PREPARATORY COLLOQUIUM FOR THE XIXTH INTERNATIONAL CONGRESS OF PENAL LAW (MOSCOW, 24–27 APRIL 2013)*

DOMINIK BRODOWSKI,
Ludwig Maximilians University (Munich, Germany)

For most crimes, the Internet in particular or information technology in general is merely one of several means they can be committed. With information and communications technology becoming ever more important and essential to our day-to-day lives, some 'old' crimes such as theft need to be re-thought, and 'new' crimes such as protecting data integrity need to be considered. This was the broad scope of a conference hosted by the Russian Association of Lawyers and Lomonosov Moscow State University and chaired jointly by *Vladimir Komissarov* (Russia) and *Katalin Ligeti* (Hungary) from April 24th to 27th, 2013. The recommendations drafted at this event will set the stage for the Second Section of the XIXth AIDP[197] International Congress of Penal Law, which will take place in September 2014 in Rio de Janeiro, Brazil.

1. The shift from industrial to information societies and its impact on substantive criminal law

The shift from industrial to information societies shakes two foundations or themes commonly found in criminal justice systems all over the world: their focus on human decision-making, and their focus on tangible goods.

In information societies, at least some decision-making is transferred from humans to machines.[198] Automatic Teller Machines (ATMs) instead of cashiers control whether a customer may withdraw money; high-frequency trading decisions are made autonomously by sophisticated computer systems; and some automatic intelligence

---

[197] Association Internationale de Droit Pénal / International Association of Penal Law (AIDP / IADP) <http://www.penal.org/> accessed October 2013.

[198] Cf K Tiedemann and B Valerius in K Tiedemann (ed), *Strafgesetzbuch, Leipziger Kommentar* (12th edn, Walter de Gruyter 2012) para 263a, 2.

processing systems[199] may determine whether to put someone on a 'no-fly list'. While the implications on the victim side have been quickly understood, and criminals law have been extended accordingly (eg through provisions on *computer fraud*), the perpetrator side requires more thought in terms of attribution and *mens rea*.

As to the second point, criminal laws have put a strong focus on tangible goods for a long time, especially on tangible goods of value, such as buildings, gold, or coins. These goods needed – and still need – criminal law protection against being damaged or destroyed (eg by arson), against being forged (eg by counterfeiting of coins), and against illegal re-allocation (eg by theft, blackmail, or fraud).[200] *Information*, however, has certain characteristics which cause severe frictions with this classic approach of criminal law:[201] Unlike a chocolate bar, information can be duplicated and made fully available to more than one person at (almost) no cost. Information can be transferred from one country to another (almost) instantly. And processing large amounts of information is becoming ever easier. All this means that protecting information by criminal law against destruction, forging, illegal access and illegal distribution, but also the prohibition of certain kinds of illegal information (such as child pornography) require distinct concepts, thresholds, and limitations to the classic, tangible-centric approach of criminal law.

Moreover, with information societies becoming more and more intertwined, information flowing freely worldwide, and with computer crimes being easily committed across state borders, harmonizing computer crime laws becomes ever more important. Traditionally, much focus has already been spent on setting such minimum bars of criminal law protection through international law, eg by the – disputed – Council of Europe Convention on Cybercrime.

More emphasis, however, may have to be put also on the other side of the coin, that is, what may *not* be criminalized. The positive aspects of the Internet, being founded on a high level of freedom, anonymity and *égalité*, can only continue to flourish if these aspects are preserved and guaranteed, and *some* risks are accepted as necessary costs of a free society.[202] To me, it seems that extradition laws and asylum – which only offer limited protection against an overly broad extra-territorial

---

199 Such as the (abandoned) CAPPS II – Computer Assisted Passenger Prescreening System developed by the US.

200 When fiat money and especially book money emerged, criminal law protection was soon extended to these forms of intangible property. That process was eased by the fact that these forms of property can, in principle, only be allocated to one person at a time. Therefore, they are more closely linked to tangible property than to pure information.

201 Cf D Brodowski and FC Freiling, *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft* (Forschungsforum Öffentliche Sicherheit 2011) 54–61; U Sieber, *Straftaten und Strafverfolgung im Internet* (CH Beck 2012) C 84ff, C 153.

202 Cf D Brodowski, 'Cyber-Sicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets' in HJ Lange and A Bötticher (eds), *Cyber-Sicherheit* (Springer 2013).

enforcement of criminal laws – and international human rights law – which only guarantees a *minimum* standard – may not provide sufficient 'safe harbors' for the citizens of the Internet age, the *netizens*.

This implies that more regulatory decisions must be taken on the international level, such as decisions on striking the balance between legitimate whistleblowing and illegitimate data disclosure; on the balance between freedom of expression and libel and slander; on the balance between intellectual property and the fair use of information and knowledge. Criminal law, due to its moral impetus – and its internationally strong enforcement system – serves as an important regulatory model, but it can provide only one piece of the puzzle of adapting the laws to the age of information society.

2. Cybercrimes as one piece of the puzzle

In their welcoming words at the preparatory colloquium, Vice-Dean *Natalia Kozlova* (Russia) and *Komissarov* pointed out that different paths to tackle cybercrime are taken in different regions of the world, which makes 'Information Society and Penal Law' an excellent umbrella topic for the upcoming Congress. It also underlines the role the first-ever preparatory colloquium hosted in Russia may serve in this regard. *John Vervaele* (Netherlands) thanked, on behalf of AIDP, the Russian Association of Lawyers and Lomonosov Moscow State University for organizing this event, and went on to point out how the relationship between cybercrime and cybersecurity, which at first was only discussed thoroughly in the USA and in Russia, has now become a worldwide issue. The worldwide communications structures have become interests as such, but face systematic attacks where the infrastructure of the 'digital society' is at stake. It is still an open question, so *Vervaele*, to what extend criminal justice plays, should play and should not play in the protection of the digital infrastructure. Some thought on this matter has already been spent on this matter, such as in floating the idea on a protocol on cybercrime to the UN Convention on Transnational Organized Crime (the so-called Palermo convention) or on a distinct UN convention on cybercrime. *Vervaele* then introduced the classical differentiation of three types of cybercrimes, as utilized in the Council of Europe Convention on Cybercrime (the so-called Budapest convention) – first, crimes concerning confidentiality, integrity and availability (such as illegal access, system interference and misuse of devices); second, computer-related offenses (such as computer-related forgery or computer-related fraud); and third, content-related offenses (such as child pornography).

The general rapporteur for the Second Section, *Emilio Viano* (USA) summarized his key findings from the national reports received. As many European countries – most of them current or future member states of the European Union – replied, but only two non-European countries (Argentina and Brazil), *Viano* noted that more thought needs to be spent on other regions of the world and their approaches on cybercrime, and pointed

out how important the interrelation between cybercrime provisions and other areas of law are – such as criminal procedure or intellectual property law. For example, new non-compliance offenses require or cause the retention of many data, and advances in modern technologies (eg locational services) lead to the storing of ever more data. All this data may later on provide a useful – but potentially dangerous – tool for investigators (and competitors) to go on 'fishing expeditions' to look out for incriminating or discrediting information. This may lead to 'chilling effects' and to new dangers on privacy, which also needs to be taken into account when formulating criminal provisions.

3. Criminal law and cyber security

In starting the second session, *Komissarov* discussed the interrelation of Criminal Law and Cybersecurity. He pointed out that international cooperation is *the* key in tackling the misuse of the global information technology for illegal means, as not only the Internet but also many cybercrimes are transnational in nature. According to *Komissarov,* the first and foremost issue to enhance international cooperation and to tackle transnational cybercrimes is to harmonize activities and laws; therefore, he went on to highlight some issues Russia faces in its cybercrime legislation. First of all, he noted a certain ambiguity when we talk about computer crimes, as that term may be interpreted in a narrow sense – referring to computer data or computers as an *object* of criminal law protection – or in a broad sense – also including crimes committed *using* information and communications technology. Secondly, he noted that the Russian legislation has not kept up with the advances in modern technology in the past 17 years. This causes problems in terms of legal certainty when adapting the three articles on computer crimes drafted in 1996 to current cybercrimes. Thirdly, conflicts of jurisdiction are in practice mostly 'solved' by the random fact which country is first to arrest the offender, but this approach may cause tensions at the international level. Finally, due to the complexity of modern cybercrimes, one crime may in fact be covered by several different statutes. In the Russian criminal justice system, this may cause duplication in punishment. *Komissarov* expressed his hope that discussions both in this preparatory colloquium and 2014 in Rio de Janeiro may provide valuable input enabling Russia – but also other states – in addressing these issues.

4. Regulating Cybersecurity

Later on, *Oleg Demidov* (Russia) addressed the question of 'Adaption of the international humanitarian law vs development of new international legal mechanisms: alternative or complementary approaches to the regulation of conflicts in cyberspace'. He noted that cyberspace regulation so far is largely out of reach of international law, at least on a global perspective. This is underlined by the fact that neither cyberwar nor cybercrime share a common definition.

Demidov pointed out that one possibly way forward is the development of new international legal mechanisms. One such means could be the broad draft of a UN Convention on Information Security which was tabled by Russia in 2011 and which also covers the protection of information infrastructure against aggressive behavior by other states. The reality of international diplomacy has slowed its progress down, though, as it faces severe criticism by the US and Western Europe, especially for provisions on prohibiting the use of information technology for undermining social stability in other states. Therefore, Russia nowadays is updating its proposal and aims at agreeing upon such a convention with other major players, possibly with the exception of the US.

Another path taken, though, is the adaption of existing international humanitarian law, eg the Hague and Geneva Conventions and customary international law. Based on these sources, a Tallinn Manual on the International Law Applicable to Cyber Warfare was recently published by an independent expert group. Though it was written on invitation by the NATO Cooperative Cyber Defense Centre of Excellence, it does not reflect an official view. The Manual asserts that cyberterrorism may lead to self-defense, so that cyberterrorism may not only become a case for law enforcement, but also for military action. Furthermore, it suggests that not all cyberwarfare operations against civilians are prohibited, but only attacks which injures or spreads terrors among the civilian population. Moreover, the Manual also addresses questions of command responsibility.

Demidov considers both approaches to be potentially complementary, but adds to the picture a procedural and jurisdictional perspective by calling for an international criminal court or tribunal for cyberspace (ICTC).[203] Such an international body should, according to *Demidov*, have jurisdiction on individual criminal responsibility for certain acts of cyberwarfare, especially when critical infrastructure is at stake. In response too *Ligeti*'s question, *Demidov* acknowledged that his concept of cybersecurity is indeed largely linked to the Russian draft convention. Therefore, he considers it ever more urgent to come up with an international solution as soon as possible.

5. Online social networks and violations committed by information technology

Stanislaw Tosza (Poland) presented his special report on 'Online social networks and violations committed by information technology – identity fraud and theft of virtual property'. Marco Gercke's disputed definition of the phenomenon as a 'criminal act where the perpetrator fraudulently obtains and uses another

[203] S Schjølberg J, 'An International Criminal Court or Tribunal for Cyberspace (ICTC)' (2011) EastWest Institute (EWI) Cybercrime Legal Working Group Paper <http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf> accessed September 2013.

person's identity'[204] shows that three elements are at stake: first of all, acquiring the information, eg through phishing, hacking or insider attacks, secondly the possession and/or transferring of this information, and thirdly the use of this information for criminal purposes. Within this last step, *Tosza* differentiated further between using the information within social networks (eg to create fake profiles or to adding information to existing profiles) or outside social networks (eg to commit tax or bank fraud or to go shopping online using another person's identity). Identity fraud within social networks may pursue a large variety of criminal goals, starting with advertisement and spamming over financial gains (eg if males are lured to a fake profile of an attractive supermodel) to cyber bullying.

After this phenomenological overview, *Tosza* noted that his comparative analysis showed that state reactions to identity fraud largely follow three categories: some states use an all-encompassing provision to criminalize identity fraud (eg in the US, Canada, Australia and – *de lege ferenda* – in Argentina), others only criminalize impersonation (eg France, India, Italy, Poland), and some criminal justice systems lack specific provisions (eg Germany and the requirements to national penal laws specified in the Council of Europe Convention on Cybercrime). *Tosza* concluded that while there are similarities to classic, 'offline' types of identity-theft, there are also distinctions in social networks which call for specific offenses, which should include fictitious profiles. Some steps in this direction may be taken by the European Commission, *Tosza* noted, as its DG Home Affairs is currently looking into identity fraud and identity theft.

On questions by *Vervaele* and *Viano*, who pointed out the risk that such provisions would infringe the freedom of expression and that it may be legitimate or even necessary to impersonate another (fictitious) person in some societies, *Tosza* acknowledged that a requirement of intent should guard against overcriminalization. However, *Nils Rekke* (Sweden) and *Hein Wolswijk* (Netherlands) advocated using more general criminal provisions instead of adding specific provisions. Moreover, *Tatiana Tropina* (Russia) pointed out the implications to the anonymous use of the Internet which such specific provisions may cause. *Tosza* replied that he considers identity theft to cause a certain, distinct harm in itself, leading to a need for specific criminal provisions which should also cover the acquisition and transferring of data, not only the (mis-)use of it.

6. The gist of the national reports

Each national rapporteur present at the preparatory colloquium was given the floor to report shortly on the main points of their findings. *Madalena Pampalk* noted that there is very little jurisprudence yet on the cybercrime provisions in Austrian. The legislation is mostly influenced by and in accordance with European

[204] M Gercke, *Computer und Recht* (CH Beck 2005) 606–612.

Union requirements. However, the provision on unlawful access to computers faces criticism as it requires triple intent which is very difficult to prove in court: intent to obtain the data, intent to make the data available to another person or to the public, and intent to obtain a financial gain.

Olivier Leroux and *Stijn de Meulenaer* noted that Belgian jurisprudence on cybercrimes is on the rise. Both the legislative and the jurisprudence approaches move from a 'substance'-related view of crimes to a data-oriented view, such as can be seen in case law which considers fake credit cards to be fake computer systems, and which considers the provision on theft to be applicable not only on 'real' goods and electricity, but also on 'virtual goods' – as long as these goods have economic value and can only be owned only by one person at a time.

Eduardo Saad-Diniz pointed out that Brazil lacks specific regulations except some symbolic provisions, eg on child pornography. As information technology is on the rise also in Brazil, there is a need to improve criminal law protection and to avoid impunity, but also to guard against overcriminalization.

The last major reform of cybercrime laws in Finland occurred in 2007 with the goal to implement the Council of Europe Convention on Cybercrime and related EU legislation. *Jarmo Koistinen* also reported a lack of judicial proceedings in this area. However, it was decided that theft and other crimes requiring 'movable property' are not applicable to the virtual world, so that 'virtual goods' and 'personal data' cannot be stolen or fraudulently be used.

Roberto Flor reported that the Italian law of the land on cybercrime was most recently amended in 2012 to implement the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the so-called Lanzarote Convention). He is worried about the diversity of legal offenses leading, in some parts, to overcriminalization. A current major issue in Italian jurisprudence concerns omission liability of Internet Service Providers for crimes committed by users.

German national rapporteur *Bettina Weisser* suggested to structure the discussions by distinguishing the legal interests to be protected – economic interests, content-related issues relating to the society as a whole (such as propaganda or incitement to racial hatred) and interests of the individuals (such as violations of the secrecy of personal data or unlawful intrusions into private life). In contrast, however, the German cybercrime law is unstructured and needs to be considered to be 'work in progress'. *Weisser* pointed to judicial decisions on online demonstrations – the legislator reacted to acquittals by amending the German criminal code – and to the question whether one possesses child pornography if the data is only stored in cache files or only in a computer's memory.

According to *Wolswijk*, the Dutch legislator made a fundamental choice in 1993 to consider 'data' not to be 'goods', even though the latter term traditionally also covers non-tangible objects such as electricity. This choice was taken as the legislator didn't seem it wise to maintain the same level of protection, especially as such an

approach would hinder the free flow of information. However, with amendments in 2006 and currently under discussion, in the end 'data' has become protected more or less the same as 'goods'; also, Dutch criminal courts do apply the criminal law provision on 'theft' also when virtual objects are stolen. Therefore, *Wolswijk* suggests reconsidering the decision taken by the legislator in 1993.

Małgorzata Skórzewska-Amberg reported that the Polish legislator attempts not to describe special cases of cybercrime, but instead prefers to formulate laws to apply both 'online' and 'offline'. For example, a criminal law provision on bullying also covers 'online' acts. Her largest concern relates to crimes on child pornography, which were already changed several times in Poland. For pornography depicting 15 to 18-year old children, intent to disseminate is required for conviction, which has proven to be unpractical.

Tropina added to *Komissarov*'s presentation that the Russian law on cybercrime is not bad per se, but its structure is incompatible to international standards, especially as it was formulated before the Council of Europe Convention on Cybercrime was drafted. For example, it links illegal access and data interference together, which proves to be too narrow in today's world. On a question by *Koistinen*, *Tropina* referenced that Russia is not inclined to ratify the Council of Europe Convention on Cybercrime and that, in fact, its inclination to collaborate on the basis of this convention has decreased in the past few years. The main obstacle relates to art 32(b) of the Convention, which allows for a transnational access to private data by state authorities. She added that while the convention allows for reservations in principle, it does not so in relation to art 32.

In Sweden, an expert committee discusses what changes are required to implement the Council of Europe Convention on Cybercrime, the accompanying Protocol and related EU legislation. According to *Rekke*, the committee's opinion seems to be that the substantive criminal code is already in accord with these requirements. Traditionally, Sweden has tried to have a technique-neutral legislation, so that eg the provision on fraud already covers acts of fraud committed online. Furthermore, the Swedish law on child pornography also covers virtual child pornography as well as the intentional observation of child pornography.

7. A comparative perspective and the way forward

In summarizing these and the other reports received, *Viano* noted that most countries mentioned the Council of Europe Convention on Cybercrime and European Union instruments as international legal sources and a need to bring their legislation in line. This euro-centric view needs to be overcome, at least at the Congress in Rio de Janeiro. *Viano* pointed out that one of the main questions this section faces is whether and to what extent cybercrimes are specific, or merely attributive to old and long-known crimes and thus new wine in old bottles.

Viano went on to discuss several common cybercrimes from a comparative perspective. Regarding the common cybercrime of illegal access, additional elements such as whether the access relates to systems or to data cause tension on the international level. Intercepting communications data is also a common crime – as it dates back to the interception of telegraphs – but nowadays increasingly faces the difficulty of distinguishing (unprotected) public from (protected) private communications. Regarding the misuse of devices or so-called 'hacking tools', there is a strong need to criminalize only the criminal use, not the ethical use of the same devices or tools eg in self-defense or in protecting one's own systems. Therefore, many countries require a specific intent; it may be useful, though, to distinguish two types of devices – malware on the one hand, passwords on the other – in future. On privacy and data protection, *Viano* reflected on the notion of a post-privacy society and noted that most reports distinguish between involuntary and voluntary disclosure of data, even though this distinction is less clear in practice than it is in theory.

Overall, *Viano* noted some convergence in criminal provisions on cybercrimes, especially when the national laws are brought in line with the Council of Europe Convention on Cybercrime. On a broader perspective, one needs to take a balanced approach between a 'maximalist' call for criminal law protection, especially by those who fear a cybercrime 'epidemic', and the 'minimalist' approach which is concerned about overcriminalization and fearsome of a growing intrusion of the state on the private life of the citizens.

Taking this into account, *Vervaele* proposed to draft the resolutions on three building blocks, namely criminal policy – what are the *lacunae* we should address, where is a need to reduce overcriminalization, – regulatory design – including the question of deference to the judiciary – and legislative technique. *Viano* referred instead to his first draft of resolutions and called for a specific and detailed approach, taking into account a pre-existing academic proposal on a global protocol on cybercrime,[205] with the AIDP taking a position on specific aspects of each crime. In response, *Gert Vermeulen* (Belgium) proposed to address the general questions – eg regarding the place of criminal law in regulating the Internet – and the underlying principles – proportionality etc – first, before tackling the intricate detail questions.

In a first discussion on the draft resolutions, the group focused on its concerns and its aims which should be reflected in the preamble. It was noted that an evidence-driven approach needs to be taken which guards against overcriminalization and against overly restrictions of personal liberty, but provides – in general – no less protection 'online' than 'offline'. Concern was expressed of overly relying on penal sanctions instead of other regulatory options. Instead, the responsibilities of the

[205] S Schjølberg and S Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime* (Cybercrimedata 2009) <http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf> accessed September 2013.

private sector in securing the cyberspace and preventing cybercrimes must be taken into account. On the next day, based on an updated draft by *Viano* and in fruitful and open-minded discussions, consensus could be reached on both the preamble and on the recommendations which are now submitted to the Congress in Rio de Janeiro. The preparatory colloquium concluded with expressing gratitude to its hosts, and especially to *Gleb Bogush* and *Maria Filatova* for taking care of all administrative burdens.

References

1. Brodowski D and Freiling FC, *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft* (Forschungsforum Öffentliche Sicherheit 2011) 54–61.

2. Brodowski D, 'Cyber-Sicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets' in HJ Lange and A Bötticher (eds), *Cyber-Sicherheit* (Springer 2013).

3. Gercke M, *Computer und Recht* (CH Beck 2005) 606–612.

4. Sieber U, *Straftaten und Strafverfolgung im Internet* (CH Beck 2012) C 84ff, C 153.

5. Tiedemann K and Valerius B in K Tiedemann (ed), *Strafgesetzbuch, Leipziger Kommentar* (12th edn, Walter de Gruyter 2012) para 263a, 2.

Information about the author

Dominik Brodowski (Munich, Germany) – Senior Research Assistant at Ludwig Maximilians University (1 Geschwister Scholl Platz, Munich, 80539, Germany, e-mail: dominik.brodowski@jura.uni-muenchen.de).