Prof. Arkadiusz Lach

Head of Department of Criminal Procedure

Nicolaus Copernicus University in Torun

National report Poland *

(B) Jurisdictional issues

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

According to the Polish Criminal Code (CC), a crime is committed in a place where the perpetrator acted or failed to act he was obliged to, or where the effect of the crime described in the definition of the crime took place or was intended to take place (article 6 § 2 CC). Therefore it is possible that there is more than one place of commission of crime. In each such place a jurisdiction to adjudicate may be exercised. The above mentioned rules apply to crimes committed in cyberspace as well. Of course, in case of cyberspace the criteria are not clear because the perpetrator may be regarded as acting in the place where he is physically present or acting remotely in other place (ex. where the attacked computer is situated). It is important to make a distinction between so called formal crimes (without an effect) and material crimes (with an effect). In case of formal crimes committed in cyberspace, a jurisdiction can be exercised only in a place where the perpetrator acted or failed to act. In case of material internet crimes some authors argue, that the crime is committed in every place where the effect took or was intended to take place. The others are of opinion that the mere possibility that the content is accessible in every place does not mean that in all the places jurisdiction could be exercised.

Because usually from a legal point of view the crime was committed in more than one place, it is necessary to determine which authority is territorially competent for conducting of the proceedings. Under the Code of practice for public prosecutors 2010, in cases committed through teleinformatic or telecommunication network, preparatory proceedings are to be conducted or supervised by the entity, in which circuit the perpetrator acted (§ 124 (2) of the Code of practice). As one may see, the regulation points on the place of activity of the perpetrator, not the place of the effect in case of material crimes, but it still lefts unresolved

* 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.

the question, in which place the perpetrator shall be assumed to act. It must be observed that in case of material crimes normally it is easier to indicate the place of the effect. Determination of the place where the perpetrator acted is often done at later stage of preparatory proceedings and may be connected with presentation of the charges to the suspect. Therefore requiring that the authority in which circuit the perpetrator acted shall be competent would put task impossible to fulfill by the police and the public prosecution service.

(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.

As it was described above, the place of commission of a crime is defined in Polish law broadly. Therefore if the effect took place in a certain place in Poland, localization of the place where the information is held is not necessary for prosecution of the perpetrator. Of course it may be important for evidential purposes to know where to send a request or order. In such situation the request will be sent (also by a rogatory letter) to the seat of the entity or to the person authorized to produce the data sought.

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

A crime could be investigated in Poland and the alleged perpetrator prosecuted without a precise determination of the locus delicti. In this case auxiliary rules of jurisdiction apply: territorially competent is the court in which circuit the crime was discovered, the accused arrested, the accused has a permanent or temporary residence and if it is not possible to indicate the court on the base of the above mentioned rules, competent is the county court for the center of capital city Warsaw (art. 32 CCP).

(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?

In case of cyber crime general jurisdictional rules apply. If the crime was perpetrated outside the Polish territory (by a Polish citizen or against the Polish state, Polish citizen, Polish legal person or other entity, was a terrorist crime or any other crime in CC punished by deprivation of liberty of more than 2 years, when the perpetrator is present at the Polish territory and he is not to be extradited) the double criminality principle must be normally observed with few exceptions (art. 110 – 111 CC). First, the principle shall not be applied to the Polish public official who, while performing his duties abroad, has committed an offence there in connection with performing his functions, nor to a person who committed an offence in a place not under the jurisdiction of any state authority (art. 111 § 3 CC). Besides, notwithstanding the provisions in force in the place of the commission of the offence, the Polish penal law shall be applied to a Polish citizen or an alien in case of the commission of:

1) an offence against the internal or external security of the Republic of Poland;
2) an offence against Polish offices or public officials;
3) an offence against essential economic interests of Poland
4) an offence of false deposition made before a Polish office

5) an offence from which financial gained was obtained, at least indirectly, on the territory of Poland.

If the state does not have jurisdiction over the above mentioned offences, the proceedings cannot be initiated.

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

In the CCP the procedure of transfer of the proceedings is regulated. If Poland and other country both have jurisdiction under certain crime, they may decide to stop the proceedings in one country because of proceedings in the other. The procedure may be initiated by the Minister of Justice ex officio or on a request of public prosecutor or a court (art. 590 – 592 CCP). It is not used frequently but the possibility is seen as a way of avoiding problems with gathering of evidence by Polish authorities in cases where the evidence is located mainly abroad. Where the conflict of jurisdiction is between the MS of the EU, special regulations apply which provide for direct consultations between courts or public prosecutors (articles 592a – 592f CCP).

(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?

The CC provides one situation of universal application of Polish criminal law: when the offender is a Polish citizen or foreigner in relation to whom the decision of extradition was not taken and Poland is obliged to prosecute the offender on the base of an international treaty (article 113 CC).

(C) Substantive criminal law and sanctions

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

Our legal system does not distinguish crimes with international dimension as a specific group of crimes. One may consider that the following crimes have such character most frequently: hacking, credit card fraud,

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

They do not contain jurisdictional elements in Poland.

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

They do not contain 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.

As criminal law is a matter of national competence and interest, it is primarily the state who can and should regulate cyber crime offences. This is a very sensible question of sovereignty. It is hard to imagine that agreement on transfer of sovereignty concerning cyber crime could be concluded and any organization would be authorized to create transnational legislation defining elements of crime and indicating penalties for the criminal acts. The problem of enforcement would arise as well.

On the other hand, certain state may be not interested in prosecuting acts which are not regarded as harmful significantly for the state, but they are harmful to other states. In this case

common interest and security may require taking a regional or global initiative to limit the number of safe heavens. Besides, smooth cooperation in criminal matters may require certain level of harmonization, especially having in mind the double criminality principle.

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

In Poland responsibility of corporations was introduced in 2002 but it is rather not regarded as a criminal responsibility. It is sometimes called as quasi – criminal or repressive. The attribution of responsibility does not have any special jurisdictional implications.

(D) Cooperation in criminal matters

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

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

Interception of communication may take place in the course of criminal proceedings on the base of CCP or as an operational measure on the base of Police Act 1990 and several other similar acts regulating powers of specific forces.

Once the formal proceedings have begun, the court may order interception on the base of chapter 26 of the CPP, and in relation to certain categories of crimes listed in article 237 of the CPP. In urgent situations, a public prosecutor may order interception by himself, but he is required to apply to a court within three days for a confirmation of the order.

Interception may also be ordered by a court in the course of police operations when it is suspected that one of the crimes listed in Police Act might be committed. Where information gathered is likely to be useful in criminal proceedings, the materials may be transferred to a public prosecutor and used as evidence. Besides the police, similar powers have been granted to other bodies, such as the Agency of Internal Security, Border Guard, Central Anticorruption Bureau and fiscal inspection. In exigent circumstances the decision on interception may be taken by the head of the force but then it requires confirmation by a court.

Both procedures of interception allow direct and indirect surveillance (including wireless communication).

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

Interception orders may be issued only for entities within the Polish borders. Outside the borders the instruments of mutual assistance apply.

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

The national law in Poland does not provide expressis verbis for mutual legal assistance concerning interception of communications (although general rules on mutual assistance apply to interception). It must be mentioned that Poland signed two important international conventions: the EU convention on mutual assistance 2000 and the additional protocol 2001 to the CoE convention on mutual assistance 1959. In the Polish law transposition of international treaty to domestic law is not necessary and in case of conflict between an act of Parliament and ratified treaty, the latter prevails.

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

The most relevant ground for refusal of mutual assistance is listed in the article 588 § 2 CCC according to which public prosecutor or court refuse to give mutual assistance if the act requested would be against the principles of legal order or would breach the sovereignty of Poland. The non - mandatory grounds for refusal are: lack of competence of public prosecutor or court to execute the request under the Polish law, lack of reciprocity and lack of double criminality (art. 588 § 3 CCP).

(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?

First of all, lack of double criminality is only non-mandatory ground for refusal of cooperation. The principle is observed if the act is a crime under the Polish law.

(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.

The only known way of carrying out investigation outside the borders is by taking part in a Joint Investigation Team (JIT). Creation of JIT is possible under the Polish law with the other MS of the EU or on the base of binding international treaty. An example of such a treaty is the second additional protocol 2001 to the European convention on assistance in criminal matters 1959 adopted by the CoE.

Besides, that the law does not allow for both kinds of extraterritorial investigation. Moreover, pretending to be an official and carrying out his tasks is penalized by the article 227 of CC.

(6) Is self service (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?

The law does not regulate self service. In practice obtaining publicly available information is done or one of the parties could be asked or order to provide information available to the party. The same may be said concerning the passive practice but the subject within the Polish borders may be bound by national regulations concerning protected information.

(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?

The legislation is written rather in general terms and does not distinguish between search performed in the country and outside. As the authorities do not have powers to act outside in their capacity (with the exception of the above mentioned JIT), search outside the Polish territory is not possible. Analysis of the content of publicly available webpage located in foreign country would be done rather as inspection.

(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. 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.

As a MS of the EU Poland is bound by the agreements concerning PNR exchange concluded by the EU, especially with the US. Besides the EU adopted legislation implementing so called Prum treaty. It was done by the Council decisions 2008/615/JHA and 2008/616/JHA. The decisions create a framework of exchange of such information as DNA, fingerprints, etc.

The above mentioned directives were implemented into the Polish law by the act of Parliament on exchange of information with the investigative authorities of the MS of the EU, adopted on 16 September 2011. Under the regulation contact point was created operating on 24/7 basis to exchange data.

(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? 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?

The data mentioned in the decisions 2008/615/JHA and 2008/616/JHA may be exchanged for purposes of criminal investigation. The legal basis for that are the decisions and the domestic regulations implementing the decisions. The information could be used in evidence unless there is a limitation from the authority exchanging the information. The data subjects have several rights concerning their personal data such as right to information if the data is processed, right to request correction, deletion or discontinuation of processing the data.

Polish law provides the Notice and Take Down procedure. It is regulated mainly by the article 14 of the Electronic Services Act 2002. The procedure is used in practice.

(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)?

I do not think that such a system would be possible or effective. A regional enforcement system is hard to introduce. The differences between the world legal systems and sovereignty issues are so visible, that one should be skeptic if international system could be introduced.

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

It is not expressis verbis allowed or forbidden. In practice, the authority may consult open databases. In case doubts are raised as to reliability of such evidence, a formal request could be necessary.

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

Poland is a party to Interpol treaty and as a MS of the EU participate in the activities of Eurojust and Europol as well.

(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?

The most important constitutional and human rights norms applicable in the context of criminal investigation using IT tools are: right to privacy, inviolability of home, personal data protection. The general concept of fair trial is also applicable.

If the investigation is conducted in Poland, the procedural guarantees apply. Protection of such rights as rights to privacy or inviolability of home in relation to subjects outside Poland may be based on relevant regulations in the country where the activity took place.

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?

Civil responsibility for cooperation between the MS of the EU is regulated in framework decisions and directives. The issues of responsibility of requesting state was discussed in few cases by the European Court of Human Rights. Certainly a state may be responsible for using evidence obtained by another state by torture.

(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?

In my opinion hearing by videoconference shall be widely used in relation to accused, witnesses, victims and experts. The key problems are protection of the rights of the participants of criminal proceedings (for example right to information, right not to testify) and ensuring reliability of evidence (for example by verification of identities of persons heard).

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?

The possibility of hearing by videoconference or teleconference exists under the EU convention on mutual assistance 2000 and the second additional protocol 2001 to the CoE convention on mutual assistance 1959. Unfortunately, Poland made a reservation to the instruments that it will not ask or allow for remote hearing of accused (suspect). The reasons for such reservation were not given and are rather unclear. Probably the government was of the view that remote hearing could have negative impact on the right of the accused (suspect).

Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

No