The nature of the internet makes it possible for perpetrators to find free havens under the jurisdiction of countries which do not penalize cybercrime offences systematically, do not maintain up to date jurisdiction rules, or does not have sufficient extradition agreements or traditions. Cybercrime and the volatility of electronic data create a need for swift and sometimes secret procedures. Enhanced mutual assistance rules which often depend on a double criminality requirement also cause a need for equivalent and harmonised substantive provisions.

---

[6] E.g. in which place the major part of the criminality occurred, the place where the majority of the loss was sustained, the location of the suspected or accused person and possibilities for securing its surrender or extradition to other jurisdiction, etc.

[7] E.g. the obligation to contact, to reply, to respond, the minimum of information to be provided in the request, etc. The 2009/948/JHA Framework Decision aims at achieving a consensus on any effective solution in order to avoid the adverse consequences arising from parallel proceedings and the waste of time and resources of the competent authorities concerned.

Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

a. Under Danish law, legal persons are subjects to criminal liability in all types of cases where acts by individuals are penalised under the Penal Code, see PC § 306. Common principles regarding criminal liability for corporations, public agencies, etc., are stipulated in PC §§ 25-27. Most other relevant legislation holds explicit provisions regarding corporate liability under the common principles laid down in the Penal Code.

b. When Denmark claims jurisdiction based on a personality principle, double criminality might typically be required. In order to avoid jurisdictional restrictions if the other state concerned does not recognize legal persons as subjects to criminal liability, a specific provision has been inserted into the Penal Code. With regard to legal persons, an offence is considered to have been committed where an act implying liability for the legal person was committed, see PC § 9 (1). In accordance with the territoriality principle and the ubiquity principle, this implies Danish jurisdiction when an act is committed in Denmark within a legal entity or when a relevant result of the act is covered by the above mentioned provisions in PC § 9 or § 9 a. Any act attributable to a certain individual as well as offences generated due to anonymous or accumulated errors or managerial errors or flaws is covered. If an act or its results can only be located outside Denmark, Danish jurisdiction might be established under the common provisions in PC §§ 7 ff. as mentioned above, e.g, under a personality principle. The issue regarding domicile is to be decided under corporation law.[8]

(D) Cooperation in criminal matters

To what extent do specificities of information technology change the nature of mutual assistance?

a. ICT enhances the need for international cooperation considerably. The transnational nature of cybercrime causes former relevant cooperation between counterparts with shared physical frontiers replaced by increased transnational collaboration.

(2)(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

a. Invations into the right to secrecy of communications by law enforcement authorities are dealt with under Chapter 71 of the Administration of Justice Act [Da.: Retsplejeloven], see § 780 ff.[9] The provisions here cover observation and data reading and allows the police, pursuant to a written court order and after appointing an attorney for the suspect, to infringe the secrecy of messages by: wiretapping; monitoring conversations or statements with the use of a device for that purpose; recovering information concerning phones and similar communication devises that have been connected to a certain phone or device ('teleinformation'); recovering information concerning phones and similar communication devices that are in a certain specific area and have been connected to other phones or devices ('extended teleinformation'); retaining, opening, and acquainting oneself with the content of letters, telegrams, and other mail; blocking the delivery of mail mentioned under the above.[10]

b. The Administration of Justice Act § 781 enables interception of telecommunication if (1) there is a specific reason to presume that the relevant means of telecommunication is a vehicle for information, transmission, etc., to or from a suspect; (2) the means sought are of vital importance to the investigation; (3) the investigation is related to an offence which holds a maximal penalty of 6 years imprisonment or more, or is related to terrorism or to other specificly mentioned offences,[11] e.g. hacking[12] and attacks like DoS (Denial-of-Service).[13]

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

a. Very relevant. Danish authorities would have to rely on mutual legal assistance, see answers above and the subsection below.

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication?

---

[8] Various issues regarding liability for criminal ommissions, etc., are treated extensively in the travaux préparatoires for the 2008 amendments.

[9] In 2004, an obligation for suppliers and providers of telenetworks to registrer and retain traffic data for one year was inserted into the Administration of Justice Act § 786 a. The provision corresponds with the Council of Europe Convention on Cybercrime 185, 2001 art. 16 and 17. The one year logging period was set up with view to the requirements in EU Directive 97/66/EC on concerning the processing of personal data and the protection of privacy in the telecommunications sector. Regarding Excecutive Orders further regulating the obligations of the providers regarding logging and assistance to the police, see bkg. 988, 2006 and bkg. 1145, 2006 respectively.

[10] Translation into English by Spang-Hanssen 2006 (167).

[11] Administration of Justice Act § 781 (2-4).

[12] Administration of Justice Act § 781 (2) with reference to PC § 263 (2)

[13] Administration of Justice Act § 781 (3) with reference to PC § 279 a (data fraud) and PC § 293 (1) (vandalism).

a. International legal assistance is practiced on the basis of the common provisions in the Administration of Justice act or by analogy of said provisions. The condition for executing a request for a certain measure is that a requirement regarding double criminality is met and that the requested measure would be authorised in a similar criminal case handled by the Danish police in Denmark.[14]

Did your country conclude international conventions on it?

a. Denmark has implemented all the relevant Framework Decisions based on the principle on mutual recognition in criminal matters.[15]

b. Denmark has ratified Convention on Mutual Assistance in Criminal Matters between Member States of the European Union and its provisions on interception of telecommunication (art. 17-22).[16] The provisions increase the effectiveness of mutual assistance between the member states by obligating them to make gateways in their territory directly accessible to other member states in order to enable lawful and more rapid interception (art. 19). The intercepting member states shall inform the notified member state of the interception prior or immediately after it becomes aware that the subject is in the territory of the notified state (art. 19 (4)).

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

a. If the situation is purely a national matter despite the fact that the information might be located on a server elsewhere, the national grounds for refusal would be applicable (e.g. the search has to be of significant importance to the investigation and proportional).

b. Recently, the Danish Supreme Court has stated that search of a Facebook and Messenger account is legal even though the information is stored on a server in a foreign country. The actual search was conducted on the basis of investigations by Danish authorities and legally obtained information (passwords obtained via interception of telecommunication) that was related to a crime subject to Danish jurisdiction, and the search was conducted without the involvement of foreign authorities.[17]

c. In situations involving another state, the competent authorities have to apply for mutual assistance, and the general grounds for refusal in relation to mutual assistance will be applicable.

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

a. Under Danish law, the common double criminality requirement has been modified by implementation of the relevant Framework Decisions, e.g. on the European Arrest Warrant and the European Evidence Warrant, allowing for execution of certain judicial decisions without verification of double criminality. It is well known that cyber crime is on the positive list established by such instruments.

b. When assisting countries outside the EU, Denmark applies the provisions in the Administration of Justice Act by analogy which makes dual criminality a requirement.

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

a. Denmark allows for extraterritorial investigations pursuant to art. 40 (cross boarder observation) and 41(hot pursuit) of the Schengen Convention.

b. Denmark has entered bilateral agreements with Germany and Sweden regarding police cooperation in the border regions.

(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in

---

[14] See Vestergaard 2007 (422 f.) and Gade et al. 2005 Chapt. 22.5.1.

[15] See Vestergaard & Adamo 2009.

[16] Council Act of 29 May 2000 on Mutual assistance in Criminal Matters between the Member States of the European Union. The treaty was implemented in 2002 [lov 258, 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet og lov om international fuldbyrdelse af straf m.v.]. The provisions related to interception of telecommunication is found in the Administration of Justice Act chapter 71 as mentioned above. The provisions related to gateway access were inserted into the Act on Competition and Consumer Conditions on the Telecommunication Market [lov om konkurrence og forbrugerforhold på telemarkedet § 8 a and § 15]. Today the provisions are found in the Act on Electronic Telecommunication Nets [lov 169, 2001 om elektroniske kommunikationsnet og -tjenester § 2 (17) and § 10 (3-4).

[17] See UfR 2011.129 H.

order to allow self service? Please differentiate for public and protected information.

a. ICT has made it possible for law enforcement authorities to collect data and obtain evidence without being physically present in another state. If the information is publicly accessible and can legally be accessed from another state, e.g. information available online, it may be obtained without the involvement of Danish authorities.

b. Denmark has ratified the Cybercrime Convention,[18] which in art. 32 deals with the regulation of transborder access to data where mutual assistance is not required. The article addresses two situations: first, where the data being accessed is publicly available, and the second, where the party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has legal authority to disclose the data to the Party through that system.[19]

c. Protected information contained in another member state is normally accessible by applying mutual assistance procedures. In the context of general criminal cooperation some protected information are made available to authorities in other EU countries, e.g. the DNA, fingerprint, the motor vehicle register,[20] and other information contained in the Schengen information system, SIS. The DNA register enables the discovery of a matching profile. Elaborating information has to be applied for. As a general condition the access of foreign authorities have to have explicit statutory authority, sufficient safeguards, safety provisions, and respect the general data protection principles.

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

a. Yes, see subsection above.

(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law.

a. Denmark does not take part in the adoption by the Council of proposed measures pursuant to TEUF Chapter IV of Title III of Part III, cf. Protocol on the Position of Denmark.[21] This leaves Denmark outside the PNR[22] and SWIFT[23] agreements between the European Union and The United States of America. Denmark has not concluded parallel agreements.

b. A provision relating to passenger data is found in the Air Navigation Act [Da.: Luftfartsloven] § 148 a,[24] which imposes on airline companies a duty to register and retain for one year passenger data and allow the police intelligence service to collect information that could be related to crimes against the state or to terrorism.

c. The intelligence service can exchange data with foreign services in order to prevent and investigate serious international crime. The exchange has no statutary basis but has to be in accordance with the guidelines and have the approval of the Director of the Legal Department of the Danish Security and Intelligence Service or his or her deputy.[25]

d. Denmark is not a party to the SWIFT agreement. Danish financial transactions involving other parties to the SWIFT agreement could probably legally be transferred to the U.S.[26]

e. Pursuant to the Act on Financial Corporation [Da.: lov om finansiel virksomhed] § 354 (6)(2), financial corporations may

---

[18] With reservations regarding art. 9, 14 and 38 of the Convention. The text of the reservations is available through http://conventions.coe.int/treaty/Commun/ListeDeclarations.asp?NT=185&CV=1&NA=&PO=999&CN=2&VL=1&CM=9&CL=ENG

[19] See the Explanatory Report to the Cybercrime Convention sec. 294.

[20] The transposition of the Prüm agreement into EU Law made national registers accessible in other EU countries. The agreement was implemented in 2008 [lov 479, 2008 om ændring af lov om Det Centrale Dna-profil-register, retsplejeloven, lov om registrering af køretøjer og lov om konkurrence- og forbrugerforhold på telemarkedet]. Exchange of relevant information is also allowed in relation to states outside the EU if the exchange has authority in an agreement and is authorized by the Minister of justice [lov 715, 2010 om ændring af lov om Det Centrale Dna-profil-register, retsplejeloven og lov om registrering af køretøjer].

[21] Since 1993, Denmark has had four opt-outs covering defence policy, the Economic and Monetary Union (EMU), Union citizenship, and Justice and Home Affairs (JHA).

[22] Agreement of 26 April 2012 between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, L 215/5/2012.

[23] Agreement of 27 July 2010 between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, L 8/11/2010.

[24] Inserted in 2006 as a consequence of the implementation of Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences. See text here: http://www.slv.dk/Dokumenter/dsweb/Get/Document-8762/Air_Navigation_Act_Order_no._731_of_21_June_2007.pdf.

[25] See further: https://www.pet.dk/English/International%20cooperation/Exchange%20of%20information.aspx.

[26] See art. 16 in the SWIFT Agreement.

transmit confidential information to police or the prosecutor in the course of criminal investigation.

f. Regarding the DNA-register, see subsection above.

Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

a. Denmark is a party to Eurojust, Europol and Interpol. Se further the subsection below.

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence?

a. See answers above.

Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

b. The Administration of Justice Act authorizes seizure and the PC § 75 allows for confiscation of a domain if it contains illegal materials.

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

a. Hopefully! At least on a European Union basis.

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

a. Within the European Union, Denmark allows for the direct consultation of the DNA, fingerprint and motor vehicle register,[27] see subsection above. Moreover, the Denmark allows for direct access to information via the Schengen Information System, SIS.

(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

a. Denmark participates in Europol and Eurojust so far as supranational amendments have yet not been enacted under the Lisbon Treaty. Denmark is also a full member of Interpol.[28]

(E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted?

a. ECHR has been incorporated into Danish law, naturally including art. 8.

How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

a. According to a set of strict liability provisions under the Administration of Justice Act, the Danish state is accountable and obliged to pay compensation if somebody has been arrested or subject to pretrial custody, if prosecution is waived or the defendant is acquitted. Compensation may also be awarded in case of other investigative measures having been implemented. Se § 1018 a and § 1018 b. These rules only apply to measures enacted by Danish law enforcement or judicial authorities.

(F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

---

[27] See footnote above regarding the implementation of the Prüm agreement. The provisions are to be found here: lov om Det Centrale Dna-profil-register § 5 (2), retsplejeloven § 116 a, lov om registrering af køretøjer § 17 a.

[28] Denmark has been a member of Interpol since 1926.

a. The sovereignty of states, due process principles, and fundamental procedural rules (e.g. translation into ones native language, self-incrimination, and the rules related to a non-compellable witness and oath) should be respected. Direct contact between the accused and a foreign state would make this a difficult task. A solution could be to apply existing mutual assistance procedures with the possibility of applying an investigating order with a view to ensure swift assistance. The European Union's Framework Decisions based on a principle of mutual recognition is an example to follow.

Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

a. The Administration of Justice Act § 190[29] enables court hearings via telecommunication in transnational cases unless it is incompatible with the general legal order. Denmark has declared a reservation to the EU Convention on Mutual Assistance in Criminal Matters[30] art. 3 (2): A request for evidence to be taken on oath from a witness or expert may be refused if the competent Danish court does not consider the oath to be necessary.[31]

[29] Implemented in 2002 [lov 258, 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet og lov om international fuldbyrdelse af straf m.v.] § 2.

[30] Council Act of 29 May 2000 on Mutual assistance in Criminal Matters between the Member States of the European Union.

[31] http://www.official-documents.gov.uk/document/cm19/1928/1928.pdf p. 15

Literature

Betænkning 1417/2002 om IT-kriminalitet.

Betænkning 1488, 2007 om dansk straffemyndighed.

Blume, Peter: *Databeskyttelsesret*, Jurist- og Økonomforbundets Forlag 2008.

Frese Jensen, Malene et al: *The Principal Danish Criminal Acts*, 3rd Edition, DJØF Publishing, Copenhagen 2006.

Gade, Ingeborg et al: *Det politimæssige og strafferetlige samarbejde i Den Europæiske Union.* Jurist- og Økonomforbundets Forlag 2005, Chapter 22.5.1.

Greve, Vagn et al.: *Kommenteret straffelov. Almindelig del.* 9. udgave, Jurist - og Økonomforbundets Forlag 2009.

Greve, Vagn et al.: *Kommenteret straffelov. Speciel del.* 10. udgave, Jurist - og Økonomforbundets Forlag 2012.

Karnovs lovsamling.

Langsted, Lars Bo & Charlotte Bagger Tranberg: "Internet-kriminalitet", i Jan Trzaskowski (red.): *Internetretten*, Ex Tuto, 2012 (675-722).

Langsted, Lars Bo, Peter Garde & Vagn Greve: *Criminal Law in Denmark*, Third Revised Edition, DJØF-Publishing & Wolters Kluver 2011.

Smith, Eva et al.: *Straffeprocessen*, 2. udgave, Forlaget Thomson 2008.

Spang-Hanssen, Henrik: Chapter Eight in *Cybercrime and Jurisdiction – a global survey*, T.M.C Asser Press 2006.

UfR: *Ugeskrift for Retsvæsen*.

Vestergaard, Jørn (red.): *Forbrydelser og andre strafbare forhold*, Gjellerup 2009.

Vestergaard, Jørn: *Straffeloven & straffuldbyrdelsesloven – med henvisninger og sagregister*, 17. udgave, Karnov Group 2012.

Vestergaard, Jørn: "Dansk lovgivning om bekæmpelse af terrorisme." In *Enhver stats pligt… International strafferet og dansk strafferet.* Eds.: Lars Plum & Andreas Laursen, Jurist- og Økonomforbundets Forlag 2007, Kapitel 13.

Vestergaard, Jørn & Silvia Adamo (2009): "Mutual Recognition in Criminal Matters: The Danish Experience." In the series: *Scandinavian Studies in Law*, Volume 54: *Criminal Law*. Ed.: Peter Wahlgren. Stockholm 2009 (431-462). Also published in the book: *The Future of mutual recognition in criminal matters in the European Union/ L'avenir de la Reconnaissance Mutuelle en Matière Pénale dans L'union Européenne.* Eds.: Gisèle Vernimmen-Van Tiggelen, Laura Surano and Anne Weyembergh, Institut d'Etudes Europeennes, Editions de l'Université de Bruxelles, Brussels 2009.

Waaben, Knud: *Strafferettens specielle del*, 5. udgave, Thomson Gad Jura 1999.

Waaben, Knud: *Strafferettens specielle del*, 5. udgave v. Lars Bo Langsted, Karnov Group 2011.