SECTION I – CRIMINAL LAW GENERAL PART
INFORMATION SOCIETY AND PENAL LAW
GENERAL REPORT

Thomas WEIGEND*

(A) Introduction: Scope of the Report
This report deals with crime related to information and communication technology (ICT) and cyber space. These crimes affect individual and collective interests which, in the 21st century, define the quality of life for many individuals. It is therefore a timely effort on the part of the AIDP to address issues of “Information Society and Penal Law” in its XIXth International Congress of Penal Law.

This report is based on responses from 16 legal systems1 to the questionnaire approved by the Board of Directors of the AIDP and distributed to the national groups. The General Reporter is most grateful to the authors of the excellent national reports, which contain a wealth of information and highly relevant considerations. In addition, Mr. Stanislaw Tosza has submitted a special report on social networks, which has also been a most valuable source for this Report.2

The deliberations of Section I of AIDP Congresses have traditionally been devoted to issues of the General Part of the criminal law. But there are few issues concerning what is normally regarded as the “General Part” that relate specifically to ICT and cyber crime. Therefore, the decision was made to define the area of the debates of Section I more broadly and to cover:

- protection of legal interests specifically related to ICT and the challenges of cyber space;

* Professor of Criminal Law. University of Cologne (Germany)
1 National reports have been received from Argentina (AR), Austria (A), Belgium (B), Brazil (BR), Finland (SF), France (F), Germany (D), Greece (GR), Hungary (HU), Italy (IT), Japan (J), the Netherlands (NL), Poland (PL), Romania (RO), Spain (E), and Turkey (TR).
2 Reference to the special report will be made by the abbreviation SNW for “social networks”.
- extension of criminal prohibitions, e.g., to preparatory acts and to the possession of materials;
- the problem of respecting the principle of legality, especially the requirement of precision in criminal prohibitions;
- changes in the concept of perpetratorship and accessorial responsibility, especially with respect to access providers and web hosts;
- the role of criminal law in relation to alternative ways of protecting legal interests, especially by web-specific means such as blocking of access or removal of websites;
- legislative reactions to the problem that internet users often remain anonymous;
- international efforts in coordinating and harmonizing law in an area that is definition transcends national borders.

The breadth of the agenda for the deliberations of Section I is related to the specific challenges of ICT and cyber crime, which differs in many ways from old-style criminality. It is these challenges that make dealing with ICT and cyber crime both interesting and difficult. Typically, concepts developed for traditional crime do not quite fit for ICT and cyber crime, hence they may need to be adapted in a somewhat flexible fashion. On the other hand, the principles protecting against an overbreadth of the criminal law, such as the principles of ultima ratio and of legality, may have to be re-defined and adapted to the specifics of ICT and cyber crime.

When we refer to ICT and cyber crime, these expressions comprise quite diverse phenomena. We can distinguish four types of criminal conduct that this report will deal with:

1. "ordinary" criminal offenses, e.g., fraud or forgery, that are committed by means of information and communication technology;
2. crimes directed against the proper functioning of ICT systems, e.g., hacking, manipulation of computer systems, or the destruction of stored data;
3. "ordinary" crimes, e.g., fraud, stalking or defamation, committed by means of the World Wide Web;
4. According to a survey, around 80% of adult internet users in Brazil were victims of some sort of cybercrime, such as the invasion of profiles in social networks, phishing, and viruses.
(4) crimes against interests that are web-specific, e.g., the “theft” or manipulation of virtual personalities.

It does not require explanation that the legal and practical problems connected with these four types of crimes differ significantly from each other. It is an open question whether one can or even should try to develop common principles for criminal laws concerning ICT and cyber crime as such. In this report, no effort will be made to develop a “system” of ICT and cyber criminal law that would contain rules for all of these offenses. Rather, the General Report limits itself to presenting, in strongly abbreviated and simplified form, the “state of the art” with respect to some of the issues named above as can be gleaned from the various legal systems included in this study.

(B) Legal Interests Protected by ICT and Cyber Criminal Law

(1) General Aspects

(a) Conventional Crimes “going digital”

ICT and the cyber space have enabled offenders to be more “efficient” than in earlier times when they wish to commit fraud, slander, copyright violations, and other traditional crimes. They can use computers and/or the web in order to address, with one single mouse click, millions of potential victims or do to vast harm to the reputation or the protected copyright of a single victim. But in these instances only the modus operandi differs from traditional forms of fraudulent or slanderous conduct; the interests affected remain the same. As the Dutch report points out, in devising new crime definitions for traditional offenses “by using computers”, one needs to be careful to avoid overlap or an imprecise duplication of criminal provisions covering more or less the same conduct. There may also be problems concerning the principle of equality when an act that is not punishable (or punished less severely) in the “real world” is defined as a serious crime where the perpetrator employs ICT technology or the web in order to commit the offense.

Examples of “computerized” versions of traditional crimes contained in criminal codes are fraud by using ICT systems, revelation of government secrets stored

---

6 For a mix of all these types of crime in one act of legislation, see AR 2.
7 For a list of “traditional” legal interests protected against interference through ICT, see A 1, TR 1.
8 The Dutch report speaks of “a new dimension of the classic crime”; NL 7.
9 NL 7.
10 See B 13: The Belgian Constitutional Court found a violation of the right to equality where the offense of cyber stalking carried more severe penalties than the general crime of stalking.
11 Belgium has introduced a new crime of providing illegal opportunities for gambling on the net; B 10.
electronically, forgery of digitally stored data, and defamation or stalking ("cyber bullying"). Copyright violation by illegally offering or downloading protected materials in the internet is another example of a "conventional" crime taking on a different quantitative (and perhaps qualitative) dimension when the commission is facilitated by the opportunities created by the web. In France, commission of a copyright violation through an online or public communication network is regarded as an aggravating circumstance. Finally, pornography (including pornography involving children) is today mainly transmitted and distributed electronically, hence some legal systems have introduced special criminal prohibitions concerning "cyber porn". Where perpetrators use social networks for establishing contact with potential victims of sexual offenses, in particular with children, they cross the line between traditional crime (contacting children with the purpose of committing sexual acts on them) and the type of crime that depends on the existence of the internet. "Grooming" of children for potential sexual abuse has indeed been defined as a criminal offense in many jurisdictions.

---

12 See A 5, B 20, GR 11-15, 28-29, SF 6.
13 See GR 5, 26-27.
14 D 6, E 2, GR 28, J 3, SF 5-6. In the Netherlands, the courts have extended the traditional crime of forgery of written documents to similar manipulations of digitally stored data; NL 15.
15 See SNW 10.
16 See B 11, GR 22-24, 30-31, NL 21, PL 5, SF 8-10 (mentioning specific problems in adapting old provisions against copyright violations to new circumstances), TR 3. See also E 7 (discussing lack of adaptation of the statute on copyright violations to distribution of protected materials through the net).
17 F 4.
18 See AR 4, BR 6, F 4, J 4, RO 2-3. German law still requires transfer of some pornographic "material" and therefore fails to cover streaming and other non-material transmission of digital recordings; D 8. The Polish report (PL 5) points out that digital technology offers new possibilities of creating pornographic materials: "Advancement and expansion of digital technologies have contributed to the development of relatively cheap tools allowing to create virtual reality, including pornographic materials, mostly simulated child pornography, i.e. artificially generated materials showing more or less realistic images of a non-existing person or modified images of adults made to look like children, or children used "virtually", which means modifying children's images." It is an open question whether such materials should be put on the same level as materials depicting real children. Whereas Polish law covers such images, Austrian law, for example, limits punishability to the distribution, display etc. of images that appear to depict real events (A 6-7).
19 See, e.g., A 7, E 3.
(b) New Offenses

Other forms of ICT and cyber crime are directed against interests that did not exist before the invention of computers and the advent of the WorldWideWeb. It is one of the challenges of the criminal law of the 21st century to correctly define these legal interests, to protect them from improper interference and at the same time to draw limits to the scope of criminalization. The latter concern is important because the invention of ICT and the creation of cyber space have opened up to individuals a host of new possibilities and a new sphere of freedom not only of gathering information but also of spending their time, of being creative, of communicating with others, and of pursuing commercial interests. If criminal law is applied too broadly, individuals are deprived of this new freedom and its great potential for self-fulfilment. It would be a high price for society to pay if its members were afraid of surfing the net or of using the comfort offered by ICT in their daily lives for fear of criminal punishment if they take a wrong step. It is therefore crucial that criminal prohibitions be devised such that they curb serious and harmful misconduct but do not restrain too severely the freedom of the cyber world.20

Several legal systems emphasize the need to protect the functioning of individual ICT systems (computers, networks, etc.) through criminal laws.21 In a broader sense, the public trust in the “functioning” of ICT systems and of cyber space as such is seen as needing protection,22 because it is “a supra-individual macro interest which encapsulates all the diffuse interests without which secure communication is impossible in cyberspace”.23 The main interest to be protected here is the confidentiality, integrity and availability of information systems and electronic data.24 As the Polish national report points out, there are indeed individual liberties at stake whenever the functioning of cyber space is being jeopardized:

"The main legal interest protected by criminal law with regard to virtual space (cyberspace) is the traditional freedom and security of an individual, yet understood from a specific, cyberspace-oriented perspective. Therefore, the right is understood inter alia as the right to privacy of the individual, as trust of individuals to electronic system, as trust to documents and data stored in such a system. Also an individual’s right to decide on information is protected (i.e. an individual’s right to freely decide for instance as to the free and exclusive right to

20 See IT 12 on the limited utility of the concept of protected interests (Rechtsgut) in preventing an over-extension of criminal law in this area.
21 See, e.g., TR 1.
22 See BR 2-3, E 1, J 1.
23 E 1.
24 GR 2.
administer information in the individual’s disposal, as well as to freely decide on
the scope and type of disclosed data referring to the individual), as well as the
constitutionally guaranteed right to protection of privacy and secret of
communication.”

This general interest in maintaining the “institutional” integrity of the ICT and cyber
world can be broken down into more specific aspects, all of which are sensitive to
illegal interference.

(2) Particular Interests

(a) Interference with ICT systems

One basic interest is the “integrity” of private or public ICT systems, that is, the
functioning of these systems in accordance with the operating rules and the input
provided by the rightful owner. Because any unauthorized interference can cause
grave harm and threatens to undermine the trust in the proper functioning of the
ICT system in question, many legal systems provide for criminal punishment of
such interference. Unauthorized transmission and changes of data, removal and
destruction of data and software as well impeding access to an ICT system are
typical offense descriptions of a crime that might best be described as “computer
sabotage.” In some legal systems, the destruction, falsification or concealment
of data stored in someone else’s ICT system is regarded as a separate offense.
Infection of an ICT system by a virus or similar malware is normally covered by
the general provisions against interference with ICT systems. In some states,
even the intentional possession of such malware can be punished; but
unintentional (even reckless) infection of a system by a virus is not a criminal
offense.

(b) Hacking

In order to manipulate or sabotage an ICT system, it is necessary to acquire
access to it. Since most ICT systems are protected from unauthorized access, a
person needs to break through the security system installed by the owner in order
to obtain confidential information stored in the system or to eventually manipulate

25 PL 2. For a similar assessment, see F 1. The Greek national report correctly points out
that “electronic data constitute … the means for participation in the information society”;
GR 3.
26 Concerning the problems of a legal system where no such protection is provided as yet,
see GR 6-10, 25-26.
27 See, e.g., A 2, B 6, BR 3, D 4-5, E 1; F 2, IT 2, J 1-2, PL 3-4, RO 2, SF 4-5, TR 2-3.
28 See, e.g., A 4, D 7, F 3, IT 3, J 3.
29 See AR 3, A 5, B 6, D 7, E 3, PL 4, TR 3.
30 See BR 6-7 (lex ferenda), F 3-4.
31 See SF 4.
Many legal systems have defined this act of “hacking” someone else’s ICT system as criminal, regardless of the purpose the offender seeks to accomplish. Modern legislation therefore describes the offense merely as entering a protected ICT system without authorization, even if the offender does not (or may not even wish to) obtain information stored in the system. With regard to the interest in the “integrity” of an ICT system, hacking is an offense of endangerment, because the unlawful entry does not by itself affect the proper functioning of the ICT system in question.

(c) Illegal Monitoring

A related but different offense is the breach of the confidentiality of an ICT system by installing or using monitoring devices or software. Illegal (private) wiretapping is an older precursor of this crime, and sometimes that offense has simply been extended to ICT systems. Illegal monitoring differs from hacking by the fact that the perpetrator not only enters an ICT system without authorization but also seeks to obtain information that has been stored there or will be transmitted to that system.

(d) Innovative Criminal Prohibitions

The cyber world not only opens up many new possibilities for communication, commerce and the dissemination of information and opinion but also creates new interests that can be harmed by others. The law needs to react to these new sensitivities. It is therefore no surprise that some legal systems have created new offense definitions specifically geared toward protecting individual interests in the cyber world.
A very general criminal provision against cyber harassment has been introduced in Belgium in 2005. According to that law, it is a criminal offense for any person to “use a network or electronic communications service or other electronic means to annoy or cause damage to his correspondent, or to install any device intended to commit the offence and the attempt to commit it.”40 One may wonder whether (and if so, why) annoying a person through electronic means is more reprehensible than annoying him face-to-face.

Another risk typically associated with the internet is the quick dissemination of photos and images of persons without their consent or against their will. The Spanish legislature has addressed this problem by creating the crime of broadcasting, revealing or providing to a third party, without the authorization of the affected person, “images or audiovisual recordings of the affected person that were obtained with his consent in a home or any other place out of the sight of third parties, when the revealing of such image seriously undermines the personal privacy of that person.”41 It is interesting to note that this offense definition does not apply to the unauthorized making of photographs or recordings but only to their unauthorized dissemination, which will typically be accomplished by using the internet.

A similar Dutch offense definition is narrower in that it only covers the “distribution of data retrieved through a violation of confidentiality”. This offense definition seeks to resolve problems of proof when confidential information is passed through the internet and it is not clear whether the person who distributed it was also responsible for illegally obtaining the information.42

The virtual world of cyber space certainly is distinct from the real world, but there are passages between the two, and persons can be affected by the loss of “cyber goods” as much as by losing tangible property.43 This fact raises the question whether laws against theft and fraud, which primarily concern goods and property of the “real” world, can also be applied to the cyber world. In a recent Dutch case, a boy had, by investing much time and effort, acquired an amulet and a sword in an online role play game. The perpetrators forced the boy by threats (in real life) to transfer the sword and the amulet to them (in the cyber game). The Dutch Supreme Court confirmed their conviction of theft, but this result was based on a broad interpretation of the term “goods”,44 which may not be applicable in other jurisdictions. A Finnish appeals court, for example, in a very similar case did not accept such a broad reading of the theft offense and came to the conclusion that

40 B 7.
41 E 3.
42 NL 6-7.
43 See SNW 16-17.
44 For a discussion of this case, see NL 7-9.
the unauthorized acquisition of virtual “hotel furniture” was not punishable.  

These cases show that legislatures may need to consider the introduction of specific provisions punishing “cyber theft” where the objects unlawfully acquired by the perpetrator are not tangible “things” but images which are of value (only) in the cyber world.  

The usurpation of a person’s virtual identity that he uses for communication on the web affects a more “real” dimension; it is often – but not necessarily – connected with attempts to defraud in real commerce. For example, a perpetrator may illegally acquire the victim’s access data and order goods from an internet store, leaving payment of the bill to the victim. Some legal systems do not (yet) have specific criminal laws covering this type of fraudulent behavior, whereas others have rather broad offense definitions. Under French law, for example, it is a crime to illegally adopt the identity of another person or to use data making it possible to identify him – including his IP address or his nickname in a social network – in order to disturb his or someone else’s calm or to attack his honor or reputation. Similar provisions can be found in a few states of the U.S. U.S. Federal law as well as Canadian law provide for the punishability of illegally acquiring or using someone else’s “means of identification” with the intent to thereby commit an unlawful act. In other legal systems, courts have applied the offense definitions of computer forgery, fraud by false representation, wrongful impersonation of another person, defamation, or dissemination of information violating personal privacy to such cases. The method of getting access to

---

45 SF 10-11.  
46 See also SNW 18.  
47 For the enormous incidence of “identity fraud” see the figures given in SNW 2.  
48 For various definitions of identity fraud and identity theft, see SNW 3-4.  
49 See, for example, A 6, D7, E 3, J 4 (but it is a criminal offense in Japan to sneak into a protected social network by using a false identity; J 11), NL 10 (but the Netherlands have a broad concept of the crime “deception to gain benefit”, which may cover some of the cases in question), TR 3 (but Turkey has criminal offenses of illegally obtaining, giving or disseminating personal data and of obtaining illegal benefit through the abuse of ITC systems).  
50 F 4. This provision is said to also cover the intent of doing material harm, for example, by ordering goods using the victim’s cyber identity. Poland has a very similar provision; P 4; and a draft law to the same effect has been proposed in Argentina; AR 14.  
51 SNW 10.  
52 Cited in SNW 9, 11. See also a draft law in Argentina to the same effect; SNW 12.  
53 See B 9.  
54 SNW 15 (concerning England).  
55 SNW 15-16 (concerning India, Italy and Poland).  
56 SF 10-11.
someone else’s identity on the web can, of course, by itself be criminal, e.g., hacking or interfering with the integrity of an ICT system.\textsuperscript{57}

Given the great importance of the reputation and integrity of cyber personalities especially in social networks, legislatures may well see a need to criminalize the usurpation or falsification of a person’s virtual identity even where the perpetrator does not intend to cause material harm. Voicing certain opinions, placing ads or disseminating fake information under another person’s cyber identity may do serious damage to that person’s “good name” in the cyber world\textsuperscript{58} and may thus be regarded as even more harmful than the loss of some money through fake orders from an online store.\textsuperscript{59} It may, however, be difficult to properly define the gist of the crime without interfering with internet anonymity in general.\textsuperscript{60}

(C) \textbf{Actus Reus and Mens Rea of ICT and Cyber Crime Offenses}

Given the novelty of ICT and cyber crime, it is of interest to observe how legislatures cope with the task of defining such offenses. Are there characteristics typical of new offense definitions in the areas of ICT and cyber crime?

(1) \textbf{Definition of actus reus}

Traditional crimes, such as murder, causing bodily harm, or fraud, are often defined in such a way that the causation of a certain harmful effect is part of the \textit{actus reus}. With respect to ICT and cyber crime, this seems to be the exception rather than the rule; in most cases, doing a certain act has been made criminal, regardless of the consequences the act may or may not have caused to the protected interest. For example, obtaining access to a protected ICT network or the transmission of pornographic images via the net are defined as offenses.\textsuperscript{61} These acts certainly have some “result” aspect – for example, a person who tries to distribute pornographic images but fails to get access to the internet from his laptop has not “transmitted” the images.\textsuperscript{62} But the harm that the legislature wishes to protect against – the violation of confidentiality of certain information in the case of hacking, the stimulation of the market in child pornography – need not occur in order to make the perpetrator punishable for the completed offense. The majority of ICT and cyber crimes can thus be categorized as offenses of

\textsuperscript{57} SNW 13-14.  
\textsuperscript{58} See SNW 7.  
\textsuperscript{59} In a case decided in Finland, the perpetrator had placed an online advertisement under the (cyber) name of a 12 year old boy allegedly looking for sex with another boy; SF 10-11.  
\textsuperscript{60} Cf. NL 10, SNW 19.  
\textsuperscript{61} See, for example, F 5, PL 5-6.  
\textsuperscript{62} For that reason, the Spanish national report maintains that most ICT offenses are “result” crimes; E 4. But this applies only if one uses the term “result” in an empirical sense: getting access to a protected ICT system then is the “result” of the perpetrator’s activity with the intention to get such access.
("abstract") endangerment. Only a minority of crime definitions require an actual disturbance of an ICT system for conviction. Often, actually causing the harm that the criminal prohibition is designed to avert – e.g., damaging data through interfering with an ICT system – is treated as an aggravating circumstance in sentencing.

Most ICT and cyber crimes can be committed by any person, but a position of special responsibility can lead to an enhanced sentence. For example, in Greece a person who violates data secrecy can be punished more severely if he is a provider of telecommunication services or his legal representative or a responsible for the safeguarding of the secrecy.

(2) Definition of mens rea

The great majority of typical ICT and cyber offenses require intention on the part of the perpetrator. This includes, in many legal systems, the variant of dolus eventualis, that is, the conscious and voluntary taking of a risk that the prohibited act or result occurs. But several legal systems also provide for negligent offenses. Typically, negligence suffices with respect to doing harm to data or an ICT system after having illegally (and intentionally) gained access to it. Under Dutch law, professionals (but not normal users) are punishable for negligently distributing malware. The violation of data protection laws and the possession of devices for secretly collecting information can also be committed by negligence under French law, and in Italy the omission to adopt measures for securing privacy can be committed negligently. But these isolated provisions appear to be exceptions from the general rule that violations of ICT and cyber laws can be punished only where the perpetrator has acted intentionally.

---

63 See TR 4.
64 See A 8, PL 6, RO 3. In Italy, any act meant to destroy "information, programs or computer data used by the State or other public body or computer data that have public utility" has been criminalized; IT 9.
65 See B 11, IT 2.
66 See BR 9, D 9, J 5, RO 4.
67 See BR 9, D 9, J 5, RO 4.
68 Cf. I 5, J 5, SF 2. However, with regard to possession of child pornography Austrian law requires at least knowledge on the part of the perpetrator that the file he views or downloads contains pornographic images; A 9.
69 See B 12, TR 5; see also PL 6.
70 NL 27; see also AR 7 for the crime of negligent destruction of official records.
71 F 6-7; see also GR 34.
72 IT 5.
(D) Extent of criminalisation: Preparation and Possession

(1) Preparation

The somewhat elusive character of ICT and cyber crime, which can generate problems of proof of actual harm or endangering, seems to have led to a widespread legislative practice of incriminating acts in preparation of the harmful conduct itself, including the mere possession of devices or software that can be used for attacks on the integrity of ICT systems. This is exceptional in that most legal systems do not generally regard the mere preparation of criminal conduct as worthy of punishment, except with respect to very serious crime or to conspiracies of two or more persons. But in the area of ICT and cyber crime, many legal systems have followed the demand of Article 6 of the Cybercrime Convention to criminalize the production, sale, procurement for use, import, distribution or otherwise making available of devices, including computer programs, designed or adapted primarily for the purpose of committing any of the ICT offenses listed in the Convention, as well as of computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of these offenses.

Several legal systems have copied almost verbatim this broad definition of preparatory acts from the Cybercrime Convention. Typical examples of preparatory acts along these lines are “phishing” of web addresses or other personal data (e.g., bank account and credit card numbers, passwords) that can be used in order to defraud persons or to do other harm to their interests on the net. The same applies to the production or sale of devices or software that can be used for hacking, for intercepting communications or for circumventing the protection of copyrighted material. In Japan, a similar provision relates to information on electromagnetic records encoded in credit or payment cards. Austrian law makes punishable only the sale or possession of software that has been specifically designed or adapted for committing punishable acts; but legal writers have criticized this restriction as too narrow and would only demand that

---

73 Cf. NL 18.
74 See B 24, BR 10 (Brazilian draft law), IT 3, NL 19, RO 5-6, SF 15; see also SNW 4-5.
75 See, e.g., D 7, IT 4, 6-7, J 8-9. Italian and Polish law extend punishability to the production, acquisition, sale or making accessible to other persons computer passwords, access codes or any other data enabling someone to gain access to an information system protected by security measures; IT 8, PL 8.
76 A 6 (requiring a commercial intent), B 24, D 7, HU 8, J 6-7.
77 B 24.
78 B 25, E 7, F 8, TR 8.
79 J 7.
the software in question should be “apt” for being used in committing crimes. Another limitation is the requirement that the perpetrator act with the intention of committing an ICT or Cyber crime, which excludes computer security experts from the reach of the criminal prohibition.

A special form of preparatory conduct that has been criminalized in some legal systems is the “grooming” of children, that is, making contact with them by using the internet, with the intent of subsequent sexual abuse or of producing child pornography.

The extension of criminal responsibility to preparatory acts, in the wake of the Cybercrime Convention, seems not to have met with much opposition, except that in Spain the equality of penalties for preparation and for the complete ICT crime was criticised.

(2) Possession

Criminalization extends not only to those who produce or distribute devices or software that are suitable to be used for committing ICT or cyber crimes, but in many legal systems also covers the mere possession of such tools, including those that are to be used for intercepting communication. An exception is Greece, where the legislature has so far decided against introducing criminality of the mere possession of electronic tools that can be used for hacking.

With regard to child pornography, the mere possession of certain materials, also in the form of data files, is frequently defined as a criminal offense. Whereas there exists a broad consensus that the storing of such materials in one’s computer is a crime, because the sale and acquisition of child pornography perpetuates the illicit market of such materials and thereby promotes the abuse of children, opinions are divided as to whether “possession” extends (or should extend) to the mere viewing of pornographic material on the net. Some states

---

80 A 10-11. For a similar provision, see RO 5.
81 A 11.
82 NL 20.
83 NL 21.
84 E 7. See also the criticism in IT 8.
85 See, e.g., A 12, B 24-26; HU 8, IT 8-9, RO 6.
86 For a statement of the reasons and of reform proposals, see GR 44-50.
87 Polish law extends the prohibition to possessing data propagating fascist or other totalitarian regimes as well as data inciting to hatred for national, ethnic, racial, religious reasons; PL 8-9. Turkish law extends the prohibition to pornography involving violence, animals, dead human bodies or “unnatural” sexual behavior (which may include fetishism and homosexuality); TR 9.
88 See B 27.
include the act of knowingly acquiring access to child-pornographic materials on the internet in the criminal prohibition, whereas others require some sort of permanent possession. Another contentious issue concerns the question whether the prohibition only extends to “real” images of children in sexual poses or activities or also covers virtual images, e.g., computer-generated drawings or illustrations.

(3) Responsibility of Providers

Many criminal offenses can be committed by posting certain information, images, or statements in the internet. Libel and defamation, incitement to racial hatred, fraud, violations of copyright and pornography laws are the most common types of such crimes. For technical reasons, their commission is not possible without the activity of internet service providers (ISP) of various kinds, who serve as intermediaries between those who wish to post information and those who receive it. To what extent may ISP be made criminally responsible? Legal systems have given different answers to this question, but the trend goes toward limiting punishability to situations in which a provider has been made aware of criminal contents on a site under his care and does not take appropriate action.

The first question concerns the kind of potential criminal responsibility of ISP under general rules of criminal law. ISP may be qualified as aiders and abettors to any criminal offense committed by posting illicit information on sites they host or give access to, and they may be criminally liable for an omission to interfere (e.g., remove objectionable content from their site) and thus (hypothetically) cause a result incriminated by the law. But the latter concept raises the question on what legal grounds there may exist a duty to act for ISP, and whether a responsibility for omission can be recognized at all when the offense definition does not require a result but (only) the performance of certain acts. Both accessorial liability and responsibility for omission require knowledge of the existence of the objectionable information on the website provided by the ISP in question. In legal systems that

---

89 This applies, e.g., to Austria (A 11), Finland (SF 8) and Germany (D 13-14).
90 See B 26-27, arguing that a mere viewer does not “knowingly” possess pornographic materials although they are temporarily stored in the RAM of his computer; see also E 8, F9, GR 50-53, IT 10, RO 6, PL 9.
91 This is the approach, for example, of Belgian, Greek and Italian law; B 27, GR 18-21, IT 4.
92 For an extensive discussion of this issue, see GR 54-59. An Italian high court found an ISP criminally liable for aiding and abetting, by omission, a privacy violation committed by one of its users, because it had not specifically informed users of their obligations concerning sensitive data as provided by statute. But since this duty applies only to the area of data privacy, this judgment cannot be transferred to other areas of the law; IT 10-11.
93 For brief discussions of these problems, see A 12-14, NL 26, TR 10.
have no special rules on responsibility of ISP, their lack of knowledge normally precludes any criminal liability on their part, because, as the national report from Japan puts it, "service providers and so on are not required to perform continual surveillance of uploading illegal information". 94

Many European legal systems have adapted their laws to the model established by the EU E-Commerce Directive of 2000. 95 The Directive provides that Member States shall not impose a general obligation on ISP – including access providers, caching providers and hosts of websites 96 – "to monitor the information which they transmit or store, nor [sic - or] a general obligation actively to seek facts or circumstances indicating illegal activity". 97 The Directive sought to prevent proactive censoring and the ensuing chilling effects on the free flow of information. 98 But this privilege for ISP, which normally excludes criminal liability for providers, has been limited in various ways.

First, providers lose the protection of the privilege as soon as they go beyond serving as a mere conduit or providing a cache for cyber communication, for example by initiating transmission of data, selecting the receiver or modifying the information transmitted or stored. 99 Second, ISP can be criminally liable when they have been informed of specific illegal content in their domain and fail to promptly remove it. 100 Such information can derive from official agencies 101 or from users. 102 In France, ISP are obliged to positively invite users to alert them to certain prohibited content, such as child pornography, incitement to violence and assaults on human dignity, and they must promptly remove from their sites contents that are “manifestly illegal” 103.

94 J 9. For similar statements, see HU 8, RO 6.
96 The Turkish national report correctly points out that in Web 2.0 it may be difficult to distinguish between mere hosts and content providers; TR 11.
97 Article 15 (1) Directive 2000/31/EC.
98 NL 23; see also the jurisprudence of the European Court of Justice cited in IT 11.
100 A 13-14, BR 10, D 18, F 12-13, PL 10, TR 9-10. For practical examples of criminal convictions on this basis, see E 8, NL 25.
101 In the Netherlands, the public prosecutor can order ISP to render illegal content inaccessible; NL 23.
102 E 9.
103 See F 9-10. The Finnish national report (SF 13) states that the operator can be held responsible for illegal and racist material if he “doesn't on its own initiative remove clearly illegal material”. It is not quite clear whether this obligation requires the ISP to actively...
The ISP privilege does not apply to persons who set hyperlinks to other websites. Generally, a person who links his website to another one is considered to have provided the content of the other website. But conscious setting of links should be distinguished from merely listing websites, as is routinely done by search engines.

Generally, the law in many states appears to leave sufficient freedom for ISP of various sorts and avoids making them responsible for contents they cannot control and cannot even know about. One may consider, however, to what extent ISP should be encouraged to become proactive in gathering information about certain offensive materials.

(E) Specific Sanctions

In addition to imprisonment and fines, some legal systems provide for sanctions that are specific to the offenses discussed here. Offensive devices can be confiscated. More specifically, in Belgium the prosecutor may use all technical means to make data inaccessible if these data "are the subject of the offence or have been produced by the offence and if they are contrary to public order or good morals or constitute a danger to the integrity of computer systems or data stored, processed or transmitted through such system". Using that power, prosecutors may order an internet service provider to delete the domain name of a site that violates the law, e.g., by distributing child pornography. In France, the court may, as an additional sanction for violating a copyright, ban the offender from using online communications for up to one year. A similar sanction can be imposed under Turkish law as an alternative to a prison sentence of up to one year.

The general principle that sanctions should not be disproportionate to the seriousness of the crime bears emphasis here. In some states, legislatures tend to overreact to the threat of ICT and cyber crime by providing for excessively high sentences for these new crimes.

(F) Challenges to and Limits of Criminal Legislation

Legislatures that approach the task of defining ICT and cyber crime offenses often face specific problems. They find themselves in a dilemma: they should define the relevant criminal act in such a way that the provision does not become

---

104 Cf. NL 26, TR 9.
105 See A 14.
106 B 33.
107 F 8, 16.
108 TR 11.
109 Cf. GR 60.
obsolete whenever new technologies, new hardware devices or just new terms of art are invented and enter the market; on the other hand, legislatures need to respect the principle of legality which demands that criminal statutes are precise and explain in clear terminology exactly what conduct is prohibited. A related policy concern is the risk that overbroad criminal statutes may discourage individuals, who fear criminal liability, from making use of the opportunities that ICT and cyber space offer. In the background, there are concerns that criminal prohibitions in the area of ICT and cyber space may interfere with important civil rights and freedoms.

(1) Keeping in Line with Technological Progress

In view of the risk that technological and terminological developments may quickly make the wording of a criminal statute obsolete, some legislatures try to keep abreast of the latest progress; for example, a French criminal statute refers to transfer of data to “le nuage Internet”. 110 Other legislatures strive to use non-technical, generic language, refer generally to civil or administrative law, or employ express legal fictions. For example, in the German Penal Code “writings” are defined as comprising – among other objects – data storage devices, images and other representations. 112 This extension nevertheless leaves loopholes with respect to pornography since it arguably fails to cover streaming videos. 113 The Argentinian legislature has tackled the problem head-on; one criminal statute refers to certain technologies and adds the words “o la tecnología que en el futuro la remplace”. 114

(2) Respecting the Principle of Legality

The Argentinian approach clearly is at odds with the ideal of precision in criminal prohibitions; but so is the use of broad generic terms such as “interference” as a description of criminal conduct, 115 and even the terms “data”, “information system” and “interception” may be vague unless given a specific definition by law. 116 Legal systems differ with respect to their sensitivity to this issue, which typically plagues legislatures attempting to deal with multifaceted and fast-changing phenomena such as ICT and cyber crime. Where a legislature avoids overbroad formulations

110 F 8.
111 [T 7.
112 § 11 sec. 3 German Penal Code. See also B 18-19 (discussing the use of the generic term “système informatique” in Belgian law).
113 D 12.
114 AR 8. For a similar formulation (“comparable to those in any other way”), see SF 1, 12.
115 See NL 6, 16. Other examples are the wide-open statutory “definitions” concerning child pornography in Brazilian law (BR 7); see further RO 4, TR 6-7 (discussing the terms “personal data” and “communications”).
116 Cf. GR 31-32, 35-36, 38.
of the prohibited conduct, sometimes the courts feel compelled to extend existing narrow provisions by analogy in order to adapt them to a changing world. In that vein, Dutch courts have interpreted the term “goods” in theft law as also comprising data\(^{117}\) - an approach which is at risk of conflicting with the “literal interpretation” branch of the principle of legality.

If criminal prohibitions are defined in broad, vague terms or are expanded beyond the natural meaning of their words by the courts,\(^{118}\) they may deter individuals from making use of the rights that criminal provisions are meant only to limit. In order to avoid that chilling effect of criminal laws, the Italian and the Japanese legislatures have limited certain offenses to acts that are done “without justifiable grounds”,\(^{119}\) Greece has limited some offenses to acts done “without right”,\(^{120}\) and in Spain certain conduct is punishable only where serious harm results from it.\(^{121}\) Requiring (specific) intent may also be a measure to avoid deterrence overkill.\(^{122}\) The introduction of prosecutorial discretion not to prosecute\(^{123}\) is, however, not very likely to resolve the problem as long as the individual cannot determine in advance whether the prosecutor will actually refrain from prosecution in his case. It would be preferable to circumscribe as narrowly as possible the conduct that is prohibited; if relevant technology changes, the legislature may adapt the wording of the statute to the new situation.

(3) Respecting Constitutional Limits

Any criminalization of communicating in cyber space is in latent conflict with the freedom of expressing one’s opinion,\(^{124}\) protected in the constitutions of most countries, and may also involve the freedom of the press\(^{125}\) and the freedom of art.\(^{126}\) Infringements of these liberties are permissible only to the extent that they are proportionate to the evil they seek to combat.\(^{127}\) Some legal systems have also enshrined in their constitutions the “harm principle”, which limits the reach of the criminal law to conduct causing harm or imminent danger to an interest worthy

---

\(^{117}\) NL 6; see also, on the same issue, B 13, GR 6-8, and further IT 11, J 6.

\(^{118}\) Another example of an over-restrictive reaction to perceived dangers is the former practice in Turkey to block access to whole domains after one objectionable file has been found there; see TR 7.

\(^{119}\) IT 7, J 6-7.

\(^{120}\) For an analysis of this term and a criticism of its vagueness see GR 41-43.

\(^{121}\) E 6.

\(^{122}\) See D 11, IT 7, 9.

\(^{123}\) See B 18.

\(^{124}\) See GR 64-65.

\(^{125}\) See, e.g., AR 10-11, BR 11-12, D 19, E 10, GR 63-65, J 10, PL 11, TR 10.

\(^{126}\) GR 62-63.

\(^{127}\) See the jurisprudence of the French Conseil constitutionnel with regard to combating copyright violations; F 15.
of protection. In these countries, it may be argued that some ICT offenses, e.g., hacking without further detrimental effects, violate this principle. The criminalization of the mere possession of tools that can be used for hacking may also jeopardize the freedom of research.

The actual application of criminal laws against ICT and cyber crime may violate the principle of culpability, namely when courts try to avoid problems of proof by convicting persons whose IP number was identified as one from which certain offensive data were entered into the system but without proof that they intentionally committed or supported the actual offense. Whereas such unfair application of criminal laws is not specific to ICT and cyber crime, certain criminal prohibitions concerning communications in the internet typically conflict with the freedom of expression. Legislatures should be aware of this potential conflict and should respect the free market of communication that cyber space provides.

(G) Alternatives to Criminalisation

According to the ultima ratio principle, criminal law should be employed only as a last resort for dealing with a social problem. Nevertheless, several national reports have noted that legislatures in their legal systems seem to regard criminal laws as the primary means of combating ICT and cyber crime.

There exist both administrative and civil mechanisms to deal with the phenomenon of ICT and cyber crime.

(1) Administrative Measures

An important tool for administrative agencies is to order the removal of certain content or to “close down” offensive websites. In various states, this possibility exists, for example, with respect to websites displaying child pornography: an administrative agency may order the access provider to block access to the website in question. These orders are addressed to domestic access providers but effectively also cover access to websites operated abroad. In Japan, a private company is in charge of filtering and blocking harmful websites, and in the

128 Cf. TR 10.
129 See GR 61.
130 Cf. TR 10.
131 See E 11, PL 11, RO 7, TR 11. The actual number of convictions for such crimes does not seem to be exceedingly high; according to the Austrian national report, convictions of computer crime – with the exception of child pornography – in 2007 were in the one-digit range; A 15.
132 F 17, IT 14, RO 7, SF 13, TR 12; see also HU 9. In Belgium, the Brussels investigative judge may order providers to block their services whenever he thinks that there exists a danger for public health, public safety, national security, national defence or consumer interest; B 32-33.
133 J 11.
Netherlands the private ISP sector has agreed to close down offensive sites upon complaints made by users.\textsuperscript{134} But in some countries there is strong opposition against such laws and practices because of the fear that they may open the door to censorship of the internet. For example, in Germany and Poland laws providing for the establishment of a list of pornographic websites to be blocked met with so much criticism that the respective laws never went into effect.\textsuperscript{135}

\textbf{(2) Civil Remedies}

In many legal systems, individual victims can sue for damages incurred through illicit activity on the net.\textsuperscript{136} Yet it seems that this avenue is difficult and cumbersome for private victims and hence seldom used,\textsuperscript{137} with the sole exception of violations of copyright.\textsuperscript{138} One interesting alternative to the official court process exists in the Netherlands, where the private ISP sector has established a Notice-and-Take-Down procedure: When a person or an institution encounters illicit activity or information on a website, he can report this to the service provider. The complaint is then sent to the customer. If there is no satisfactory reply, the ISP may take down the site or remove the offensive information.\textsuperscript{139} A similar system of self-regulation exists in Hungary, but there it is the Association of Hungarian Content Providers that may remove illicit content or even impose a temporary ban on members who violate the rules.\textsuperscript{140}

\textbf{(3) Limiting Anonymity of Users}

An indirect way of obviating ICT and especially cyber crime is to limit the anonymity of users, because the cloak of anonymity encourages individuals to place or receive illicit contents, thinking they do not have to fear detection. If users were made to move in the net using their real name and/or disclosing identifying data, the lure of cyber crime might be significantly reduced. On the other hand it is part of the attraction of the cyber world that persons can change identities and play with them; removing that freedom would certainly have a grave impact on what is conceived of as the freedom of the net.

\textsuperscript{134} NL 31.
\textsuperscript{135} D 20, PL 12-13. Similarly, in Greece the constitutionally protected right of participation in information society is said to prevent any general blocking of access to websites; GR 68.
\textsuperscript{136} See, e.g., A 15, BR 12, GR 67, IT 13 (pointing out that civil liability only requires negligence whereas proof of intent is needed in parallel criminal cases).
\textsuperscript{137} See F 16, PL 11. In Turkey, private parties can sue for removal of content and for having a reply published; TR 11.
\textsuperscript{138} D 19, NL 29. In Greece, a wronged copyright holder may demand that access to the offending website is blocked by the relevant ISP; GR 67-68.
\textsuperscript{139} NL 30.
\textsuperscript{140} HU 10. Hungary also has a National Cyber-Security Center that coordinates responses to serious IT security breaches against government networks and critical information infrastructures.
A middle road might be to either require users to register with access providers, disclosing their true identity, or to require access providers to store data (such as IP numbers) that make subsequent identification of individual users possible whenever a suspicion of criminal wrongdoing on the net arises. Finally, one might consider a prohibition of encrypting files, or at least an obligation of users to divulge passwords and encryption codes for the purpose of a criminal investigation.

(a) Registration of Users
To the extent that internet access is only provided for a fee, access providers normally have contractual relations with individuals who use their services. But such contracts do not require a reliable establishment of the user’s true identity, especially when prepaid access devices are being used.141 Moreover, the fact that a person has a service contract with an access provider does not prove that the individual has used that provider’s services at a given point in time. Therefore, registration of users has little impact on the facilitation of the investigation of (and, consequently, enhanced deterrence from) cyber crime.

(b) Storing Access Data
A more reliable method of connecting individual users to certain activities on the net (for example, placing offensive content on a website or viewing a website with such content) is to register and store IP numbers. With the help of IP numbers and the respective addresses, it is possible to trace activities on the net back to individual ICT devices, such as computers or mobile phones.

National laws differ with respect to whether they oblige access providers to temporarily store IP numbers. In Japan, no such storage is required, and hence subsequent control of an individual’s internet usage is only possible if the provider has recorded and stored the relevant data for business purposes.142 The situation is similar in Germany, since a law providing for automatic storage of IP numbers has been ruled unconstitutional and the governing parties have not yet been able to agree on a successor statute.143 But the great majority of states have imposed a legal obligation on access providers to store individualized access data for periods between three months and two years.144 Providers are obliged to furnish these data to law enforcement agencies and courts when requested to do so in

141 Cf. D 18, F 19, GR 74, PL 15, SF 16.
142 J 12.
143 Cf. D 21.
144 See A 17 (6 months), B 19 (one year), BR 11 (one year), F 10, 13-14 (one year; in France, this obligation extends to owners of cyber cafés and even private employers who offer their employees access to the internet; F 18), HU 11 (one year), IT 15-16 (one year, and two years for telephone traffic data), PL 15 (2 years), RO 8 (6 months), SF 15-16 (3 months), TR 9 (one year).
the context of a criminal investigation. These laws constitute an exception to
the general principle of the secrecy of telecommunications, which precludes
providers from disclosing data concerning connections made or attempted by
their customers. By enacting laws on the mandatory storage of access data,
EU member states have fulfilled their obligation under EU Directive 2006/24/CE
of 2006.

(c) Limiting Encryption of Files

Encryption of files as such is not prohibited in any of the participating states. Most
legal systems also accept the impediment to criminal investigations that
encryption of files causes; coercing a suspect to disclose his passwords or to de-
encrypt his files would be regarded, in these states, as a violation of the principle
that no one may be forced to incriminate himself. But there are states that
permit law enforcement agencies to enlist the help of experts and of ISP to
de-encrypt files if needed for a criminal investigation. French law goes even
further. Not only does it regard encryption of a document as an aggravating
circumstance when the document has been used in order to commit or facilitate
the commission a crime; under French law it is a criminal offense for a person
to refuse to disclose to judicial authorities the secret code – known to him – of an
encrypted document that had been used in preparing for, facilitating or committing
a criminal offense, or that could be used to prevent the commission of a crime.
It is not clear whether this offense of refusing to provide a secret code may also
be committed by the defendant in a criminal case, if he would indirectly
incriminate himself by providing the secret code.

(4) Shifting the Burden of Protection to Users

Some offenses in the ICT and cyber spheres could easily be prevented by proper
cautions on the part of the persons who become victims of these offenses, in
particular by using anti-virus software and by protecting one’s own computer and
one’s access to the internet and to particular websites by using safe passwords.
This raises the question whether the burden of preventing ICT and cyber crime
may be shifted to the user, making him responsible for protecting his own

---

145 A 17, B 29-30, E 11, F 18, GR 73, HU 11, PL 15, RO 6, SF 16.
146 Cf. PL 14.
147 EU Directive of 15 March 2006 on the retention of data generated or processed in
connection with the provision of publicly available electronic communications services or of
public communications networks.
148 See AR 12, A 18, D 21, E 11, GR 75, J 12, RO 9, SF 16, TR 13.
149 B 34.
150 PL 16.
151 F 6.
152 F 20.
interests rather than imposing penalties on the perpetrator of crimes that would have been easy to prevent.

Several states encourage users to employ the possibilities of self-protection. 153 Only few states, however, go so far as to make it a crime not to use appropriate protection and thereby to make possible not only one’s own victimization but also the use of one’s ICT device for the distribution of malware to others or for other violations of the law. 154

On the other hand, the carelessness of the victim with regard to web security does not provide a general defence for defendants accused of ICT and cyber crime. In some legal systems, hacking or interfering with someone else’s ICT system is punishable regardless of whether it was protected. 155 But in other states, offenses involving illegal access to ICT systems are defined in such a way that they cannot be committed unless there had been some protection in place that the offender managed to circumvent, 156 and that solution might better harmonize with the principle that criminal law should be the ultima ratio in protecting legal interests. 157

(H) Aspects of Internationalization

Cyber crime, almost by definition, transcends national borders. This fact raises issues of jurisdiction and of the application of national laws to transnational conduct. It also makes international cooperation in combating cyber crime a necessity.

(1) Jurisdiction

Most states exercise their jurisdiction and apply their criminal laws to any offense that has been committed on their territory. This applies to cyber crime whenever the perpetrator acts (e.g., uses a device for illegally getting access to an ICT

153 See, e.g., B 33.
154 This is the case in Austria; but the national reporter regards it as unlikely that an administrative fine for violating the obligation of using reasonable protection for telecommunication installations would ever be imposed on a private user; A 16. In France, an internet user who fails to protect his access from unauthorized use by others, after having been warned by the proper authority to do so, commits an infraction if a violation of copyright occurs using his internet access; F 17-18. In Italy, it is punishable not to adopt security measures for the protection of privacy as prescribed by law; IT 5. In Turkey, “mass use providers” of internet access (such as internet cafés) are required to deploy and use filtering tools to block access to illegal internet content; TR 12.
155 See A 16, RO 8, TR 13. In Greece, a defendant accused of illegally accessing an unprotected website may, however, claim an exculpatory mistake of fact or law concerning the consent of the owner; GR 69.
156 See, e.g., D 20 (§ 202a German Penal Code on data espionage), E 11, HU 10, IT 14, PL 13.
157 Cf. GR 70.
network) on the territory of the state in question. States also exercise their jurisdiction if the perpetrator acts abroad but the effect, as required by the applicable offense definition, occurs on the state’s territory. Views differ as to what “effect” means in the context of cyber crime. In some legal systems, the mere fact that a website with criminal content can be viewed in a state is regarded as sufficient grounds for that state’s jurisdiction; others require more direct “harm” occurring in that state, such as the loss of property by a person residing in the state, or the interference with a computer system located on state territory.

With respect to acts performed abroad, some states extend their jurisdiction to these acts if the perpetrator had the forum state’s citizenship and the act was punishable both in the forum state and where it was performed. The Cybercrime Convention indeed requires application of states’ jurisdiction in this situation.

Another recognized basis for jurisdiction is the fact that the offense committed abroad has negatively affected the state that claims jurisdiction, or one of its citizens. In the latter situation, there is normally a requirement of “double criminality”, that is, the act must be punishable where it was committed and in the forum state.

It may be advisable to define rules on jurisdiction that take account of the “non-tangible” quality of certain cyber offenses and therefore to abandon the traditional connection of jurisdiction to “territory”. On the other hand, one should avoid creating a system of universal jurisdiction for all types of cyber crime by assuming that such crimes are committed wherever offending websites can be viewed.

(2) International Harmonization

Almost all national reporters have mentioned the important influence that certain international legal instruments have had on the relevant legislation of their states. The greatest common denominator is the Cybercrime Convention of 2001, which has had an impact on legislation even in those states that have not ratified it. In the European Union and even beyond, the EU Framework Decision 2005/222/JHA on attacks against information systems has had a similarly

158 See, e.g., A 18, BR 13, §§ 3, 9 (1) German Penal Code, IT 16, RO 9.
159 See D 21-22, TR 13-14.
160 See A 18, SF 16.
161 See, e.g., § 7 (2) German Penal Code, J 13, NL 32.
162 Article 21 (1) (d) Cybercrime Convention.
163 See, e.g., § 7 (1) German Penal Code, PL 16. No requirement of “double criminality” exists in Turkey (T 14), and it does not apply to all offenses in the Netherlands (NL 32).
164 Accord, GR 76-77.
165 See AR 13, BR 13, GR 78-79, IT 17, TR 15.
166 See TR 14.
important influence on national legislation. The EU Data Retention Directive 2006/24/CE has likewise been implemented by most member states. Further, certain EU instruments concerning the combat of individual crimes, such as the Framework Decision 2005/222/JHA on the sexual exploitation of children and child pornography, have been of relevance, because some of the crimes to which these directives relate are typically committed by using the internet. The representatives of many states continue to actively work together in order to adapt harmonized legislation to the latest developments in ICT and cyber space.

(I) Trends for the Future
A host of ideas about trends for the future in ICT and cyber crime and relevant legislation have been mentioned by national reporters. Some of these ideas are:

- a need to lower intent requirements, thus enabling courts to overcome otherwise insurmountable problems of proof;

- an interest in reconciling the interests of copyright holders and of users with respect to inexpensive access to protected music;

- the need to criminalize new modes of harmful conduct such as cyberbullying, cyberstalking, identity theft, spamming, and illegal acquisition and distribution of data;

- the necessity to protect information and network systems as a whole against theft and other offenses;

- the question whether criminal liability of ISP should be expanded;

- the need for a systematic and extensive legislation on cyber crime.

The national reporter from the Netherlands observed that at the moment the balance sways to more supervision and control and that it is hard to predict when the scales will return to the free flow of information as a basic principle of the rule of law. The upcoming AIDP Congress may help to bring about a return to the ideal of the freedom of the internet and to cut back on efforts of some states to gain excessive control over cyber space by overextending the criminal law.

\[\text{References:}\]

167 Cf. PL 17.
168 A 20.
169 FR 21.
170 AR 14-15, E 12, SF 20.
171 J 14, SF 20.
172 IT 17.
173 BR 15.
174 NL 32.