INTERNATIONAL ASSOCIATION OF PENAL LAW

19th International Congress 'Information Society and Criminal Justice'

Preparatory Colloquium Section 4
International Criminal Law | Helsinki, 10-12 June 2013

REPORT FOR BELGIUM

National Rapporteur: Gert Vermeulen[1]
Co-author : Lynn Verrydt[2]

1. Jurisdictional issues

1.1. General jurisdiction rules

The concept of cybercrime tends to provoke lively discussions with regard to jurisdiction. Nevertheless, Belgian criminal law does not include jurisdictional provisions which are specifically aimed at cybercrime. General provisions regarding jurisdiction can be found in articles 3 and 4 of the Belgian Criminal Code, hereinafter referred to as CC, the former introducing the general territoriality principle which implies the applicability of Belgian criminal law to offences committed on Belgian territory, whilst the latter entails the possibility of its extraterritorial application, be it limited to those instances when such is explicitly provided for by law. These extraterritorial provisions (at least the general principles thereof) can be found in the second chapter of the Preliminary Title to the Belgian Code of Criminal Procedure, hereinafter referred to as PT CCP. However, it must be stressed that the possibility of extraterritorial jurisdiction for these specific crimes is only linked to cybercrime with regard to child pornography as provided by article 10ter PT CCP jo. 383 bis §§1 and 3 CC.

1.2. General localization theory

In light of the application of the territoriality principle enshrined in article 3 CC to cybercrime, it is of the utmost importance to determine when a cybercrime can be considered to have taken place on Belgian territory. Here, rather than introduce a specific theory of localization targeting crimes committed in cyberspace, the generally applicable theory of localiza-

[1] Professor of Criminal Law, Head of Department Criminal Law and Criminology, Ghent University. Director Institute for International Research on Criminal Policy (IRCP) (www.ircp.org). Extraordinary Professor of Evidence, Maastricht University.
[2] Academic Assistant Criminal Law & PhD Candidate at the Institute for International Research on Criminal Policy (IRCP) (www.ircp.org), Ghent University.

tion is wielded. This general theory, known as the ubiquity doctrine, determines that an offence is committed on Belgian territory - thus falling under the scope of Belgian criminal law - as soon as a physical act which makes up a constitutive element of the offence, takes place on Belgian territory. The broad nature of this theory provides the possibility of establishing jurisdiction over a cybercrime without necessarily determining the location of the user, the provider of the location where the information or evidence is held.

In other words, no specific theory for determining the *locus delicti* of offences committed in cyberspace exists. In order to determine whether or not a cybercrime can be said to have taken place on Belgian territory, it must be established whether a constitutive element of the said offence took place on Belgian territory.

Nevertheless, examples of cases where the application of the ubiquity doctrine does not provide sufficient (legal) clarity are easy to come by. Consider, for example, the crime of hate speech. The question arises whether hate speech can be considered to be an offence committed on Belgian territory any time a computer screen, located on Belgian soil, showcases the messages of an instigator/perpetrator, located abroad, perhaps even at the other side of the world. Similarly, the question arises whether the offence would be located in Belgium when those called upon by the instigator choose to follow command and cause damage. Finally, the question arises to what extent specific targeting is required, e.g. because the hate speech calls specifically for riots in a Belgian city or because it is formulated in a Belgian national language. The legal uncertainty resulting from the lack of a specific localization theory and of specific jurisdictional rules in relation to cybercrime, are to be considered problematic, as the above examples illustrate.

1.3. Conflicts of jurisdiction

The possibility of a broad territorial jurisdiction claim, implied by the ubiquity doctrine, can give way to positive conflicts of jurisdiction. This statement is particularly true since Belgian law, for certain offences, considers the public nature of certain material elements of the offence (or the fact that publicity has been given to certain words, images etc or that there has been a certain spread thereof) as a constitutive element in itself. This is e.g. the case in the context of violations of sexual morals, or in the case of certain forms of incitement to violence or hatred (e.g. racial or ethnic) or condoning, denying or grossly trivializing (WWII) genocide. Consequently – applied to the reality of the information society – the public nature or character for such offences (through cyber or ICT media) may well prompt Belgian territorial jurisdiction over them, even if it would seem reasonable in exercising jurisdiction to take account of whether the perpetrator effectively intended or targeted publicity on Belgian soil. To the extent that (many) other states have comparable legislation, major positive jurisdiction conflicts are theoretically likely to arise.

Regardless of this substantial possibility for jurisdictional conflicts, Belgian criminal law does not provide specific rules with regard to their prevention or settlement, other than through the so called denunciation on the basis of mutual legal assistance treaties in place.[3] Belgium is not a party to the Council of Europe European Convention on the Transfer of Proceedings in Criminal Matters.

1.4. Universal jurisdiction?

The absence of cybercrime-specific jurisdictional principles does not necessarily imply universal jurisdiction. The enforcement of universal jurisdiction to cybercrime in general is to be avoided, for it not only gives way to serious conflicts of jurisdiction but will additionally cause significant problems regarding mutual legal assistance, particularly when there is an asymmetry in the criminal nature of the offence between the requesting and the requested state.

2. Substantive criminal law

2.1. Offence definitions

Jurisdictional provisions (which in general can be found in the second part of the PT CCP) are separate from provisions containing offence definitions as well as from provisions relation to participation, which can be found in the CC or special laws. In other words, definitions of (cybercrime) offences and provisions concerning participation[4] in these offences do not contain jurisdictional elements. When regarding the matter from a substantive rather than a procedural viewpoint, it can be noted that the offence definitions are not endowed with a transnational dimension either. The provisions included in the Belgian CC do not differentiate between national and transnational offences. They provide an open formulation of the offence definition, which can thus be applied to national and transnational offences alike.

2.2. Criminalizing cybercrime

Cybercrime offences often include a foreign element. This must be taken into account when considering whether or not it is preferable for states to criminalize cybercrime offences. A number of difficulties are likely to arise. Reference can be made to the difference between criminalizing the consumer and the provider. For a state to regulate the acts of e.g. a person, located on its territory, who consciously and deliberately engages in an act which is illegal in that country by means of a personal computer, e.g. watching child pornography or online purchasing of pepper spray, seems perfectly reasonable. For a state to equally criminalize

[3] E.g. article 21 of the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters (ECMA).
and article 42 of the 1965 Benelux Treaty on Extradition and Mutual Legal Assistance. Neither relates specifically to cybercrime.
[4] Article 67 CC.

the provider of this content, residing outside its territory and having no link with the state other than providing content to a computer screen which is physically located in its territory, is likely to be problematic, however. In such cases, the question arises whether the state in which the provider acts, considers these actions criminal. If the answer is positive and both states consider the actions of the provider illegal, minimal problems occur, likely to be limited to a positive conflict of jurisdiction. However, when the answer to the forgoing question is negative and consequently the double criminality test fails, difficulties in having mutual legal assistance requests executed are likely, at least when the measures requested are coercive in nature, or intrusive, or potentially impact on the privacy of the person concerned. Given the universality-like nature of the criminalization of acts posed on the territory of another state, it seems preferable for an international or at least regional (e.g. EU) framework to guide states' national legislation in this matter. Problems would at least be diminished if e.g. EU member states were to agree for certain offences to criminalize the actions of the provider throughout the EU. If EU member states would individually criminalize provider actions in or onto other member states' territory, the question e.g. arises whether this would not contradict with the right of free movement (of services), a principle that is fundamental to the functioning of the internal market.

2.3. Internet providers as criminally liable legal persons

The Belgian CC provides a legal basis for criminal responsibility of legal persons. Article 5 CC introduces a general principle of criminal liability for legal persons, which can be applied to cybercrime offences. The open formulation of the said article does not differentiate between a national and an international legal person.

However, concerning jurisdictional issues regarding legal persons, reference must be made to article 12bis PT CCP. This provision provides automatic implementation of mandatory jurisdictional rules embedded in secondary EU legislation, meaning that no additional Belgian implementation legislation is required in such cases. In other words, provisions concerning mandatory jurisdiction to prescribe included in (amongst others) EU Framework Decisions and Directives are automatically applicable. As a result, Belgian authorities are competent to prosecute and convict legal persons whose headquarters are located on Belgian territory for various EU core crimes, including racism,[5] attacks on information systems,[6] corruption[7] and

[5] Article 9 § 1 (c) Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, European Union: Council of the European Union 28 November 2008.

[6] Article 10 § 1 (c) Council Framework Decision 2005/222/JHA of 21 February 2005 on attacks against information systems, European Union: Council of the European Union 21 February 2005.

[7] Article 7 § 1 (c) Council Framework Decision 2003/568/JHA of 22 July 2003 on combating corruption in the private sector, European Union: Council of the European Union 22 July 2003.

counterfeiting.[8] The jurisdictional competence remains intact, even when the offence is committed by a daughter corporation outside the Belgian territory.[9]

3. Cooperation in criminal matters

The rise of information technology, such as e.g. low and medium earth orbiting satellites and foreign servers, has profoundly impacted upon the nature of mutual legal assistance. It has created a need for cooperation and mutual legal assistance where no such need existed before by adding an international dimension to situations which formerly were purely national.

For instance, mutual legal assistance may even be required when a Belgian authority wishes to perform a telephone tap on a conversation between two Belgian nationals both located on Belgian territory, if routed through a satellite-based personal communication system. This because the technical point for interception may now be located outside of the Belgian borders, i.e. in a ground station of a low or medium earth orbit satellite constellation, located abroad. Another example concerns criminals or criminal organizations setting up constructions and hosting illegal websites through (multiple) foreign servers to avoid detection. This represents another example of a case where a criminal investigation will require mutual legal assistance. These simple examples clarify the effect of increasingly complex technological advancements on the nature and scope of mutual legal assistance.

3.1. Interception of telecommunication

Within the national framework, article 90ter CCP provides a competence for the Belgian investigative judge to intercept (wireless) telecommunication. The concept of "telecommunication" is described as 'private and telecommunication'.[10] This is a broad concept, including amongst others telephone conversations, email and voicemail.

The possibility of exercising this competence is subjected to the fulfillment of three strict conditions. First and foremost, interception can only take place when there are serious rea-

[8] Article 9 §1 (c) Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of noncash means of payment, European Union: Council of the European Union 28 May 2001.

[9] Other framework decisions refer to Member States establishing jurisdiction when a legal person is "established in the territory of that Member State." See e.g. article 8 § 1 (c) Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking, article 7 § 1 (c) Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, article 4 § 1 (c) Council Framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence, Article 17 § 2 (b) Directive 2011/92/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.

[10] Article 90ter §1 CCP.

sons to believe that the suspect committed one of the crimes included in a limitative list.[11] The offences included in the said list are of a grave and serious nature and include, amongst others, murder, trafficking in human beings, taking of hostages and kidnapping. Second, this must be considered a subsidiary measure, seeing how the possibility of interception is made reliant upon the insufficiency of other measures. Third, interception is only to be used reactively, meaning that the measure is applied in the presumption that one of the aforementioned offences has already taken place, rather than to prevent it.

In a European context, Belgian law provides for the possibility of interception of wireless communication in accordance with the EU MLA Convention.[12]

As Belgian criminal law is familiar with concepts of interception of telecommunication and mutual legal assistance, it is feasible for Belgian judicial authorities to provide mutual legal assistance concerning interception of telecommunication vis-à-vis non – EU – member states.

3.2. Refusal grounds

With regard to refusal grounds concerning internet searches and other similar computer and network searches, national law remains silent. Simultaneously, Belgium is bound by refusal grounds derived from treaty law, more specifically those enumerated by article 27 § 4 of the 2001 Convention on Cybercrime.

For most forms of cooperation between the EU member states, the double criminality requirement has been lifted for a set of offences, including computer related crime in general as well as e.g. child pornography, incitement to terrorism, racism and xenophobia as content specific cybercrime offences. As a result, in spite of the diversity in the national criminalization provisions, states will not be able to call on that diversity to refuse cooperation. For reasons of completeness, reference can also be made to the more recent possibility to issue a declaration clarifying the scope of the offences for which double criminality has been lifted. In the cooperation with Germany, the use of the European Evidence Warrant is limited along the cybercrime definition found in the related framework decision, complemented with the definition included in the Council of Europe Convention.

3.3. Extraterritorial investigations

In principle, Belgian investigators can only exercise powers on foreign territory to the extent that mutual legal assistance arrangements allow them to do so. Clearly, there is no legislation allowing self-service abroad in general. However, in the specific context of information systems, reference must be made to article 88ter CCP, authorizing – under certain condi-

[11] Article 90ter § 2 CCP.

[12] Council Act of 29 May 2000 establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

tions[13] – the extension of a search ordered by the investigating judge in an information system (or a part thereof) to an information system (or a part thereof) located in a different place than where the search physically takes place, to the extent that the persons mandated to use the original information system to which the search pertains, have access to the information system (or part thereof) located in the different place. Unlike when the data accessed in this way appear to be located on Belgian territory (in which case the data concerned can not only be seized, copied, blocked, made inaccessible and even removed on the basis of article 39bis CCP), data located abroad may only be copied, in which case the competent authorities of the foreign country (provided that the latter can be reasonably identified) will be informed thereof through the Belgian ministry of justice. Finally, accession of publicly available information is considered unproblematic.

3.4. Databases and information exchange

Regarding information exchange, Belgium is a party to the 2007 PNR Agreement between the United States of America and the European Union,[14] as well as to the 2010 TFTP2 Agreement.[15] In accordance with article 35 of the 2001 Cybercrime Convention, the Federal Computer Crime Unit (FCCU), which is part of the federal judicial police's Direction for Combating Economic and Financial Crime, functions as a 24/7 call unit.

Furthermore, Belgium is a founding member of the 2005 Prüm Treaty, which entails a possibility of direct consultation of or automated (hit/no-hit based) comparison of data (fingerprints, vehicle registration data, DNA profiles) contained in national databases, without a need for a request. In 2008, the Prüm Decision[16] incorporated this instrument into the EU-acquis. With regard to the consultation of and contribution to international databases, Belgium frequently works with Interpol, the Visa Information System (VIS), the Schengen Information System (SIS), Eurodac, Europol and Eurojust, under the conditions set forth by their legal framework.

---

[13] Being that the extension is necessary in terms of truth-finding as regards the offence to which the search pertains and that other measures would be disproportionate or there is a risk that elements of proof would be lost if the search would not be extended.

[14] Agreement 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 (2007 PNR – Agreement); 30 November 2009. - Wet houdende instemming met de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het Ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), gedaan te Brussel op 23 juli 2007 en te Washington op 26 juli 2007.

[15] 2010 Agreement 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 the purposes of the Terrorist Finance Tracking Program.

[16] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

A possible future initiative worth mentioning is the European Police Records Index System, also known under its acronym "EPRIS".[17] This proposal is aimed towards developing a hit/no hit database, similar to the Prüm system, in order to find out if and where in the EU certain relevant (in particular suspect-related) information is available in criminal investigation databases.

3.5. Notice and take-down

Belgian criminal law is familiar with the concept of the notice and take-down of websites in as far as it is foreseen in an international instrument, e.g. Article 35 jo. 40 of the Prüm Convention. Additionally, article 39bis §3 CCP provides Belgian judicial authorities, more specifically the public prosecutor, with the competence to take down ('to make inaccessible') a website containing information that is to be considered criminal or contrary to public order and common decency.

An international enforcement system with regard to take-down decisions relating to cybercrime on a regional level (in particular the EU) seems feasible. In this case, an EU-instrument could serve as a legal basis for the concept. Given the kick-off as per the 1st of 2013 of the European Cybercrime Centre (EC3), hosted by Europol, such evolution would even seem a logical next step. EC3 will be the focal point in the EU's fight against cybercrime (encompassing in an initial stage: online fraud, online child sexual exploitation and cybercrime affecting critical infrastructure and information systems in the EU), contributing to faster reactions in the event of online crimes, supporting both member states and the EU's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

4. Human rights concerns

Although the involvement of information technology in criminal investigations can certainly be described as relevant from a human rights perspective, no specification of the legal consequences of the usage of such technology has yet been made explicit.

With regard to evidence collected by another state in violation of international human rights standards, reference must be made to Article 13 of the Belgian law of 9 December 2004 concerning international mutual legal assistance in criminal matters. This provision lists specific circumstances which imply exclusion before a Belgian court of evidence gathered unlawfully abroad. This is the case when the unlawfulness bears the mark of manifest illegality on account of infringement of essential procedural requirements according to the law of the state

[17] G. Vermeulen, V. Eechaudt, W. De Bondt, J. Focant, G. Kazlauskaité, W. De Wever, M. Lombaerts and T. Meulemans, EPRIS: possible ways to enhance efficiency in the exchange of police records between the member states by setting up a European police records index system, European Commission, Brussels, 129 p., http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/epris-final_report_en.pdf.

where the evidence was gathered or affects the reliability of the evidence. It does not follow from that, however, that all other unlawful foreign evidence will be per se admissible or not eligible for exclusion. The latter contrast with the applicable jurisprudence concerning nationally gathered evidence. Here the 2003 *Antigoon* Case, adjudged by the Belgian *Cour de Cassation*, establishes that nationally gathered irregular or unlawful evidence can remain admissible, provided the irregularities neither result in absolute nullity, nor impact the reliability of the evidence or the rights of the defense. This approach, which showcases a clear difference between unlawful evidence gathered abroad and domestically (minimum and therefore non-limitative exclusion conditions for foreign unlawful evidence vs limited inadmissibility grounds for national unlawful or irregular evidence), implies that the exclusion of evidence due to irregularities or unlawfulness is more likely to occur when such evidence is gathered by foreign authorities.

5. Future developments

5.1. Cross-border contact

Taking into consideration articles 10 and 11 of the EU MLA Convention,[18] the following is to be said concerning the influence of modern technology on cross-border contact. Due to the guarantees set forth by the classical rules on mutual assistance, it is essential that these be applied to all contact with the accused as well as with witnesses during a trial. These guarantees are less of an issue with regard to victims. Here, modern technology could, for instance, allow a victim to follow the trial from a distance. With regard to an investigation, it is conceivable that a police officer uses telecommunication equipment instead of sending out a mutual legal assistance request, provided that there is no pressure or coercion to provide information. It is, for example, perfectly feasible that a Belgian police officer simply calls a Dutch victim in search of information, provided he or she doesn't pressure the victim in question.

Further, a possible application of the *aut exequi, aut tolerare* principle[19] seems like an attractive possibility. This principle entails that a state, when unwilling to execute a mutual legal assistance request for capacity reasons, must tolerate the execution of investigative measures (e.g. hearings) on its territory by the competent authorities of another state. Though this principle may sound revolutionary, accepting the competence of foreign authorities to operate on their territory is already accepted in cross-border surveillance or hot-pursuit situations, and is also used in the context of setting up joint investigation teams. The

[18] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

[19] See: G. Vermeulen, *Free Gathering and Movement of Evidence in Criminal Matters in the EU : Thinking Beyond Borders, Striving for Balance, in Search of Coherence*. Antwerp, Belgium; Apeldoorn, The Netherlands: Maklu, 2011, 51 p.

acceptability of applying this new principle in this particular context could be increased considering that new technologies allow execution of these measures without actively entering the territory of the other state.

5.2. Skype

Skype does not provide adequate guarantees required for a videoconference. As such, it is not advisable to use Skype-technology to set up hearings via screen in transnational cases. Skype-technology could be used as an alternative for telephone hearings. The scope for telephone hearings is much more narrow compared to video hearings, seeing how much of the non-verbal communication – essential when adjudging the reliability of a witness – is lost.

5.3. Other issues

Additional issues, brought about by technological advancement, concern mostly the possibility for (potential) offenders to remain undetected. Pre-paid SIM cards, which require no registration, allow for perpetrators to make phone calls which are untraceable, a phenomenon that completely undermines any regulation concerning interception of telecommunications. Equally untraceable is internet use through hot spots using alternating IP addresses, e.g. in airports. VoIP, also known as voice over IP, allows telephone calls using the internet. When using VoIP from a hot spot, these conversation may well remain impossible to trace. Furthermore, detection on the internet can easily be dodged, especially by using the Tor Browser, but also by simply installing an IP-shielder. Even using the "incognito-mode" readily provided by Google Chrome is rendering law enforcement more difficult.

Other challenges, because largely unregulated, are cross-border observation through camera use, spy drones and environmental taps (from a distance, e.g. through laser measuring of window vibration and deducting voice from that).