Section 2: Concept paper and questionnaire

Emilio C. Viano

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

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

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Emilio C. Viano: emilio.viano@gmail.com

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).
(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?
(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?
(2) Are there also negligent offenses in this field?
(3) If yes, please, provide a list of those offenses.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission
a. Object – system or data?
Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?
b. Requirement of infringement of security measures?
Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

2. Data and system interference
a. Object – protection of system/hardware/data?
Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.
b. Act – destruction/alteration/rendering inaccessible?
i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?
ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under *a*?

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-diallers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data?

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;
- Their disclosure practices;
- Their professional ethical obligations;
- And whether patients or clients have any control over the disclosure of their personal data?

ii. Which data are specifically protected, if any?

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

b. Subject – Type of perpetrators?

Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply *for each category listed below* citing the relevant law and its provisions, if available:

1. Illegal collection
2. Illegal use
3. Illegal retention
4. Illegal transfer

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

ii. In particular, does your criminal law:

- Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:

1. to transmit,
2. make available,
3. export
4. and intentionally access child pornography on the Internet;

- Allow judges to order the deletion of child pornography posted on computer systems in your country;

- Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;

- Criminalize:

1. Knowingly accessing child pornography on the internet
2. Transmitting child pornography on the internet
3. Exporting child pornography on the internet
4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it…?

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

vii. *Mens rea*: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?
2. cyber-bullying?
3. cyber-stalking?
4. cyber-grooming?

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud
2. Infringement of Intellectual Property IP rights
3. Industrial espionage

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?
(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.
(3) Do victimization surveys in your country include questions on cyber-crimes?
(4) What types of computer crime / computer fraud are most often reported in your country?
(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?
(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.
(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?
(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)			
Hacking (illegal intrusion into computer systems; theft of information from computer systems)			
Malicious code (worms, viruses, malware and spyware)			
Illegal interception of computer data			
Online commission of intellectual property crimes			
Online trafficking in child pornography			
Intentional damage to computer systems or data			
Others			

(9) In addition, to the above, if there are there any other forms and means of cyber-crime that have occurred (either frequently or infrequently) in your country, please identify them as well as the frequency with which they occur in the following table:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently

Thank you for your valuable collaboration!

Annex 1

John A.E. Vervaele

(1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society Castells1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

(2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

1. The integrity and functionality of the cyber-ICT system (CIA offences)
2. Protection of privacy
3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, The Coming of Post-Industrial Society, New York, Basic Books , 1976.

Manuel Castells, The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1. Malden: Blackwell. 2d Edition, 2000

S. Sassen, The global city , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, Mastering Complexity in the Global Cyberspace, in M. Delmas-Marty & M Pieth. Les chemins de l'harmonisation Pénale, Paris 2008, 127-202.

Annex 2

The Information Society and Related Crimes

Emilio C. Viano

The modern networked society is highly vulnerable to information-age related deviance and criminal behaviors. Globally, in the past few years, concerns have increased sharply over cyber-security, including the issues of cybercrime or high technology crime, "cyber-war," "cyber-defense," "cyber-terrorism," critical infrastructure protection, and information security. At the same time, growing attention is also being paid to how responses to cyber-security may affect and how they should be balanced with human rights values, such as individual autonomy, privacy, anonymous political speech, freedom of expression and freedom of association, human development goals, including access to knowledge, and economic interests, including innovation, competition, and the protection of trade secrets and other proprietary information. These issues of policy and values also present complex technical issues, such as the issue of "attribution," that is, the extent of the ability to determine the true senders of any message or request for information.

There is no question that the technologies that make the information society possible and functional have become essential tools that have significantly affected various aspects of personal and social lives, ranging from education, business, to cultural and leisure activities. With the widespread use of personal computers and of other electronic devices (iPhone, iPad, iPod, iTunes, etc,) and technology (Skype, Google Earth, etc.) and high speed internet, various related deviant and criminal behaviors have increased significantly, such as hacking, illegal downloading of music and software programs, and stealing others' passwords or identity.

While the accurate extent and overall cost of cyber deviance is unknown and the estimated cost of it actually varies, there is no question that it is now a global and growing phenomenon.

Consequently, cyber-security has become a major concern of governments and the private sector around the world. There seems to have been a major shift in consciousness, stemming from a variety of sources, including:

- Increased appreciation of how critical the Internet and its resources are in multiple spheres of human endeavor and how many infrastructures and systems are increasingly dependent on Internet connectivity and capacity

- Continuing disclosures of major data breaches at financial institutions, other corporations, government agencies and academic institutions globally

- Continuing releases of malware and the increased sophistication of what is deployed

- Continuing reports of varying levels of governmental accessing, monitoring and filtering (or censorship) Internet use and content

- Unattributed cyber-attacks on key infrastructure, e.g. in Lithuania, Estonia, Georgia and other countries and most recently on a nuclear plant and on a munitions base in Iran. Stuxnet and Duqu used against Iran are considered the world's first 'super weapons' for cyber war.

- Concerns with governmental and corporate espionage

- Increased concern over cybercrime, including online fraud, identity theft, child pornography, theft of intellectual property, and related criminal movement of money and money laundering on the Internet

- Privacy concerns about corporate and governmental data access and the widespread collection, recording and diffusion of private information on practically everyone worldwide

As the reach of the information technology and software continues to grow exponentially among the world's population, and given the apparent lack of adequate user awareness on implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of entities. These include criminal enterprises, "hackers" (whether for financial gain or as a challenge), cause-based groups, businesses spying on other businesses, proxies for governments, and governments, including their military and intelligence agencies. Motives for the attacks range from financial gain to the advancement of national security interests to the satisfaction of peer recognition.

Any effort to reach international consensus on cyber-security is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the Internet, of human rights, and of economic policy. Some see cyber-security as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block

any undesirable content. Others strongly believe that Internet governance (including Internet security) involves an integration and balancing of interests, including not only national security but also human rights and the economic and developmental interests associated with a vibrant, innovative and competitive information society. These differing perspectives manifest themselves in many areas. Even the definition of computer crime is debated and contested.

(A) Cybercrime: Terminology and Definition

A cybercrime is a type of crime that involves the abuse of information technology. The term cybercrime covers a series of crimes which range from cyber terrorism to industrial espionage. Some cybercrimes may involve only limited influence of computers and networks while others rely almost entirely on the use of a computer or other electronic device and a network. First, an individual might use a computer or other electronic device to engage in criminal activity. Second, the evidence needed to prove a criminal case might be stored in computerized or electronic form. The law governing use of a computer or electronic device to commit a crime is substantive electronic crime law, because it concerns the scope of substantive conduct that has been criminalized. The law governing the collection of computerized evidence is procedural electronic crime law.

Cybercrime is an extensive phenomenon expressed via an intricate ecosystem of operators, victims and instruments. Over the years, in fact, cybercrime has acquired a hierarchical and international organization, with a genuine “black market” for the commerce of data, tools and skills.
As the instruments have become more streamlined, the expertise required to access the world of cybercrime has been lowered: whereas cybercrimes were once perpetrated by groups of “black hats”, today almost anyone with some technical skills can download and use instruments in order to carry out some type of attacks, from anywhere in the world.
Today’s cybercrimes are characterized by these two aspects: on the one hand, crimes can take numerous different forms in terms of expertise and attacks; on the other hand there is a series of well-structured schemes and mechanisms that typically characterize organizations and markets focused on profit.
Cybercrime refers to any crime that involves a computer or electronic device (iPhone, iPad, tablet, Blackberry, etc.) and a network where a computer or an electronic device may or may not have played an instrumental part in the commission of the crime. Many of the techniques involve the use of a computer/electronic device and of a network. However, many other techniques have nothing to do with computers other than information stored in text files on the computer’s hard drive. Because of the diversity of computer/electronic-related offenses, a narrower definition would be inadequate. The rapid emergence of electronic technologies and software and the exponential expansion of the Internet have spawned a variety of new, technology-specific criminal behaviors that go beyond the category of "computer crimes." The terms “cybercrime” or high technology crime or information and communication technology crime are umbrella names for all crimes involving certain electronic devices and an information and communication network, mostly known today as “the internet.” Debating semantically whether an act is a computer crime versus a cybercrime versus a high technology or an information and communication technology crime is not that important. Gaining a better grasp of the problem and of its criminal law implications and response is more important. To combat these new criminal behaviors, many countries have indeed passed specialized legislation.
Experts have had difficulty calculating the damage caused by computer and electronic crimes due to the difficulty in adequately defining them; victims' reluctance to report incidents for fear of embarrassment, losing customer confidence and diminished competitiveness; and the lack of detection.

(B) Legal Interests Deserving Criminal Law Protection

The major interests identified in this Section II as deserving of the criminal law protection are:

(1) The integrity and functionality of the cyber-Information & Communication Technology (ICT) system (CIA offenses)

Offenses against the confidentiality, integrity, and availability of computer systems (called the “CIA” offenses) constitute the major threat to this primary interest of the ICT system.

(2) Protection of privacy

The term “privacy” is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. Philosophical debates concerning definitions of privacy became prominent in the second half of the twentieth century, and are greatly influenced by the development of privacy protection in the law. Some defend privacy as focusing on control over information about oneself ; others see it as a broader concept required for human dignity or essential for intimacy; others consider it the value that accords us the ability to control the access others have to us. The earliest calls for explicit recognition of privacy protection in law were in large part motivated by the expanding communication technology. It is clear that many people still view privacy is a valuable interest and realize it is now threatened more than ever by technological

advances. There are massive databases and Internet records of all sorts of information about anyone of us, from individual financial and credit history to medical records, to purchases and Internet searches and communications. Most people do not know what information is stored about them or who has access to it. The ability for others to access and link the databases, with few controls on how they use, share, or exploit the information, makes individual control over information about oneself very challenging. The questionnaire for Section II in great part covers the major types of offenses against privacy.

(3) Protection of digital personality

Our Digital Personality is the pool of digital information about each one of us available to anyone with the right access, tools and motivation to find it. In the digitized world, it represents each one of us. Increasingly it is the first impression that we make upon others, and first impressions are important.
This phenomenon has grown almost accidentally. There are now many ways through which businesses and ordinary people are creating, using, sharing and storing increasing amounts of personal information.
Business tools are emerging to link the various parts of our Digital Personality together to create comprehensive views of each one of us.
There has been continuing outrage at this invasion of our personal space.Yet we persist in using new digital technologies and willfully post material on ourselves that create even more information for others to find.
Personal information on the internet and social media generally legally belongs to the businesses that hold it. They can manipulate, use, trade and store endless amounts of our personal information and yet we currently have limited legal rights to challenge this situation.
Additionally, as digital technologies become increasingly pervasive, we find ourselves living within ubiquitous intelligent interactive systems. Interacting with them is a complex and time-consuming task that sometimes is difficult for everyone, even Information Technology specialists, and at times impossible for certain groups of people. Although there are many user-centric approaches to deal with this phenomenon, ironically, it seems that the only unnatural part of the digital environment is the real human being. To solve this problem the creation of a context-based digital personality (DP) is being worked on as a proxy between digital surroundings and the final user. DPs will benefit from mobile technologies for context-creation, maintenance and usage; and from semantic technologies for formal decisions and verifications. The DP is conceived as being an electronic alter ego that exists independently of us, having executive powers and carrying our identity when we deal with the electronic world. Using it should simplify everyday interaction between users and digital environments and provide a framework for implementing value-added services for mobile operators.
Pertinent questions in Section II address the major possible violations and exploitation of our digital personality, how to protect it, and how to rebalance this lopsided equation of power over sensitive information about us.

(4) Protection against illegal content

One could summarize illegal content to be any content, images, code, or software that executes or promotes:
- Malware and malicious code
- Denial-of-service attacks
- Computing viruses
- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare
- Harassment
- Spam, or the unsolicited sending of bulk email for commercial purposes
- Unauthorized access of licensed or protected software, or other intellectual property.
- Drug trafficking
- Terrorism
- Child pornography, child grooming, and some content inappropriate for minors.

Many jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

As a reaction to the actual or potential placement of “illegal” material on the web, government policies concerning censorship of the Internet may be broadly grouped into four categories:

(a) Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies.

In these countries laws of general application apply to illegal Internet content such as child pornography and, in some, incitement to racial hatred.
It is not illegal to make content "unsuitable for minors" available on the Internet, nor must access to it be controlled by a restricted access system. Perhaps all such governments encourage the voluntary use of, and ongoing development of, technologies that enable Internet users to control their own, and their children's, access to content on the Internet (e.g. parental controls).

(b) Criminal law penalties (fines or jail terms) applicable to content providers who make content "unsuitable for minors" available online.
Additionally, in these countries, laws of general application forbid other illegal content, like child pornography.

(c) Government ordered blocking of access to content deemed unsuitable for adults.
Some countries require Internet Service Providers (ISPs) to block material while others only allow restricted access to the Internet through a government controlled access point.

(d) Government prohibition of public access to the Internet.
A number of countries either prohibit general public access to the Internet, or require Internet users to be registered or licensed by a government authority before permitting them restricted access as in (c) above.
In the many countries that have restrictive Internet censorship laws, governmental focus appears to be on prohibiting and/or restricting politically sensitive speech, criticism of the government, etc.
Concerns about access to content on the Internet vary markedly around the world and regulatory policy reflects this. What is illegal in one country is not illegal in others, and what is deemed unsuitable for minors in one country is not in others. However, by and large, child pornography is widely criminalized.

(5) Protection of property (including intellectual property rights)

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.
IP is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs. The innovations and creative expressions of indigenous and local communities are also IP, yet because they are “traditional” they may not be fully protected by existing IP systems. Access to, and equitable benefit-sharing in, genetic resources also raise IP questions.
Information and Communications Technology is also widely used to commit traditional crimes like fraud. In our very competitive business world, industrial espionage is reportedly conducted frequently to unjustly obtain competitive advantages.

(6) Protection against acts committed exclusively in the virtual world

Crimes, as traditionally thought of, are committed in the so-called real world, in our shared physical reality. The conduct used to commit such crimes, the circumstances involved in their commission, and the harms that result from their commission all occur in “real” places like public streets or private residences. Consequently, existing criminal law imposes liability and penalties for conduct that results in inflicting bodily harms, like injury to persons or property or the unauthorized taking of another person’s property. The modern criminal law insists, as a fundamental premise, that liability be predicated upon some conduct—action or inaction in the face of a duty to act—taken in the external, physical world. It fundamentally rejects that liability can be imposed for incorporeal behaviors such as improper or even criminal thoughts.
At the same time, cyberspace exists along with, but distinct from the physical world. It is a shared conceptual reality, a “virtual world,” not a shared physical reality. Since it is not a physical domain, some question whether the current principles of criminal law we employ are adequate to address crimes that exploit the unique advantages of cyberspace. This inadequacy cannot exist unless there are material differences between cybercrimes and “real” crimes as to, for example, the conduct used to commit the offenses that fall into both categories, the circumstances surrounding the commission of the offenses, and the harms that result. Naturally, we should not simply assume that criminal conduct that exploits cyberspace represents an entirely new phenomenon called “cybercrime.” It may simply be perpetrators using cyberspace to engage in conduct that has long been outlawed for a long time. The telephone, the telegraph, radio, television etc. have been used to perpetrate frauds, for example. However, fraud has been a crime for centuries. The same is true of homicide, whether committed with a knife, a club, a firearm or poison.
Can there be truly virtual crimes that is offenses whose fundamental elements manifest themselves solely or almost solely in cyberspace? There are legal experts who maintain that traditional criminal law principles can be adapted to include most, if not all, the acts considered cybercrimes. Others, nothing especially the considerable difference between the world of the telephone and that

of the internet, the fact that criminals can cause a much greater harm through the internet than other means, like the telephone, to defraud others and the advantage that they have on traditional criminals in avoiding detection and successful prosecution, favor developing new principles of criminal liability and new laws of cybercrimes.

The international responses to the questions on this issue contained in the Section II questionnaire will provide us with an assessment of the direction criminal law is taking internationally on this issue.

(7) Protection of enforcement system (non-compliance offences)

Internet Service Providers (ISPs) possess valuable information that can very useful for the investigation of crimes like subscriber information; internet traffic data (log-files, IP-related data); and content data. It is natural for governments, law enforcement, prosecutors to want to access as much information derived from internet use, web surfing and other transactions as possible. This may collide with constitutional notions of privacy, protection from unreasonable searches and seizures, and forbidding governmental "fishing expeditions."

Another situation that often arises is the control that national governments want to have on the content provided by ISPs to their citizens. There are three primary motives for internet censorship: politics and power, social norms and morals, and security concerns. Protecting intellectual property rights and existing economic interests can also lead to internet censorship. In addition, blocking the networking tools and applications that allow the sharing of information is not infrequent in some countries. Censorship directed at the political opposition is especially frequent in authoritarian and repressive regimes. Some countries block Web sites related to religion and minority groups, often when these movements represent a threat to the ruling regimes. There have been well publicized conflicts and clashes between well known ISPs and the governments of certain countries on this issue. Financial interests related to intellectual property rights can also be a factor justifying drastic governmental intervention.

The questionnaire aims at obtaining information on this wide and complicated issue that reflects different legal traditions (e.g. the concept of Lèse majesté), cultural values, and economic priorities.

(C) International Approaches

Developing an international paradigm for addressing electronic crime is a challenge, given the global nature of the technology. All nations continue to struggle to define these crimes and develop electronic crime legislation applicable to both domestic and international audiences and situations. Purely domestic solutions are inadequate because cyberspace has no geographic or political boundaries and many electronic systems can be easily and surreptitiously accessed from anywhere in the world. International financial institutions are common targets for electronic fraud and embezzlement schemes. In addition, the development of sophisticated electronic technology has enabled organized crime and terrorist groups to bypass government detection and carry out destructive acts of violence. Even when computer-specific criminal statutes are in place, the rules of evidence in several industrialized countries could continue to hinder prosecutions until they adapt them to electronic crimes. Countries that restrict their political discourse face the problem that the Internet provides a source of "illegal" information that is difficult to regulate. Moreover, what constitutes "acceptable" speech in the various countries on the information super-highway differs greatly, even between Western democracies. Solutions to freedom of expression issues on the Internet have varied widely. Some European countries initially tried to target the Internet service providers (ISPs). Other countries have implemented regulations that criminalize the distribution or consumption via the Internet of "harmful" information, and at times or even permanently limit or disrupt internet access.

Intellectual property crimes are a serious problem in the international arena. International software piracy remains endemic which means that many software applications existing on electronic devices around the world continue to be unpaid-for, illegal copies. In some cases legislation has been enacted to place considerable requirements and consequently to potentially incriminate Internet Service Providers. The problems of data mining, identity fraud, online gambling, child pornography, controlling employees via information technology, privacy violations by social media and search engines, like Facebook and Google, or wireless communications, like iPhones, are attracting considerable attention and concern.
Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access, violations of privacy rights and manipulation of data. While a number of differences remain, there are significant areas of convergence in various nations' legislation. By defining specific new offenses and penalties, these codes avoid analytical difficulties that arise when general criminal laws are applied to computer crimes. At the same time, however, electronic governmental access to private or business information, bypassing traditional steps of constitutional protections and procedural criminal law, are raising concerns, new and difficult questions and the need to update substantive and procedural criminal law.
International organizations and private corporations are also working to combat ICT crimes by contributing to the drive to harmonize national legislation. Nonetheless, international efforts have been mixed.

(D) The Questionnaire

It is clear that our information society has generated many new problems, challenges and opportunities for criminal law. There is a clear need to expand the frontiers of criminal law and of its application. The protection of privacy and human rights remains a paramount concern. The many areas of intervention mentioned above are appropriate for debate in Section II since they constitute the core of the specific expansion and innovation in substantive criminal law required by the information society that more and more encompasses and even controls not only our lives and activities but also world affairs, international relations and the threat of cyber wars. The accompanying questionnaire for Section II, Special Part, has been designed
to collect relevant information on the response of criminal law to cybercrime in various countries worldwide. The questionnaire is organized around the major interests that have been identified as deserving protection (see above Section C). The questions center around the interests to be protected and the classical criminal law requirements of actus reus, mens rea, and the penalty envisioned in the law for different types of perpetrators like private persons, public officials, investigators, etc. The questionnaire limits itself to set major markers in the field and allow the National Reporters to contribute information taking into account different legal traditions and varying stages of development of national cybercrime laws. It is hoped that following this scheme of legal interests will facilitate the work of the National Reporters and elicit valuable information on the status of cyber criminal law worldwide. This should be fertile material for the development of resolutions at the Preparatory Colloquium and at the International Congress of the AIDP.