Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

CROATIAN NATIONAL REPORT*

Davor DERENČINOVIĆ*

(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).

A comprehensive reform of substantive criminal law in Croatia was launched in 2009. The new Criminal Code (hereinafter: CC) was adopted in 2011 and entered into force on 1 January 2013. All cyber-crimes in Croatian legal system, both in previous and current CC, are criminalized in Criminal Code. In previous CC cyber-crime related offences were criminalized under Title XVII (criminal offences against property - infringement of secrecy, integrity and accessibility of computer data, programs and systems; computer forgery and computer fraud) and under Title XIV (criminal offences against sexual freedom and morality - child pornography in a computer system or network). Criminal offences concerning cyber-crime from the new CC are unauthorized access, computer system interference, damage to computer data, unauthorized interception of computer data, data forgery, computer fraud, misuse of devices, unlawful use of personal data and exploitation of children for pornography (see description of these criminal offences below).

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

In Croatian legal system, court decisions are not legally binding neither for lower courts nor for other panels of the same court. However, Supreme Court has an authority to uniform/harmonize judicial practice through delivering legal opinions on various legal issues. These legal opinions, when adopted by the Supreme Court, become binding for other panels of the Supreme Court and normally lower courts follow them as well. No such legal opinion concerning cyber-crime related criminal offences has been issued so far. In addition, due to low number of prosecutions for cyber-crime related criminal offences, the impact of judicial decisions in this field is not significant.

(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.

See reply above (B/1/).

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Dr.sc. Davor Derencinovic, Full Professor of Criminal Law, Head of Chair for Criminal Law, Faculty of Law, University of Zagreb, e-mail: davorderen@yahoo.com

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

Cyber-related criminal offences always require intention. *Dolus eventualis* is sufficient and specific intent is not required by the law.

(2) Are there also negligent offenses in this field?

In Croatian legal system, negligent conduct is punishable only if prescribed by the law. This is not the case with cyber-crime related criminal offences.

(3) If yes, please, provide a list of those offenses.

n/a

(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?

Illegal access is criminalized under provision on unauthorized access (article 266. CC). Liable for this criminal offence (hacking) is „whoever accesses a computer system or computer data without authorization" (imprisonment for up to one year). Aggravated form of the offence is when unauthorized access has been made with respect to a computer system or computer data of a state authority, body of local or regional self-government, public institution or company of special public interest. In that case, punishment is imprisonment for a term of up to three years. Attempt is punishable in both cases. Preventing and hindering of the functioning or use of a computer system, computer data or programs, or computer communication is criminalized under article 267. CC (computer system interference). For this criminal offence perpetrator shall be sentenced to imprisonment for a term of up to three years. Attempt is also punishable. Despite of not being explicitly mentioned in the provision, *actus reus* of the offence consists of, for instance, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data (for instance by simultaneous sending of data from many computers). A computer system shall mean "any device or a group of inter-connected or inter-linked devices, one or more of which process data automatically on the basis of a computer program, as well as computer data stored or processed in, read or transferred into it for the purpose of its operation, use, protection and maintenance (Article 87. par.17. CC).

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?

There is no additional requirement under articles 266. and 267. CC 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. However, possession of device suitable to hack the computer system is a separate criminal offence (see reply below on misuse of devices) which means that described situation would fall under the concurrence of offences.

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.

According CC computer data "shall mean any denotation of facts, information or ideas in a form suitable for computer processing" (article 87. par. 18. CC) and computer program "shall mean a set of computer data that are capable of prompting the computer system to perform a certain function." (art. 87. par. 19. CC).

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?**

Damage to computer data (article 268. CC) means unauthorized damaging, altering, deleting, destroying, rendering unusable or inaccessible or presenting as inaccessible, in full or in part, another's computer data or programs. Punishment is imprisonment for a term of up to three years and attempt is also punishable.

***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?**

For unauthorized interception of computer data (article 269. CC) is liable "whoever intercepts or records without authorization non-public transmissions of computer data, including electromagnetic emissions from a computer system, or makes available to another the data thus procured". Punishment is imprisonment for a term of up to three years and attempt is also punishable. The data derived from the commission of this criminal offence shall be destroyed.

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.

For data forgery (article 270. CC) is liable „whoever produces, inputs, alters, deletes, or renders unusable or inaccessible without authorisation computer data of value to legal relations with the intent that they be used as authentic, or whoever uses or procures for use such data". Punishment is imprisonment for a term of up to three years and attempt is also punishable. The data derived from the commission of this criminal offence shall be destroyed.

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.

See reply above. In addition, computer fraud has also been criminalized (article 271. CC). Perpetrator is "whoever with the aim of acquiring for himself/herself or another an unlawful pecuniary advantage inputs, alters, deletes, damages, renders unusable or inaccessible computer data or interferes with the functioning of a computer system and thus causes damage to another" (imprisonment for a term of between six months and five years). If a perpetrator acquired considerable pecuniary advantage or if considerable damage is caused the perpetrator shall be sentenced to imprisonment for a term of between one and eight years. The attempt is punishable and the data derived from the commission of the offence shall be destroyed.

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?

Misuse of devices is criminalized under article 272. CC. Basic form of the offence (par. 1.) is when whoever "produces, procures, sells, possesses or makes available to another a device or computer program or computer data designed or adapted for the purpose of committing any of the cyber-crime related offences with intent that it be used for the purpose of committing any these criminal offences." (imprisonment for a term of up to three years). The perpetrator of this criminal offence referred shall not be imposed a sentence more severe than the one prescribed for the criminal offence the perpetrator intended to commit. Special devices and programs shall be seized while computer data shall be destroyed. Another form of the offence (par. 2.) is when someone "produces, procures, sells, possesses or makes available to another a computer password, access code or other data by which a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the cyber-crime related offences" (imprisonment for a term of up to one year).

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*?**

Being a separate criminal offence, misuse of devices which includes, *inter alia*, unauthorized possession (and use) of hacker's tools could be prosecuted in conjunction with other cyber-crime related offence (for instance illegal access) committed by the same perpetrator (concurrence of offences).

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

Procuring, selling and making available to another device, device or computer program or computer data designed or adapted for the purpose of committing any of the cyber-crime related offences is punishable under article 272. CC (par. 1. and 2. – see reply above)

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?

Possession is criminalized under article 272. CC (par. 1. and 2. – see reply above).

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?**

Data collectors have obligation to disclose their information practices before collecting private information from consumers according to Consumer Protection Act, Act on Protection of Personal Data and Electronic Communications Act.

***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?**

Yes. See reply above.

***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?**

Online trade companies are allowed to use data on consumer's e-mails only for the purpose of selling their products or for the advertising only if consumers have clear possibility to file a complaint free of charge (article 107. Electronic Communications Act).

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

Failure to provide disclosure is punishable as a misdemeanor and those responsible shall be fined.

b. Act – illegal use and transfer/distribution?

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

Illegal transfer and distribution of private data is criminalized as unlawful use of personal data (article 146. CC). Perpetrator is who, in contravention of the conditions set out in the act, collects, processes or uses personal data of physical persons (imprisonment for a term of up to one year).

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

Yes. See reply above.

c. Justification?

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

Conditions for authorized collection, processing, transfer and distribution of private data are set in Act on Protection of Personal Data. According to article 6., "personal data may be collected for a purpose known to the data subject, explicitly stated and in accordance with the law, and may be subsequently processed only for the purposes it has been collected for or for a purpose in line with the purpose it has been collected for. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate protection measures are in place." In principle, personal data may be collected and subsequently processed with the consent of the data subject. Exceptions must be prescribed in law (for instance, collection of personal data in public interest).

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

Personal data must be relevant for the accomplishment of the established purpose and shall not be collected in quantities more extensive than necessary for achieving the purpose defined (Article 6 of the Act on Protection of Personal Data).

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?

Professionals have an obligation to keep as secret personal information from their patients and clients. Unauthorized disclosure is criminal offence punishable by imprisonment for a term of up to one year (article 145. CC)

***ii.* Which data are specifically protected, if any?**

Information about the personal or family life confined to certain professionals in the performance of their occupation (article 145. CC).

***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)?**

Breach of confidentiality would be considered as a legitimate if a secret was disclosed in the public interest or the interest of a third party which prevails over the interest of keeping the secret. Under this very broad clause would

come, for instance, reporting child abuse. However, it does not happen in practice that professionals use this possibility that would relief them from criminal liability.

b. Subject – Type of perpetrators?

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

Professionals who are bound by specific confidentiality rules are the following: attorney-at-law, notary public, health worker, psychologist, employee of a welfare institution, religious confessor and other person (article 145. par. 1. CC).

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?

Any authorized disclosure which could be understood as a transfer and distribution is penalized under article 145. par. 1. CC.

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?

Yes, through unlawful use of personal data (article 146. CC). Criminalized is unlawful/unauthorized collecting, processing or using personal data of physical persons. Aggravating form of the offence would be if the perpetrator has acquired pecuniary gain for himself/herself or another or caused considerable damage.

b. Subject?

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

Any natural person can commit this criminal offence. An aggravated form of the offence would be if the perpetrator is public official who committed the offence in the exercise of his/her authorities. Legal person could also be held liable under Law on Responsibility of Legal Persons For Criminal Offences.

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

Actus reus of a criminal offence from article 145. CC is unauthorized collecting, using and processing of personal data.

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

Handling of personal data for law enforcement purposes is allowed under the conditions prescribed by the law (for instance storing personal data for the purpose of establishing criminal record of a convicted person).

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?**

See reply above. Conditions for authorized collection, processing, transfer and distribution of private data are set in Act on Protection of Personal Data. According to article 6., "personal data may be collected for a purpose known to the data subject, explicitly stated and in accordance with the law, and may be subsequently processed only for the purposes it has been collected for or for a purpose in line with the purpose it has been collected for. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate protection measures are in place." In principle, personal data may be collected and subsequently processed with the consent of the data subject. Exceptions must be prescribed in law (for instance, collection of personal data in public interest).

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

See reply above. Personal data must be relevant for the accomplishment of the established purpose and shall not be collected in quantities more extensive than necessary for achieving the purpose defined (Article 6 of the Act on Protection of Personal Data).

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.**

There is no specific criminal offence of identity theft but appropriating another's personal information without his or her knowledge could be prosecuted as unlawful use of personal data (article 146. CC). *Actus reus* of this criminal offense is unlawful/unauthorized collecting, processing or using personal data of physical persons. Aggravating form of the offence would be if the perpetrator has acquired pecuniary gain for himself/herself or another or caused considerable damage.

***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.**

Phishing could be prosecuted under data forgery statute (producing, using or procuring computer data with the intent that they be used as authentic, article 270. CC) or computer fraud statute (inputting computer data with an intention to acquire unlawful pecuniary advantage, article 271. CC). Since using spoofed emails designed to lure recipients to fraudulent websites is a form of misleading another by misrepresenting or concealing facts or keeping him in error, an common crime of fraud (article 236. CC) could also be used to prosecute phishing and similar practices.

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.

Digital personality does not exist as a legal concept in Croatian legal system. Avatar or digital role in an internet based simulation game would not be considered as a personal data defined in article 2(1) of the Act on Protection of Personal Data - Personal data means any information relating to an identified natural person or an identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

(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.**

Use of internet for the purpose of storing, accessing, and disseminating child pornography is criminalized through the exploitation of children for pornography (article 163. par. 2. CC). The perpetrator is whoever takes child pornography pictures or produces, offers, makes available, distributes, transmits, imports, exports, procures for himself/herself or for another person, sells, gives, exhibits or possesses child pornography or knowingly obtains access, through information and communication technologies, to child pornography (imprisonment form one to eight years). Attempt is also punishable.

***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;

It is criminalized under article 163. par. 2. CC (see reply above).

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

Pornographic material that depicts children shall be destroyed (article 163. par. 4. CC).

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

Special devices, means, computer programs or data intended for, adapted to or used for committing or facilitating child pornography shall be seized (art. 163. par. 4. CC)

 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…?

It is criminalized under article 163. par. 2. CC (see reply above).

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

Enticement, recruitment or incitement of a child to pornography (article 163. par. 1. CC) also include 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)?**

According to article 163. par. 6. CC child pornography shall mean "any material that visually or otherwise depicts a real child or a realistic image of a non-existent child or a person appearing to be a child, involved or engaged in real or simulated sexually explicit conduct, or any depiction of a child's sexual organs for sexual purposes." Any material that is artistic, medical, scientific, informative or similar in character shall not be deemed pornography. This definition has been in line with article 2(c) of the Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA as well as with article 9(2) of the Convention on Cybercrime (CETS No.: 185) and article 20(2) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.: 201).

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?**

Children trafficked for the purpose of exploitation for prostitution of the person or of other forms of sexual exploitation, including pornography (article 106. par. 2. CC) will not be prosecuted for prostitution or the appearance in pornography. Persons under age of 14 are not criminally liable in general, and for those older than 14 years, in the absence of explicit non-punishment provision other provisions of the CC will apply (for instance defense of necessity

– article 22. CC). In addition, according to article 163. par. 5. CC, a child shall not be punished for "producing and possessing pornographic material depicting him/her alone or him/her and another child, where this material is produced and possessed by them with their consent and solely for their own private use."

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.**

Virtual child pornography is also criminalized because the definition of child pornography includes, *inter alia*, a realistic image of a non-existent child or a person appearing to be a child, involved or engaged in simulated sexually explicit conduct.

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?

According to article 163. par. 2. CC perpetrator must obtain access to a child pornography "knowingly" which entails either direct intent or at least *dolus eventualis*. Person who without such knowledge, i.e. inadvertently, accessing sites containing child pornography cannot be held criminally liable.

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?

These conducts are criminalized in article 140. CC. Liable is whoever persistently and over a long period of time follows or spies on another, or establishes or seeks to establish unwanted contact with another, or intimidates another in some other way and by doing so provokes anxiety in him/her or causes him/her to fear for his/her safety or the safety of persons close to him/her. Stalking and intimidating could have different forms including following and stalking in cyberspace (for instance in chat rooms, social networks or similar).

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.

Mass distribution through internet of falsified medicinal product or medical device (article 185. par. 5.), disseminating information through the media, the Internet or by any other means, which gives, or is likely to give, false or misleading signals as to financial instruments (article 260. par. 1(3) CC), public incitement to violence and hatred through computer system or network (article 325.), insult committed through computer system or network (article 147. CC), bringing shame on another through computer system or network (article 148. CC), defamation through computer system or network (article 149. CC) etc.

(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

Computer fraud is criminalized under article 271. CC (for description see reply above). Responsibility for copyright infringement takes place when the perpetrator in "violation of regulations on copyright and related rights reproduces, adapts, distributes, stores or takes any other action for the purpose of distribution of, or communicates to the public in whatever way another's copyright work, or allows this to be done and thus obtains a pecuniary advantage or causes damage." (article 285. par. 1. CC). Communicating to the public in whatever way another's copyright work includes situation when the offence has been committed through computer system or network. Same applies to infringement of copyright concerning phonogram or videogram (article 286. CC).

(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.

Virtual child pornography is criminalized under CC (see reply above on definition of child pornography that includes so called virtual child pornography as well). Cyber-defamation is also criminalized as an aggravated form of defamation (article 149. CC, see reply above). Sexual harassment shall mean any form of unwanted verbal, non-verbal or physical conduct of a sexual nature which aims at or effectively constitutes a violation of the dignity of a person, which creates an intimidating, hostile, degrading or offensive environment (article 156. par. 2. CC). Although it is not explicitly mentioned, sexual harassment could be committed in the virtual world as well if it has been committed by person in a position of authority and if it created an intimidating, hostile, degrading or offensive environment

(f) Non-Compliance Offenses

Does you criminal law penalize noncooperation 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.

Code of Criminal Procedure (hereinafter: CCP) envisages that, among others, internet service providers must enable an access to computer system or computer data and to provide information indispensable for accomplishing purposes of the search (article 257. par. 1.). For certain most serious criminal offences including cyber-crimes, judge of investigation may issue a warrant to implement special investigative measures (for instance secret surveillance or interception, gathering and recording of electronic data, article 332. CCP). The technical operation center for the supervision of telecommunications that carries out technical coordination with the provider of telecommunication services in the Republic of Croatia as well as providers of telecommunication services shall be bound to provide the

necessary technical assistance to the police authorities. In case of proceeding contrary to this obligation, the judge of investigation shall upon the motion with a statement of reasons of the State Attorney impose a fine on a provider of telecommunication services in an amount of up to HRK 1,000,000.00 (cca 133.000,00 EUR), and on a responsible person in the technical operative center for the supervision of telecommunications that carries out technical coordination and on a provider of telecommunication services in the Republic of Croatia in an amount of up to HRK 50,000.00 (cca 6.600,00 EUR), and if thereafter the ruling is not complied with, the responsible person may be punished by imprisonment until the ruling is executed, but not longer than one month. The panel shall decide on the appeal against the ruling on the fine and imprisonment. The appeal against the ruling on the fine and imprisonment shall not stay its execution (article 335. par. 2. CCP).

(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?

Systematic collection and disaggregation of statistical data on cyber-crime related offences has not been provided. However, police does have a statistics on these offences that are known (reported) to them. Statistical data gathered by the police differs from the data made available by the National Bureau of Statistics (hereinafter: NBS) that publishes its crime reports annually. It may be due to the different criteria for collecting the data or insufficient accuracy in filling statistical reports by competent authorities. Statistical reports of the NBS are filled in by competent county and municipality public prosecutor's offices after the final decision has taken place as well as competent county and municipal courts of first instance that act after the criminal procedure has been validly concluded. Observation units are adult perpetrators of criminal offences, who can be either direct perpetrators, accomplices, instigators or assistants. Number of cyber-crime related criminal offences reported to the police and/or to public prosecutor's offices in 2011 was 228 (180 for computer fraud, 10 for computer forgery, 10 for infringement of secrecy, integrity and accessibility of computer data, programs and systems and 28 for child pornography in a computer system or network). Number of those convicted for cyber-crime related criminal offences in 2011. is 112 which is less than 0,5% of all adult perpetrators convicted for all criminal offences (23.389). Most of them have been convicted for computer fraud (86) followed by child pornography in a computer system or network (17), computer forgery (6) and infringement of secrecy, integrity and accessibility of computer data, programs and systems (3). This is an increase in comparison to 2010 (78 convicted adults) and 2009 (49 convicted adults). However, it should be taken into account that these are the convictions for criminal offences committed not only in a year when conviction was rendered but to offences that were committed in previous years as well. Number of minors (persons younger than 18) convicted for cyber-crime related offences is insignificant (1 minor convicted in 2012 for child pornography in a computer system or network).

(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.

Description of dangerousness of cyber-crime related criminal offences and damages that it causes has been published on the web page of the Ministry of Interior (www.mup.hr, only in Croatian). There are also some advices to general public and internet users on how to avoid cyber-crime victimization. Ministry of Interior in collaboration with Croatian Academic and Research Network (CARnet) has also published compendium/manual on internet security/safety that includes description of threats for internet users, contact information of competent authorities etc. (http://www.carnet.hr/tematski/sigurnost/index.html, available only in Croatian).

(3) Do victimization surveys in your country include questions on cyber-crimes?

There have been no systematic victimization surveys that include questions on cyber-crimes.

(4) What types of computer crime/computer fraud are most often reported in your country?

Computer fraud in form of e-mail letters with false notifications about lottery winning, so called Nigerian letters, phishing, child pornography on computer system or network etc. (see reply above on available statistics).

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

Unit for computer crime and protection of intellectual property was established in the Criminal Police as a functional part of the Department of economic crime and corruption. However, a few years ago that unit was disbanded. There is no special division in charge of cyber-crime related offences in public prosecutor's office.

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

There have been no separate courses on cyber-crime but relevant issues concerning that phenomenon are thought in courses on substantive criminal law and legal informatics.

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

Police Academy provides education and training on cyber-crime related issues including introduction of the courses on computer crime and informatics security/safety. Curriculum for training of judges and prosecutors in Judiciary Academy does not provide their systematic training and education on cyber-crime related issues.

(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:

For numbers of those reported to the police/public prosecutor and convicted for cyber-crime related offences see reply above. As to the trends, there has been an increase of computer forgery, phishing, hacking and computer fraud in form of so called Nigerian letters, false notifications on lottery winning etc.