INTERNATIONAL ASSOCIATION OF PENAL LAW

19th International Congress on Information Society and Criminal Justice

Preparatory Colloquium Section 1, General Part: Concept paper and questionnaire

Verona (Italy)

29 November – 1 December 2012

REPORT FOR BELGIUM*

National Rapporteur: Professor Paul De Hert[1]
Co-author : Mr. Gertjan Boulet[2]

[1] Professor Paul De Hert holds a chair at the Vrije Universiteit Brussel as well as at the Tilburg University; E-mail: paul.de.hert@vub.ac.be

[2] Mr. Gertjan Boulet is a voluntary researcher at the Vrije Universiteit Brussel and an intern at the Constitutional Court of Belgium; E-mail: gertjanboulet@gmail.com

* 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.

0. PRELIMINARY REMARKS

The scope of the questionnaire is defined in the draft guiding text of general rapporteur Prof. dr. T. Weigend:

"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."

This report is partly based on an earlier report on cybercrime legislation in Belgium, written by Paul De Hert and Frédéric Van Leeuw,[3] and presented at the Congress of Washington of the International Academy of Comparative Law.[4]

The authors of this report would like to thank Frederik Decruyenaere[5] and Frédéric Van Leeuw for their useful comments.

[3] Federal Magistrate, Office of the Federal Prosecutor of Belgium, Organized Crime Unit, Brussels, Belgium.

[4] P. DE HERT & F. VAN LEEUW, 'Cybercrime Legislation in Belgium', in E. DIRIX & Y.H. LELEU (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels, Bruylant, 2011, 867-956, http://www.vub.ac.be/LSTS/pub/Dehert/389.pdf

[5] Attaché, Ministry of Justice of Belgium, Directorate-General Legislation, Liberties and Fundamental Rights, Specific Crimes and Procedures Department, Brussels, Belgium.

A. CRIMINALISATION

1. Specific legal interests deemed to be in need of protection by criminal law

Confidentiality, integrity and availability of computer systems

Hacking: See below A.2.1 (Attacks against IT-systems), A.2.5 (Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities), A.3.1 (Typical definition of criminal conduct in these crimes by description of act or by consequence), B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation), C.1 (Criminal laws covering mere preparatory acts that carry a risk of furthering abuse), C.2 (Criminalization of the mere possession of certain data), F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet) and G.1 (Current trends of legislation and legal debate concerning ICT and internet crime).

Illegal interception: See below A.2.1 (Attacks against IT-systems), A.2.2 (Violation of IT privacy), A.3.1 (Typical definition of criminal conduct by description of act or by consequence), B.1 (Specific problems with respect to the principle of legality), C.1 (Criminal laws covering mere preparatory acts that carry a risk of furthering abuse), C.2 (Criminalization of the mere possession of certain data) and F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet).

Data and system interference: See below A.2.1 (Attacks against IT-systems), A.2.2 (Violation of IT-privacy), A.2.3 (Forgery and manipulation of digitally stored data), A.2.4 (Distribution of computer viruses), A.3.1 (Typical definition of criminal conduct in these crimes by description of act or by consequence), B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation), C.1 (Criminal laws covering mere preparatory acts that carry a risk of furthering abuse), C.2 (Criminalization of the mere possession of certain data) and F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet).

Financial interests

Computer fraud: See below: A.2.1 (Attacks against IT-systems), A.2.3 (Forgery and manipulation of digitally stored data), A.2.5 (Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities), A.6 (Specific differences between the definition of cyber crimes and “traditional” crimes), B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation) and F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet).

Computer forgery and use of forged computer data: See below: A.2.1 (Attacks against IT-systems), A.2.3 (Forgery and manipulation of digitally stored data), A.2.5 (Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities) and A.6 (Specific differences between the definition of cyber crimes and “traditional” crimes).

Civil liberties

Right to privacy

- use of forged computer data

- data theft

- identity theft: See below: A.2.5 (Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities), B.1 (Specific problems with respect to the principle of legality), B.3 (Avoidance of criminal legislation becoming

obsolete in light of rapid technological innovation), E.2 Laws or regulations obliging an internet service provider to register users prior to providing services) and G.1 (Current trends of legislation and legal debate concerning ICT and internet crime).

- spamming or stalking: See below A.2.1 (Attacks against IT-systems), A.2.3 (Forgery and manipulation of digitally stored data), A.6 (Specific differences between the definition of cyber crimes and "traditional" crimes) and C.1 (Criminal laws covering mere preparatory acts that carry a risk of furthering abuse).

Right to non-discrimination / racism: See below B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation) and C.2 (Criminalization of the mere possession of certain data).

Rights of the child / child pornography: See below A.2.6 (Other innovative criminal prohibitions in the area of ICT and internet), A.6 (Specific differences between the definition of cyber crimes and "traditional" crimes), B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation), C.3.3 (Obligation for providers to provide information on the identity of users), and D.2 (Non-criminal means of combating offensive websites used/propagated).

Copyrights: See below A.2.6 (Other innovative criminal prohibitions in the area of ICT and internet) and F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet).

2. Typical examples of criminal laws

2.1 Attacks against IT systems

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The 2000 Computer Crime Act introduced hacking in Article 550bis of the Criminal Code (CC) that punishes him or her who unauthorised enters or stays within a computer. The purpose of Article 550bis CC is to protect the integrity of the computer system. The Belgian legislator distinguishes external hacking (Article 550bis § 1 CC) from internal hacking (Article 550bis § 2 CC), the first being sentenced less severely than the latter. However, the scale of punishment is the same for both types of hacking when the aggravating circumstances are met.

An attack from outside the system (Article 550bis § 1 CC) – external hacking- is punishable by imprisonment of 3 months to one year, or, if there is fraudulent intent ('intention frauduleuse'; 'bedrieglijk opzet') of 6 months to two years[1]. An attack from within (Article 550*bis* § 2 CC) is only punishable if someone exceeds his access authority with fraudulent intent or with the intention to do damage; the penalty is 6 months' to two years' imprisonment.

Attempt (Article 550*bis* § 4 CC) and ordering and inciting (Article 550*bis* § 6 CC) to hack are also punishable. The originality of the Belgian legislation is that the penalties in this case are identical to that of the hacking carried out for both types of hacking.

The Act of June 13th, 2005 on electronic communications (see below under this section) provides a special penal provision in Article 145 § 3, 1° that punishes anyone who makes fraudulent electronic communications through a network of electronic communication. The provision could be used as a basis for the prosecution of hacking. It could supplement the specific incrimination of hacking in Article

550*bis* CC. This specific provision imposes liability to a fine of 500 to 50,000 euros and / or imprisonment for 1 to 4 years, whereas the Act of June 2005 only imposes fines (500 to 50,000 euros).

Illegal interception (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Illegal interception is specifically targeted as a crime in Article 314*bis* CC, inserted by the law of June 30th, 1994 concerning the protection of privacy in relation to the monitoring and intercepting of communications (Wiretap Act).[2] This crime concerns the intentional interception of private communications or telecommunications with any device during transport. Interception covers listening to, taking knowledge of or recording a communication. The penalty is 6 months to 1 year of imprisonment (Article 314*bis* § 1 CC). Moreover, the use of legally intercepted communications is also penalised if there is a fraudulent intent or an intention to cause damage. These acts are punishable with 6 months to 2 years imprisonment (Article 314*bis* § 2 CC). Attempt to intercept is equally punishable (Article 314*bis* § 3 CC), and the penalties are doubled in case of recidivism of illegal interception within five years (Article 314*bis* § 4 CC).
Art. 259*bis* CC, inserted by the same 1994 Act, covers similar penalisations for interception by public officials who exceed their legal authority to wiretap.

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The first paragraph of Article 550*ter* CC now punishes whoever who enters data in a system without permission, modifies or deletes the data or alters using any technological means the routine use of data in a computer system (imprisonment of six months to three years and a fine of twenty-six euros to twenty five thousand Euro or either of these penalties) (Article 550*ter*, § 1, 1° CC). If this crime is committed with intent to defraud or in order to harm, the penalty is imprisonment of six months to five years (Article 550*ter*, § 1, 2° CC).

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): '*faux en informatique*', also introduced in 2000, is incriminated under Article 504*quater* CC. The Article states that whoever "seeks to procure for himself or for another person, with intent to defraud, unlawful economic gains through entering, changing, deleting or in any other way altering the normal use of computer data in a computer system. Like with the crime of computer forgery, there is a requirement of deception. Computer fraud is punished with 6 months' to 5 years' imprisonment (Article 504*quater* § 1 CC). Attempt is punishable with maximum 3 years' imprisonment (Article 504*quater* § 2 CC), and recidivism, when related to a computer crime within five years will double the punishment (Article 504*quater* § 3 CC).

Computer Forgery and Use of Forged Computer Data (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): the Computer Crime Act also introduced a new provision specifically on computer forgery. Art. 210*bis* CC penalises forgery through entering, changing or deleting computer data or through altering their potential use, if this causes a change in the legal scope of such data. The penalty is 6 months to 5 years imprisonment (Art. 210*bis* § 1CC). This covers for instance forgery of

credit cards, electronic contracts or electronic signatures. Although the text of the provision itself does not say so, there is a requirement of fraudulent intention or intention to cause damage.[3] This interpretation was followed by the jurisprudence confirming that art. 210*bis* must be read together with art. 193 of the Penal Code which describes the infringement of forgery in a general way.[4]
The use of forged computer data is equally punishable (Art. 210*bis* § 2 CC). For attempt, the maximum penalty is 3 years imprisonment (Art. 210*bis* § 3 CC). Recidivism of a computer crime within five years will double the punishment (Art. 210*bis* § 4 CC).
We stress that the use of forged computer data (Art. 210*bis* § 2 CC) is an autonomous crime. No special intent is required. One only needs to have known that the data was false.[5]

Spamming or stalking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 145 § 3*bis* of the Act of June 13, 2005 on electronic communications incriminates "*the person who uses a network or electronic communications service or other electronic means to annoy or cause damage to his correspondent and the person installing any device intended to commit the offence and the attempt to commit it* ".

Privacy (or "data protection") Offences (See below A.2.2: Violation of IT-privacy; A.2.5: Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities; C.1: Criminal laws covering mere preparatory acts that carry a risk of furthering abuse; C.2: Criminalization of the mere possession of certain data; D.2: Non-criminal means of combatting offensive websites used/propagated): The Data Protection Act of 8 December 1992 as amended by the Act of 11 December 1998 imposes obligations on data controllers both in the public and in the private sector[6], although certain exemptions do exist like for instance in the case of the gathering of information for police purposes[7]. Less known and almost never used in legal practice are the privacy crimes contained in this Act[8]. It provides in its criminal provisions (art. 37 to 39), a whole range of sanctions for the data controller in case he fails to meet his obligations and would jeopardize the confidentiality of such data, and these will without any doubt apply to certain use of personal data, threatening the identity data of a person. Especially Article 39 of the Act is, in theory at least, a very suitable instrument to combat identity theft, hacking, secret surveillance and websites with sensitive data hosted by individuals without permissions such as websites about suspected sex offenders.[9]

Act of June, 13th 2005 on electronic communications (See above under this section: Hacking; See below A.2.2: Violation of IT-privacy; A.2.3: Forgery and manipulation of digitally stored data; A.2.4 Distribution of computer viruses; A.6: Specific differences between the definition of cyber crimes and "traditional" crimes; B.1: Specific problems with respect to the principle of legality; B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation; C.2: Criminalization of the mere possession of certain data; C.3.4: Obligation for providers to prevent access to certain information; D.1: Role of criminal law in relation to other ways of combating abuse of ICT and the internet; E.1: Laws or regulations obliging internet service providers to store users' personal data; E.3: Laws or regulations limiting the encryption of files and messages on the internet): Under Article 124 of the Act of June 13th, 2005 on electronic communications, the following actions are regarded as crimes unless the consent of all parties directly or indirectly involved has been given:
1. intentionally, taking note of the existence of signs, signals, writings, images, sounds or data of any nature that originate from and are addressed to others (Article 124, 1°);

2. intentionally, modifying or deleting this information by any technical means or identifying the other persons (Article 124, 2°);
3. intentionally taking note of telecommunication data that relate to other persons (Article 124, 3°);
4. disclosing, using in any way, modifying or destroying the information, identification and data set forth in 1, 2 and 3 above (Article 124, 4°).

2.2 Violation of IT privacy

Illegal interception: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Data and system interference: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Privacy (or "data protection") Offences: see above A.2.1 (Attacks against IT systems).

Act of June, 13th 2005 on electronic communications: see above A.2.1 (Attacks against IT systems).

2.3 Forgery and manipulation of digitally stored data

Data and system interference: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Computer fraud: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Computer Forgery and Use of Forged Computer Data: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Spamming or stalking: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Act of June, 13th 2005 on electronic communications: see above A.2.1 (Attacks against IT systems).

2.4 Distribution of computer viruses

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Terms like 'computer viruses', 'worms' and 'Trojans' do not appear in the Computer Crime Act. Like in Dutch law, they are considered a special case of data and system interference, and fall under those provisions of Art. 550*ter* CC that prohibit indirect data and system interference and indirectly changing the potential use of computer data by any technological means. Virus creation and

spreading, virus generators and denial-of-service attack scripts are also covered by art. 550*ter* § 4 CC. Sending an e-mail to transmit the virus or malware to the victim's computer may also be punishable under Article 145 §3 1° of the Act on electronic communications which punishes the use of any means of Communication to inflict harm on others (see above A.2.1: Attacks against IT systems).

2.5 Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law). Computer fraud has a very broad scope. Some authors assume that it might even cover the placing of durable cookies.[10] Another example given in this context is the act to demand or annul an internet connection or telecommunications connection using a false name or the name of somebody else. In 2008 the Court of appeal of Antwerp decided that the use of a credit card belonging to a company by an employee to carry out personal purchases is computer fraud.[11]

Computer Forgery and Use of Forged Computer Data: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Identity Theft (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 231 CC sanctions the unjustified use of someone else's name in public. However, the scope of this provision is limited, as it concerns the actual unjustified application of another person's name, but not the preparatory actions preceding the abuse.

The Act of December 8, 1992 on the protection of privacy with regard to the processing of personal data (see above A.2.1: Attacks against IT-systems), defines personal data as: "*any information concerning an individual identified or identifiable hereafter "person*"; an identifiable person can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, psychological, economic, cultural or social". This statute provides in its penal provisions (art. 37 to 39), a whole range of sanctions for the data controller in case he fails to meet his obligations and would jeopardize the confidentiality of such data (see *below*), and these will without any doubt apply to certain use of personal data, threatening the identity data of a person.

Another approach is criminalisation of identity theft on the basis of computer forgery (see above A.2.1: Attacks against IT-systems). Very illustrative is a judgement of November 28th, 2005 of the Criminal Court of Dendermonde on the creation by a journalist of an email account in the name of someone else. The Court found the journalist guilty on the charge of having committed 'computer forgery' as set forth in Article 210*bis* CC. However, the Court did not find the journalist guilty on the charge of having publicly assumed a false name as set forth in Article 231 CC, since he had not intended to make others believe that Mr E.V.M. was his real name.

In some cases, identity theft can be punished by application of Article 550*bis* § 3 CC (taking knowledge and making copies of data) or 550*bis* § 7 CC (selling and receiving of hacked data) (see above A.2.1: Attacks against IT-systems).

Privacy (or "data protection") Offences: see above A.2.1 (Attacks against IT systems).

2.6 Other innovative criminal prohibitions in the area of ICT and internet

- e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere

Child Pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 383 and 383*bis* CC cover different aspects of the expression of pornography.

Online Gambling (See below A.4: Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims; D.1: Role of criminal law in relation to other ways of combatting abuse of ICT and the internet; D.2: Non-criminal means of combatting offensive websites used/propagated): A new Act of 2010 on gambling, updates the 1999 Act on games of chance to take into account the phenomenon of gambling on Internet services.[12] Gambling games on the Internet can now legally be held, but only by legal institutions holding the same type of games "in the real world". International providers of online gambling websites are to comply with Belgian law and obtain a licence if they direct their activities towards the Belgian market. However, providers of chance games whose activity is (only) limited to internet gambling will not obtain a license from the Gambling Commission.

Infringements of Copyright and Related Rights (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The Belgian Copyright Act of June 30th, 1994 was amended by the act of May 22nd, 2005[13] which transposed the EU Copyright Directive.[14] The reform is a faithful copy of this Directive. The new Act introduces *inter alia* an exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction, an exclusive distribution right and an exclusive right of communication to the public for interactive on-demand distribution. Article 79*bis* implements article 6(1)-(3) of the Directive. More generally, Article 80 and following of the Act punishes with a fee between 100 and 100 000 € all those

- who circumvent an effective technological measure, knowingly or with reasonable grounds to know and
- who manufacture, import, distribute, sell, rental, advertise for sale or rental, or possess for commercial purposes devices, products or components or the provision of services which are promoted, advertised or marketed for the purpose of circumvention of, or have only a limited commercially significant purpose or use other than to circumvent, or are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.[15] In case of recidivism a penalty of imprisonment of three month to 2 years can be inflected. Article 87 §1 of the Copyright Act now provides that a court can issue a cease-and desist order to an intermediary service provider whose services are used by third parties for copyright infringements.[16]

The protection of the databases and the right of the producers of the databases is regulated by the Act of August 31st, 1998 which transposes the European directive from March 11th, 1996 on the juridical protection of databases.[17] This law foresees criminal sanctions for fraudulent or malicious breach of rights or the name of the producer of the databases.

Abuse registration of a domain name: The Act of June 26th, 2003 about the abuse of registration of a domain-name[18] allows the victim to ask the president of the Civil Court of first instance or the president of the Court of trade to order the immediate stop of the abusive use of a domain name which either is identical, or resembles to the point of risking confusion, in particular, with a mark, a geographical ascription or a name of origin, with a trade name, an original work, a company name or denomination of an association, with a patronymic name or a name of a geographical entity belonging to others if the registration is done without any legitimate interest regarding this domain name and with the aim of harming a third party or to take unduly benefit of a domain name.

3. Typical definition of criminal conduct (actus reus) in these crimes

3.1 By description of act or by consequence

The definition of the criminal conduct is related to the specific wording of the articles of the CC. Examples of criminal conduct defined by description of consequence are:

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The Belgian concept of hacking does not require any damage. What counts is the concept of unauthorized access. To connect itself without authorization to unprotected Wi-Fi networks of others can thus be qualified as hacking[19]. Article 550*bis* CC also contains a series of additional incriminations with regard to acts having to do with the consequences of hacking. Incriminations that regard the consequences of hacking target taking knowledge of hacked data (Art. 550*bis* § 3, 1 ° CC), using a hacked system (Art. 550*bis* § 3, 2 ° CC), keeping, using, selling or making public hacked data (Art. 550*bi*s § 7 CC).

Illegal interception (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Also punishable is someone who knowingly keeps, discloses, distributes or uses the contents of illegally intercepted private communications or telecommunications (Art. 314*bis* CC).

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): If, in doing so, the person actually damages any data, the maximum penalty rises to 5 years (Article 550*ter*, § 2CC). If the act impedes entirely or partially the correct functioning of a computer system, the penalty rises to 1 to 5 years' imprisonment (Article 550*ter*, § 3 CC).

3.2 Definition of the object ("data", "writings", contents)

The definition of the object is related to the specific wording of the articles of the CC.

4. Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims

Liability of Internet Service Providers/Providers of Electronic Payment: See below B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation); C.3 (Extension of criminal liability to service providers); E.1 (Laws or regulations obliging internet service providers to store user's personal data) and F.2 (Influence of international legal instruments on criminal law in the area of ICT and internet).

International providers of online gambling websites: See above: A.2.6 (Other innovative criminal prohibitions in the area of ICT and internet).

5. Extension of criminal liability in the area of ICT and internet to merely reckless or negligent conduct

In general, the Belgian CC lacks dogmatic refinement with regard to intent-requirements, and does not distinguish between "negligence" and "recklessness" as mens rea for unintentional offences. The required mens rea is "lack of care or prudence".[20] Criminal liability in the area of ICT and internet for lack of care or prudence can be found in Article 114 § 3 of the Act of March 21st, 1991 concerning the reform of certain economic governmental companies[21] (see below B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation) which punishes with a fine of 500 to 5 000 francs those who involuntarily, by negligence or carelessness, damage or cause to deteriorate part of a public telecommunications network or impede or prevent its functioning. When one of these acts is done by a person in the service of a third party, the pain is imposed on the employer or the person responsible for the work, depending on whether the former or the latter neglected to inform the worker in question about the presence of a public telecommunications network or the directives provided by the operator of the public telecommunications network concerned to protect this infrastructure.
Article 114 § 5 of the same Act punishes by a fine of 1000 to 10 000 francs or three to six months of imprisonment those who have been convicted on the base of § 3 and who involuntarily, by negligence or carelessness, repeat this offense within one year of the date of the verdict or of the date on which the decision has become final.

Below we discuss the extension of criminal liability in the area of ICT and internet to mere preparatory acts that carry a risk of furthering abuse and the mere possession of certain data (see below C.1: Criminal laws covering mere preparatory acts that carry a risk of furthering abuse; C.2: Criminalization of the mere possession of certain data).

6. Specific differences between the definition of cyber crimes and "traditional" crimes

The 2000 Computer Crime Act (See below B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation; F.2: Influence of international legal instruments on criminal law in the area of ICT and internet): Discussions to enact a specific law for computer crime go back to the eighties with the Minister of Justice requesting scientific reports and studies,[22] but with some magistrates and academics opposing a new initiative with the argument that existing law was sufficient to deal with problems of computer crime.[23] Everybody in Belgium was aware of the principled discussion in the Netherlands, reported by Koops,[24] about the legal status of data and the choice to consider data as falling outside of the scope of the term "good" (*goed* or *bien*). Applying theft and other classical crimes to abuses with data, comes in handy for judges and prosecutors (then there is no lacunae in law), but this approach neglects that data cannot be taken away like a traditional object, but needs to be copied and the simple fact that data are multiple and can still be, after illegal copying in the hands of the rightful owner.[25] Only ten years after the Dutch Computer Crime Act, the Belgian legislator dared to regulate the matter, carefully avoiding taking a final position in this discussion (that is still unsolved by the Belgian Supreme Court) by concentrating the phrasings of the crimes on the action taken by the criminals. Hence, the Belgian law prohibits 'hacking' but not 'stealing of data' and classical crimes such as forgery and manipulation are complemented with digital counterparts.

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The difference with the general provision on fraud ('*oplichting*'/'*escroquerie*'), incriminated under Art. 496 CC, is that computer fraud concerns interference of a machine, while traditional fraud concerns manoeuvres that damage the faith of persons.

Computer Forgery and Use of Forged Computer Data (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Classical forgery is penalised in Art. 193ff CC. Unlike the crime of theft, there was a consensus that this provision on forgery was not fitted for combating computer crime. The term '*writings*' in the original provision was deemed unfit to cover computer data.[26] Hence, the Computer Crime Act of 2000 extended this provision to forgery in 'writings, computer data or in telegrams'[27].

Spamming or stalking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law; A.2.1 Attacks against IT systems): Article 145 § 3 1° of the Act of June 13th, 2005. This provision, going beyond telephone harassment, is very broad. It requires no complaint of the victim (as is the case for the crime of normal stalking contained in Article 442a CC) and it does not require that the tranquillity of the corresponding offender is effectively disrupted. Those different criteria for cyber stalking have been deemed constitutional by the Constitutional Court.[28] It has however been deemed unconstitutional by the Constitutional Court that, compared to the general crime of stalking contained in Article 442*bis* CC,

its penalties are higher, which amounts in the view of the Constitutional Court to a breach of the right to equality for those that are prosecuted under Article 145 § 3 1° of the Act of June 13, 2005.[29]

Child Pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Articles 383 and 383*bis* CC cover different aspects of the expression of pornography: Article 383*bis* only applies if child pornography makes use of "*emblems, objects, films, photos, slides or other visual media*", while child pornography using texts or simple sound recordings fall under the general description of pornography.

B. LEGISLATIVE TECHNIQUE

1. Specific problems with respect to the principle of legality

Interception of Conversations and Mails by Employer (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 314*bis* CC is based on the principle that the content of data may be controlled only if the employee and other parties concerned (e.g. the recipient of the message) have consented to it. Employers never applauded the principle. Convinced that the sheer fact that they were paying the company's telephone bill allowed them to have full discretion about the control on it and familiar with the American and British liberty for employers to control almost all aspects of workers privacy and also familiar with current technology enabling the monitoring of workers communications, they remained unwilling to respect legislation that forced them to look for alternatives with regard to electronic monitoring. Probably this attitude accounts for their willingness to exploit any vagueness that remained about the application of the said articles. There was for instance, some confusion whether an e-mail that *was* sent to, but not (still) read by the employee, was protected by Article 314*bis*, since this Article only protects communication in transmission. The Internet caused other areas of vagueness. Does the protection of the said Articles, only extend to communication between persons, or is a person visiting a website also protected? These questions triggered initiatives by the Data Protection Authority[30] and the Collective Labour Agreement no. 81 of April 26th, 2002 on the protection of the privacy of employees in the framework of the monitoring of electronic on-line communication data by employers drafted by the National Labour Council. Hence the discussion on the impact of this provision continued. Many commentators assumed that the said provision only protected against interception of emails during their transmission, not before or after. Before or after their transmission emails were said not to be protected by any criminal law provision. Recently, the Data Protection Authority published her cyber surveillance guidelines and advised that article 314*bis* CC does not apply to the control by an employer of e-mails stored on a hard disk of the employee.[31]

It took years before the issue was dealt with by the Courts, and up until today there has been no punishment of employers. In a 2005 judgement of the Labour Court of Appeal of Gent, the Court ruled that an employer may monitor his employees' Internet use, regardless of Article 314*bis* CC.[32] The Court found that Article 314*bis* did not apply because the employer only monitored the communication afterwards and not during the time the information was being transmitted.

The IT manager of a company was condemned for violating e-mail privacy on December 4th, 2007 by the Correctional Court of Leuven.[33] In 2000, the IT manager had logged into the company's network, accessed and read the directors' and personnel's e-mails, all from the comfort of his own home computer. Predictably, the company brought charges up against the It manager, when they discovered what had transpired. The Court ruled that e-mail messages themselves, their attachments, the term of address and the subject in the heading all constituted 'telecommunication data' protected by the Act of June 13th, 2005 on electronic communications (see above A.2.1: Attacks against IT systems). Article 124 of this

Act served as the basis of the IT manager's conviction, for violating the prohibitions of intentionally taking note of telecommunication data that are related to other persons.[34] The IT manager also tried to escape charges based on Article 314*bis* §1, 1°, which he did not successfully evade, by arguing that it did not apply as he had taken note of the e-mails only after they had already arrived on the e-mail server and not 'during the transmission'. The Court, however, did not endorse this interpretation. It opined that e-mails that have already arrived on the e-mail server but have not yet arrived in the addressee's e-mail box, e.g. because he/she did not yet activate his/her e-mail box, are still in transmission. The protection afforded by the article would be meaningless/rendered nugatory if 'during the transmission' were to be interpreted in such a restrictive way that it only includes the phase of sending the e-mail (the so-called transmission phase). Intercepting an e-mail during the transmission phase was also considered quasi impossible, as sending an e-mail takes only a few seconds.

In a judgement of September 2nd, 2008, the Labour Court of Appeal of Antwerp found that an employer who after having controlled the use of the Internet and of the mails sent by an employee, could lawfully dismiss this employee because of non-compliance with the company's IT policy.[35] The Court found that principles and procedures contained in the Collective Labour Agreement No. 81 on the use of electronic online communications had been respected by the employer. Furthermore, due to the fact that there was no wilful conduct and the employer had acted after the communication had taken place- and not during (the websites had already been visited and the e-mails were already stored in the e-mail box), the Court saw no violation of Article 314*bis* CC.

In another case brought before the Court of Appeal of Antwerp, Article 124 of the Electronic Communications Act of June 13th, 2005 was used as a basis to oppose the use of email content in its proceedings. In its judgement of September 6th, 2007, the Court of Appeals agreed that the controversial emails did indeed have to be excluded from the proceedings. Subsequently, the employer appealed to the Supreme Court, and argued that Article 124 only protects information relating to the transfer of an e-mail message such as the names of the correspondents, the moment of sending and its duration, whereas the content itself is not protected by the confidentiality of electronic communications.[36] The Supreme Court deemed it to be the contrary in a judgement of October 1st, 2009, on the confidentiality of electronic communications set forth in Article 124, 1° and 4° of the Electronic Communications Act of June 13th, 2005, which protects both the existence as well as the content of an e-mail. Article 124 was found to prohibit the interception and use of an email without the prior consent of the sender thereto. According to the Court, it is impossible to become acquainted with the content of e-mail without simultaneously becoming acquainted with the existence of that e-mail. Therefore, the Court ruled that Article 124 protected both equally the content of an e-mail and the information regarding the transfer of the e-mail.[37]

Identity Theft (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Because of the limited scope of Article 231 CC, a legislative proposal was submitted in the Senate on June 28th, 2006 aimed at the sanctioning of identity theft within the context of an electronic communications network. [38] The proposed Bill, that did not make it, sought to deter from all forms of identity theft within the context of electronic communications networks, including the instances of identity theft not only via

the Internet but also via phone and referred to similar initiatives taken in the United States (the Identity Theft Penalty Enhancement Act), the United Kingdom (the Fraud Bill) and France (Bill No. 452 introduced by senator Dreyfus-Schmidt). It recognized that the greatest risk was posed by identity theft for consumers in online transactions. Though some instances of identity theft may be indirectly sanctioned, i.e. via the existing Computer Crimes Act, the very act of identity theft itself, i.e. the actual gathering of identifying elements such as names, passwords, codes, etc. remained in impunity to date. In light of the limits of Article 231 CC, the proposal wanted to introduce a new article 231*bis* in the Criminal Code, sanctioning any person who on an electronic communications network, collects, the personal identification data of an individual, legal entity or governmental instance. The sanctions proposed are imprisonment for a period of between three and twelve months and a fine of between 250 and 15,000 EUR.

Press Crimes (See below B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation; C.4: Constitutional limitations to criminalising conduct with respect to ICT and internet crime): The right to freedom of expression and freedom of the press is shaped by the articles 19, 25 and 150 of the Constitution.[39] Article 19 refers to the freedom of expression in a broad technology neutral manner, Article 25 introduces the freedom of the press and Article 150 stipulates that 'press crimes' ['*drukpersmisdrijven' 'délits de presse*'][40] should be brought before a jury court (the '*Hof van Assisen*' of 'Cour d'Assises'). What a press crime is the Constitution does not say. In case law press crimes are traditionally defined as 'an offence that implies the expression of a thought or opinion in a published and printed written work' or 'an offence which has been committed by means of the press and which has been given a certain actual publicity and is an expression of opinion'.

Contrary to article 19, the articles 25 and 150 are not formulated in the same technology-neutral manner, as they use the word '*press*' or '*printing press*'. The Belgian courts seem reluctant to extend the specific freedom of the press to new information and communication technologies. This does not alter the fact that a more extensive interpretation of the concept 'press' has been advocated. The extension of this concept in article 25 leads to an extension of the competence of the '*Hof van Assisen*'. In the past almost no cases of 'press crimes' were brought before this court. Hence, *de facto*, an extension of the concept 'press crime' will lead to an extension of the criminal immunity.

It was unclear whether 'press crimes' could be applied to actions committed over the Internet. However, today more and more courts seem to accept that a press crime can be committed by way of the Internet.

Self-Regulation and Co-Regulation/Blocking orders (See below B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation; C.5: Criminal sanctions specifically targeting cyber criminals; G.1 Current trends of legislation and legal debate concerning ICT and internet crime): On December 19th, 2007, some members of Parliament introduced a proposal which aims at obliging ISPs to contractually impose netiquette and related sanctions on their customers.[41] The proposed Act, still under discussion, takes as a starting point that ISPs cannot sanction their customers if their conduct is inappropriate but not illegal. Following the Bill, ISPs are to include an acceptable use policy in their general terms and conditions, whereby it is agreed that certain types of inappropriate conduct will be sanctioned,

including the possibility for the ISP to block the customer's Internet access or even remove the customer's Internet access equipment.

Co-Regulation/Agreements with companies for traffic data exchange (See below: C.3.3 Obligation for providers to provide information on the identity of users): With regard to traffic data, Article 46bis of the Code of Criminal Procedure (CCP) describes the rules concerning the identification of electronic communication services and their users. On January 18th, 2011 the Supreme Court held that Yahoo Inc. is an electronic communication service within the meaning of Article 46bis CCP.[42] On September 4th, 2012 the Supreme Court held that Yahoo Inc., established in the US, must in accordance with Article 46*bis* § 2 CCP comply with requests for judicial cooperation issued by Belgian law enforcement agencies. The case has been referred to the Court of Appeal of Antwerp.[43]
It should be noted, however, that other companies like Microsoft, have voluntarily concluded agreements with Belgium for the exchange of traffic data.[44]

2. Avoidance by legislation of undue chilling effects on legitimate use of ICT or of the internet

Prosecutorial discretion (See below D.1: Role of criminal law in relation to other ways of combating abuse of ICT and the internet): There is no obligation in Belgian law to prosecute every time there are signs that an offence has been committed. The public prosecutor has the right to exercise prosecutorial discretion and he can decide not to prosecute when there is not sufficient evidence or when reasons of 'opportunity' dictate him or her not to prosecute. As has been pointed out by Koops, this principle of substantive law can be seen as a useful correction for criminal provisions that are formulated broadly, covering acts that may not in themselves be very worthy of criminal prosecution: "for example, changing without authorisation, a single bit in a computer already constitutes damage to data, "(...)", but will usually not be prosecuted".[45]

Immunities for providers: See below C.3.1 (Requirements of their liability, especially concerning mens rea).

3. Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation

E.g.,

- How are changes in the use of internet and social networks taken into account?
- How is the law adapted to technological progress (e.g., by reference to administrative regulations)?

By specific cybercrime legislation

The 2000 Computer Crime Act (See above A.6: Specific differences between the definition of cyber crimes and "traditional" crimes): the 2000 Computer Crime Act introduced new penal legislation concerning computer crimes in Belgium. The Act has introduced new provisions in the CC and the CCP. The Act uses the

term 'système informatique' [46] to indicate a computer system. This broad notion covers computers, PDAs, and chip cards, but also IT-related telecommunications systems and possibly also mobile phones.[47] No definition of a computer system is given in the law, but the parliamentary preparatory works state that it is every system for storage, processing or transmitting data. In this regard, the main focus was on computers, and smart cards, but the notion also denotes networks and their components as well as telecommunication systems or their components that use information technology.[48] The 2000 Computer Crime Act does not use the term 'computer data' but speaks of 'data that are being stored, processed or transferred by means of a computer-science system'.

Child pornography: Will be subject to imprisonment, ranging from a month to a year, any persons who knowingly possesses child pornography (Article 383bis § 2 CC). This Article has recently been amended and envisages now also the person who knowingly gives himself access to child pornography via a computer system or other technological means.[49]

Identity Theft (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Under B.1 (Specific problems with respect to the principle of legality) we referred to a legislative proposal aimed at the sanctioning of identity theft within the context of an electronic communications network, but that did not make it. In a recent report, the Working Group on Information Technology and Liberties of the Belgian Senate considers to propose new criminal legislation for online identity theft, including false profiles on Facebook.[50]

Preservation order (See below E.1: Laws or regulations obliging internet service providers to store user's personal data; G.1: Current trends of legislation and legal debate concerning ICT and internet crime): Article 14 of the Computer Crime Act changed Article 109*ter*, E of the Act of March 21st, 1991 concerning the reform of certain economic governmental companies (see above A.5: Extension of criminal liability in the area of ICT and internet to merely reckless or negligent conduct) and obliges the telecom-network operators and the providers of telecommunication-services to register and preserve traffic-data concerning the used telecommunication-means and the identification-data of the user of the telecommunication-services. This information must be preserved during a certain period of time to serve the tracing, investigation and prosecution of criminal offences. The Belgian law states that the obligation to preserve the mentioned data should be in accordance within the limits of the European Union but not less than 12 months. Article 109ter E has been replaced by Article 126 of the Act of June 13th 2005 on electronic communications (see above A.2.1: Attacks against IT systems) which will be further elaborated in a Royal Decree. Until now this Royal Decree has not seen the light. It will have to specify the following points: What is meant by traffic data? What identification-data has to be preserved? Where and how the information needs to be preserved? For how long will this information eventually be preserved? First drafts of a Decree are being discussed together with a proposed Royal Decree on the implementation of the Data Retention Directive (2006/24/ EC), but have received a negative opinion of the Belgian Data Protection Authority.[51]
The Belgian law states that the obligation to preserve the mentioned data should be in accordance within the limits of European law.

Netiquette (See above B.1: Specific problems with respect to the principle of legality): Under B.1 (Specific problems with respect to the principle of legality) we discussed a legislative proposal aimed at obliging ISPs to contractually impose netiquette and related sanctions on their customers.

By technologically neutral terms in the law

Child pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 383*bis* together with Article 380 and 379 CC apply to child pornography on the Internet. [52] Article 383*bis* CC is phrased in technologically neutral terms. Advertising for services of a sexual nature with reference to services offered by minors or persons claiming to so be, is reprimanded by article 380*ter*. Article 380*ter* sanctions advertising telecommunication services of a sexual nature. The Supreme Court in a case concerning hyperlinks to child pornography decided "*that the terms 'display and diffuse' mentioned in articles 379 and 380 CC concerning pornographic material relating to minors should also be understood as 'publishing a website with hyperlinks to such kind of material*".[53]

Racism (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Due to the technology neutrality of the provisions criminalising racism and holocaust these crimes apply even when the objectionable ideas are conveyed via the Internet or electronic means of communication.[54]

By a broad interpretation of traditional criminal law

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The difference with the general provision on fraud ('*oplichting*'/'*escroquerie*'), incriminated under Art. 496 CC, is that computer fraud concerns interference of a machine, while traditional fraud concerns manoeuvres that damage the faith of persons. Examples of computer fraud are the use of a stolen credit card to withdraw money from an ATM, exceeding the limit of one's own credit card without authorisation, manipulating bank accounts by a bank employee, and the misappropriating of profit of programs entrusted for a specific goal. The crime has a very broad scope; it might even cover the placing of durable cookies.[55] Another example given in this context is the act to demand or annul an internet connection or telecommunications connection using a false name or the name of somebody else.

Data and system interference: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

By the interpretation of the law by the courts

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): A judgement of the criminal court of Dendermonde deals with "skimming" (illegal copying of data from the magnetic strip of a card). The suspects fraudulently copied bankcard data entries in a computerized terminal of a bank transaction system and used a small camera to track passwords used by card owners. The criminal court classified these facts as computer fraud (Art. 504*quater* CC), computer forgery (Art. 210*bis* CC) *and* hacking (Art. 550*bis* CC).[56] With regard to hacking they were sentenced under Article

550*bis* § 1 and under Article 550*bis* § 3, 1 ° and 2° CC because they fraudulently copied bankcard data entries in a computerized terminal of a bank transaction system. The criminal court added that this conduct happened with the fraudulent intent to break into the computerized portfolio of third parties and appropriate the money on it.[57] Before the Computer Crime Act entered in force some judges used the crime of theft with the circumstance of the use of a false key[58] to sanction cases of unauthorized use a debit/credit card.[59]

A key case in Belgian law is the so called Redattack case. Nearing the end of 2001 this hacker was convicted and fined 1,000 EUR for, over the course of 1999, hacking into Fortis Bank's, Planet Internet's and Belgacom Skynet's websites.[60] At the time, Belgian legislation had yet to be adapted to combat this new kind of cybercrime and thus, classical criminal provisions were applied. The Computer Crime Act was enacted a short time after this highly publicized incident and it entered into force on 13 February 2001. Another criminal complaint was filed by various companies against the same person for other hacking activity on 12 April 2001. This time, the suspect was accused of breaking into five different company websites, and leaving a hyperlink to a separate hacker tool website which was attributed to him. Despite Redattack's allegation that the entire plot was orchestrated by envious hackers, forensic experts were able to prove that his computers left traces on the hacked websites, although he had tried to erase his tracks. The Criminal Court of Ghent found him liable under the new Act, on December 1st, 2003, and he was sentenced to a conditional term of imprisonment of one year and a fine of 14,873 EUR.[61]

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): In 2008, the Court of appeal of Antwerp decided that the use of a credit card belonging to a company by an employee to carry out personal purchases is computer fraud. [62]

Press crimes (See above B.1: Specific problems with respect to the principle of legality): It was unclear whether 'press crimes' could be applied to actions committed over the Internet. However, today more and more courts seem to accept that a press crime can be committed by way of the Internet,[63] and this was confirmed by the Supreme Court in two judgments of March 6th, 2012.[64]

Hence, in 2004 defamation on a website was qualified as a press crime by the Court of First Instance of Brussels.[65] The same Court in 2009 equally saw a press crime in the act of posting defamatory comments below an online video.[66] We underline that the result of this is that when a normal criminal court qualifies certain facts as a press crime, then it has to declare itself incompetent to adjudicate the case as, according to Article 150 of the Constitution, only the jury Court ('*Cour d'Assises*') is competent to adjudicate such cases. Press crimes also warrant relatively short periods of prescription. This is what happened in a case brought before the Court of Appeal of Mons and judged in 2008.[67] In this case on a blog written about an incident with passenger inspections on train, the Court ruled that the process of multiplying a blogged article through a website is comparable to the process of reproducing it through classic paper printing. The Court decided that, though, the blog is not printed paper work and its reproduction does not depend on the process of classic paper printing, its reproduction is unlimited as it can be consulted by any surfer on the Internet. The printing of the article

is an option for all users. Also they all can pass it on to others. Therefore, the Court broadly interpreted the classical definition of press crimes to include this group of online, forum "publication", accessible to any Internet user at any time. Consequently, the Court declared it incompetent as it qualified the facts as a press crime.

This evolution has also positive consequences for website editor. Article 25 of the Constitution sets forth a gradual liability regime, making a publisher liable only if the author of the content concerned is not domiciled in Belgium. By bringing online publications under the 'normal' constitutional framework for writings and freedom of expression, this liability scheme expands. In a judgement of June 23rd, 2009 the Criminal Court of Brussels found that online publications can qualify as a press crime and that the related gradual liability regime set forth in Article 25 of the Constitution thus also applies to online publications. According to this gradual liability regime, a website editor is liable only if the author of the content concerned is not domiciled in Belgium.[68] The Court also found that a webmaster who undertakes work of a purely technical nature is not liable for a press crime on the website if the website editor can be identified and is domiciled in Belgium.

Liability of Internet Service Providers/Child pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law; A.4: Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims): The Supreme Court has in a judgement of 2004,[69] regarding a website containing hyperlinks to other websites showing child pornography, clarified the legal grounds of liability exclusion for service providers. The Court of Appeal of Antwerp convicted the website owner under articles 379 and 380 CC, for possession and diffusion via the Internet of pornographic material regarding minors. This interpretation of the E-Commerce Act (see below C.3.1: Requirements of their liability, especially concerning mens rea) as well as the broad application of the child pornography provisions were upheld by the Supreme Court. In this scenario because, the person did more than just provide an information society service that consisted of the transmission in a communication network of information provided by a recipient of the service or more than just giving access to a communication network, the liability exemption for conduit activities did not apply. Nor did the liability exemption under article 20 § 1 of the E-commerce Act, as it had been proved that, he had personally provided passwords to applicants to publish and activate explicit hyperlinks, of which he had previous knowledge of their content.

Liability of Internet Service Providers/Racism (See above A.1: Specific legal interests deemed to be in need of protection by criminal law; A.4: Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims): Two administrators were convicted for inciting hatred and violence against the Jewish people in a judgement of January 23rd, 2009, by the Brussels Court of Appeal. As administrators of the forum both individuals were in charge of the daily management of its content, and several articles and videos with a Zionist, racist and xenophobic content were posted.[70] The two administrators were found to have infringed the Anti-Racism and Anti-Xenophobia Act of July 30rd, 1981, as they diffused Zionist, racist and xenophobic articles and videos with full knowledge of the content thereof. Furthermore, the Court found that the liability exemption set forth in the E-Commerce Act of March 11th, 2003 did not apply (see below C.3.1: Requirements of their liability, especially concerning mens rea). If the administrator is the co-

author or the accomplice of the internet user who posts an article or video on the administrator's online forum, then the forum administrator will be held criminally liable. Furthermore the Court ruled that, to be considered the author of a criminally infringing publication on an online discussion forum, the administrator himself must have posted or diffused the unlawful messages and acted as the author thereof or if he keeps the unlawful messages available on his forum with full knowledge of the content thereof; or modifies an existing message in such a way that makes it unlawful.

This case law together with the expanding case law on press crimes (see above B.1: Specific problems with respect to the principle of legality) is of a nature to put to alert responsible editors of newspapers and websites. In a judgement on the topic of press crimes, the Criminal Court of Brussels on 27 November 2009 found that online publications can qualify as a press crimes and that the person responsible for a website or journal can be held liable for content of which the authors are unknown and this under the gradual liability regime for press crimes set forth in Article 25 of the Constitution.[71]

C. EXTENT OF CRIMINALISATION

1. Criminal laws covering mere preparatory acts that carry a risk of furthering abuse

- e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection?

See above A.5 (Extension of criminal liability in the area of ICT and internet to merely reckless or negligent conduct).

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 550*bis* CC also contains a series of additional incriminations with regard to preparatory acts. Article 550*bis* § 5 punishes those that with fraudulent intent or purpose to injure, research, collects, provides, distributes or sells hacker tools. Incriminations that regard preparatory acts target trade in hacker and access tools (Art. 550*bis* § 5 CC) and allow sanctioning the use of these tools and the diffusion of passwords of access. Article 5 of the Computer Crime Act of May 15th, 2006 has amended Article 550*bis*, § 5 CC and now punishes he "who wrongfully possesses, manufactures, sells, obtains for its use, imports, distribution or makes available in another form, any device, including data, primarily designed or adapted for the purpose of committing Computer Crimes" with an "imprisonment of six months to three years and a fine of twenty-six euros a hundred thousand Euro or either of these penalties". The term "device" denotes means of access or other tools designed, for example, to alter or destroy data, or to interfere in the functioning of systems, such as virus programs, or also programs designed to access to computer systems.[72]

Illegal interception (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Equally punishable is the placing of any device with the intention of interception (article 314*bis* CC). Article 314*bis* § 2bis CC punishes with "imprisonment of six months to a year and a fine of two hundred euro to ten thousand euro or either of these penalties", "those who wrongfully possesses, manufactures, sell, obtain in view of using, import, distribute or make available in another form a device, including data, primarily designed or adapted to enable" the illegal interception of communications and telecommunications.

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 550*ter* § 4 CC now punishes whoever wrongfully possesses, manufactures, sells, obtains for its use, imports, distributes or makes available in another form, a system including data, primarily designed or adapted for the purpose of committing offences under the §§ 1 to 3, knowing that these data can be used to cause damage to data or prevent, totally or partially correct functioning of a computer system.

Spamming or stalking: See above A.1 (Specific legal interests deemed to be in need of protection by criminal law).

Privacy (or "data protection") Offences (See above A.2.1: Attacks against IT-systems): The Act of June 30th, 1994 on the legal protection of computer programs[73] introduced a specific sanction in Article 11 §1 which foresees an imprisonment of three months to three years and a fine from 100 to 100.000 euros for those that put in circulation or which, for commercial purposes, hold a copy of a computer program knowing it is illicit or having reasons to believe it, as those which put in circulation or hold for commercial purposes any means having for only goal to facilitate the not - authorized suppression or the neutralization of the technical devices which protect the computer program. In case of recidivism, the maximum of the incurred penalty is carried to the double.

Act of June 13th 2005 on electronic communications (See above A.2.1: Attacks against IT-systems): Article 145 §1 of the Act of June, 13th 2005 on electronic communications also criminalizes the keeping and selling of equipment or related software that does not meet certain conditions of the Act, mainly with regard to security (Articles 32, 33, 35, 114 and 127 of the Act). Article 145 §3 of the Act criminalizes the setting up of installations aimed at the creation with fraudulent intent of electronic communications via an electronic communication network in order to provide for oneself or another a fraudulent profit, or aimed at causing nuisance or harm to a correspondent via an electronic communication network, via an electronic communication service or via other electronic communication methods.

- If so, has there been controversy about introducing such laws?
- Have legislatures made specific efforts to avoid over-criminalization?

No.

2. Criminalization of the mere possession of certain data

- In what areas, and on what grounds?
- How is "possession" of data defined?
- Does the definition include temporary possession or mere viewing?

See above A.5 (Extension of criminal liability in the area of ICT and internet to merely reckless or negligent conduct).

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Incriminations that regard the consequences of hacking target taking knowledge of hacked data (Art. 550*bis* § 3, 1 ° CC), keeping, using, selling or making public hacked data (Art. 550*bi*s § 7 CC). Receiving hacked data is thus also penalised (Article 550*bis* § 7 CC): if someone holds data that he knows have been acquired by hacking, or if he publishes or distributes such data, he is punishable with 6 months' to 3 years' imprisonment.

Article 5 of the Computer Crime Act of May 15th, 2006 has amended Article 550*bis*, § 5 CC and now punishes he "who wrongfully possesses, manufactures, sells, obtains for its use, imports, distribution or makes available in another form, any device, including data, primarily designed or adapted for the purpose of committing Computer Crimes".

Illegal interception (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Also punishable is someone who knowingly keeps, discloses, distributes or uses the contents of illegally intercepted private communications or telecommunications (Art. 314*bis* CC).
Article 314*bis* § 2bis CC punishes with "imprisonment of six months to a year and a fine of two hundred euro to ten thousand euro or either of these penalties", "those who wrongfully possesses, manufactures, sell, obtain in view of using, import, distribute or make available in another form a device, including data, primarily designed or adapted to enable" the illegal interception of communications and telecommunications.

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 550*ter* § 4 CC now punishes whoever wrongfully possesses, manufactures, sells, obtains for its use, imports, distributes or makes available in another form, a system including data, primarily designed or adapted for the purpose of committing offences under the §§ 1 to 3, knowing that these data can be used to cause damage to data or prevent, totally or partially correct functioning of a computer system.

Child pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): In general, Belgian law does not prohibit pornography,[74] however, regarding its distribution, Article 383 CC penalises public indecency and immorality. This provision applies to "songs, pamphlets or other written articles, whether printed or not, and figures or images contrary to morality." Regardless of the medium carrying the material, whether it is a question of illustrations, videos, CDs or the Internet, the provision applies to all texts as well as images or sounds. The advertising and/or distribution of child pornography material aimed at minors or alluding to services offered by minors is reprimanded by article 383*bis* CC originally introduced by the law of March 27th, 1995[75] and subsequently modified by the Law on the Penal Protection of the Minors of November 28th, 2000[76]. In this respect, a minor is considered to be a person under the age of 18. This concerns, any image carrier that depicts pornographic acts in which a minor is shown or represented, which has been displayed, sold, rented, disseminated, broadcasted or delivered, which is subject to a penalty of 5 to 10 years imprisonment (Article 383*bis* § 1CC). The penalty increases to 10 to 15 years (Article 383*bis* § 3 CC) if the litigious activities take place within an association.[77]
Will be subject to imprisonment, ranging from a month to a year, any persons who knowingly possesses child pornography (Article 383bis § 2 CC). This Article has recently been amended and envisages now also the person who knowingly gives himself access to child pornography via a computer system or other technological means.[78] This seems to include the intentional viewing of child pornography, in line with existing case law of the Supreme Court.[79]
What is prohibited are materials showing minors in sexual positions or acts of a pornographic nature. The scope of this article used to be limited to minors under the age of 16, but this was repealed in 2000.

The actual involvement of a minor is secondary, what counts, is that the images suggest the presence of a minor. The incrimination potentially also applies to computer-generated drawings or illustrations.
As technology operates at present, looking at data on the Internet always requires the creation of a local copy of the data on your computer. This copy can exist in the random access memory, on the hard disk or on both. Hence, at least a temporary possession is implied by simply looking at child pornography.
This temporary copy is, however, generally created in an unintentional manner without the user being aware of it. In this way, the person concerned does not intend to possess child pornography, whereas it is required under article 383*bis* that Internet users "*knowingly*" possess child pornography. This entails that temporary and purely technical storage cannot be considered punishable possession[80]. Therefore, any person who should accidentally stumble across child pornography on the Internet and unwittingly makes a copy of it is not punishable.[81]
When a copy is knowingly created, the situation is entirely other. For example, this is the case, regarding child pornography that has been knowingly downloaded. The deliberate storage of this type of graphic material automatically entails its possession and is therefore punishable under Article 383*bis*. The above-mentioned amendment of Article 383bis § 2 CC seems to confirm this. The sentence fixed is that of imprisonment (between a month and a year) and a fine of 500 to 5,000 Euros.

Racism (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Provisions criminalising racism and holocaust denial can be found in the (reformed) Act July 30th, 1981 to suppress certain acts inspired by racism and xenophobia, [82] or the Act of March 23rd, 1995 prohibiting the denial, minimization, justification or approval of genocide committed by the German National Socialism regime during the Second World War.[83] The Act of 1981, the Anti-Racism Act, punishes amongst others incitement to discrimination, hatred or violence against a person or a group on account of race, colour, origin or national or ethnic descent, in the circumstances given in Article 444 CC. The circumstances given in Article 444 CC are as follows: either in public meetings or places; or in the presence of several people, in a place that is not public but accessible to a number of people who are entitled to meet or visit there; or in any place in the presence of the offended person and in front of witnesses; or through documents, printed or otherwise, illustrations or symbols that have been displayed, distributed, sold, offered for sale, or publicly exhibited; or finally by documents that have not been made public but which have been sent or communicated to several people.

Privacy (or "data protection") Offences: See above A.2.1 (Attacks against IT-systems).

Act of June 13th 2005 on electronic communications: See above A.2.1 (Attacks against IT-systems).

3. Extension of criminal liability to service providers e.g., hosting or access providers

See above A.4 (Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims).

3.1 Requirements of their liability, especially concerning mens rea

Liability of Internet Service Providers (See below D.2: Non-criminal means of combating offensive websites used/propagated): The question of liability of Internet service providers is dealt with by the two E-Commerce Acts of March 11, 2003: the Act on Certain Legal Aspects of the Information Society Services[84] and the Act on Certain Legal Aspects of Information Society Services as defined in Article 77 of the Constitution.[85] Article 18 of the Act on Certain Legal Aspects of Services in the Information Society Service states that an internet service provider (ISP) is not held liable, when it acts as merely as conduit or provides caching and hosting activities.

First, mere conduit; in this case an ISP cannot be held liable for any such activities (e.g., transmitting information or providing access to a communications network), as long as the ISP does not initiate the transmission; select the recipient of the transmission; or select or modify the transmitted information.

Provided that the information is stored for no longer than is reasonably necessary to do so, this exception will encapsulate the automatic, intermediate and temporary storage of information for the sole purpose of carrying out a transmission.

Second, catching. Article 19 of the Act releases the provider from any liability in catching activities for the automatic, intermediate and temporary storage of information for the sole purpose of making the transmission of that information more efficient provided certain conditions. In this respect the ISP may not modify the information, it must comply with the conditions on access to the information, comply with the rules regarding the updating of the information specified in a manner recognized and used by industry; does not interfere with the lawful use of technology, widely recognized and used by industry to obtain data on the use of the information; and acts expeditiously to remove or disable access to the information upon obtaining actual knowledge that the initial source of the information has been removed or access to it has been disabled, possibly by order of a court or an administrative authority.

Third, hosting activities. Article 20, ISPs are not held responsible provided that they: (i) do not possess actual knowledge of any illegal activity or information and, as regards claims for damages, are unaware of any facts or circumstances from which illegal activity or information is apparent; and (ii) act expeditiously to remove or disable access to the information, upon obtaining such knowledge or becoming aware of such activity, As with caching activities, the act obliges the ISP to notify and collaborate with the public prosecutor.

Liability of Providers of Electronic Payment: The Act of July 17th, 2002 on the electronic transfers of funds, -which transposes into Belgian law the European Recommendation 97/489/EC of July 30th, 1997 -, contains specific rules with regard to the sharing of responsibility sharing between the issuer and the holder of the instrument of Electronic funds transfer in case of misuse of it. The regulation targets both payments made through cards as payment via the Internet or the telephone.[86] This Act was recently repealed by the Act of December 10th, 2009 on the services of payment[87] which lays down again more or less the same rules in its articles 36 and 37**.**

3.2 Obligation for providers to monitor and control what information they provide or offer access to

Liability of Internet Service Providers: ISPs do not have a general duty to monitor the information they transmit or store, nor actively to investigate facts or circumstances indicating illegal activity. This is confirmed by article 21 of the E-Commerce Acts (see above C.3.1: Requirements of their liability, especially concerning mens rea).

3.3 Obligation for providers to provide information on the identity of users

Liability of Internet Service Providers: The Act on Certain Legal Aspects of Information Society Services (see above C.3.1: Requirements of their liability, especially concerning mens rea) allows the judicial authorities to order a temporary surveillance period in specific cases, going beyond the requirements of the directive, provided this is expressly allowed by statute.

A faithful transposition of the requirements of the E-commerce Directive (2000/31/EC) is far exceeded however, by the E-Commerce Acts. Illegal content is to be reported to the public prosecutor by the responsible authorities, the former may then order the seizure of the alleged illegal data. (e.g., a computer virus). The law refers to the power of the public prosecutor in application of Art. 39*bis* CCP to order its destruction, while safeguarding a copy for instructional purposes, if the data infringes public order, affronts public decency (e.g., child pornography, see above A.1: Specific legal interests deemed to be in need of protection by criminal law) or presents a danger to the integrity of networks or data. The ISP may only disable access to the information, and may not destroy or delete it, as long as the public prosecutor has not reached a decision on the matter.

Following Article 21(2) ISPs have the obligation to notify promptly the competent judicial or administrative authorities of any alleged illegal activities committed or information provided by their customers, and they are to communicate information enabling the identification of these customers to the authorities. In the original wordings, they had to notify promptly the competent judicial or administrative authorities of any alleged illegal activities committed or information provided by their customers, and to communicate to the authorities information enabling the identification of these customers. Article 21 has been altered by Article 59 of the Programme Act of July 20th, 2005.[88] Under the new Article, however, they have to supply the authorities, at their request, with all information about their users that they have at their disposal and that helps the search for unlawful acts committed by the users' intervention.

User and Traffic Data (See above B.1: Specific problems with respect to the principle of legality): With regard to traffic data,[89] Article 46*bis* CCP describes the rules concerning the identification of telecommunication services. During the investigation of criminal offences the public prosecutor can make a motivated requisition in writing to a telecom-operator to make them identify the subscriber or user of a telecommunication service and to provide all information concerning the identification-data for certain telecommunication services on which a specific person has been a subscriber or user. It will be noted

that the legislator took care to envisage the possibility of creating a legal obligation for each operator of a telecommunication network and each provider of a telecommunication service to assist in the execution of the order issued by the Public ministry or the investigative judge and to communicate the necessary data within a time fixed by Royal decree.[90] Each and every person who has to co-operate consequently has to keep secrecy about the measures taken.

3.4 Obligation for providers to prevent access to certain information

- If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

Liability of Internet Service Providers (see above C.3.1: Requirements of their liability, especially concerning mens rea): Illegal content is to be reported to the public prosecutor by the responsible authorities, the former may then order the seizure of the alleged illegal data. (e.g., a computer virus). The law refers to the power of the public prosecutor in application of Art. 39*bis* CCP to order its destruction, while safeguarding a copy for instructional purposes, if the data infringes public order, affronts public decency (e.g., child pornography) or presents a danger to the integrity of networks or data. The ISP may only disable access to the information, and may not destroy or delete it, as long as the public prosecutor has not reached a decision on the matter.

Costs (See above A.2.1: Attacks against IT-systems): Article 127 §1 of the Act of June 13th, 2005 on electronic communications empowers the King to determine the remuneration of the provider's costs. An annex to the Royal Decree of February 8th, 2011 regarding the legal duty to cooperate with judicial requests regarding electronic communication[91] introduced fixed rates for certain measures. For non-listed measures, like the prevention of access to certain information, actual costs are reimbursed.

4. Constitutional limits to criminalising conduct with respect to ICT and internet crime

- e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements?

Freedom of expression, freedom of the press: See above B.1 (Specific problems with respect to the principle of legality).

Freedom of association: The freedom of association might play a future role with regard to peer-to-peer networks. Case law in France already considers such networks as associations.

Mens rea requirements: see above A.5 (Extension of criminal liability in the area of ICT and internet to merely reckless or negligent conduct).

Refusing a request for assistance in criminal matters: The Act of December 9th, 2004 on International Mutual Legal Assistance in Criminal Matters, which came into force on January 3rd, 2005, governs the grounds for refusing a request for assistance in a criminal matter which falls outside the scope of an international legal instrument on mutual legal assistance between Belgium and the requesting State. Harming "Belgium's essential interests", is the main reason provided for denying a request.

5. Criminal sanctions specifically targeting cyber criminals

- e.g., a temporary ban from using the internet?

Self-Regulation and Co-Regulation: See above B.1 (Specific problems with respect to the principle of legality).

D. ALTERNATIVES TO CRIMINALISATION

1. Role of criminal law in relation to other ways of combatting abuse of ICT and the internet

- Relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT

Criminal settlement (see above B.2: Avoidance by legislation of undue chilling effects on legitimate use of ICT or of the internet): Public prosecutors are free to decide against commencing proceedings even when the facts show that all the elements of an offence are present (Art. 28*quater* CCP).[92] Instead of prosecuting, they can also propose a criminal settlement, an out-of-court procedure whereby the prosecutor does not prosecute in exchange for the advanced payment of a sum of money by the alleged offender. This type of criminal settlement is not a punishment nor does it appear in the police records. Before the Acts of April 14th, 2011 and of July 11th, 2011[93] it remained a possibility for all offences punishable by a fine, a term of imprisonment of no more than five years, or both – the computer crime offences listed in this questionnaire generally fall into these categories.[94] Following a combined reading of the Acts of April 14th, 2011 and of July 11th, 2011 it is also possible for offences which are punishable by a term of imprisonment of more than five years, but according to the public prosecutor would be punished at the end of the procedure by a term of imprisonment of no more than two years.
At the end of 2011, the federal prosecutor successfully proposed a criminal settlement of €150.000 to Google because the unintentional interception of communication data from non-secured WiFi-networks by Google Street View-cars violated the Act of June 13th, 2005 on electronic communications (see above A.2.1: Attacks against IT systems; see below D.3: Self-protection by ICT users).[95]

Online Gambling (See above 2.6: Other innovative criminal prohibitions in the area of ICT and internet): Another novelty is that the Gambling Commission is entitled to impose administrative fines instead of public prosecution when the public prosecutor chooses not to pursue a violation of the Act.

2. Non-criminal means of combatting offensive websites used/propagated

- e.g., closing down websites, blocking access to websites?

Obligatory Blocking Orders Against Internet Providers:

1. Article 2 §4, 5 and 6 of the second E-Commerce Act of March 13th, 2003, the *Act on Certain Legal Aspects of Information Society Services as defined in Article 77 of the* Constitution, allows the Brussels investigative judge to order certain providers to block their services (see above C.3.1: Requirements of their liability, especially concerning mens rea). When there is a danger for public health, public safety, national security and national defence and for consumer interest, the Investigating Judge can, when he is called to do so by certain authorities[96] turn to a Belgian provider and ask the blocking of certain services provided for by firms in other EU countries, when the Belgian providers are able to do

so. The order can be given for one month. The judge may extend one or more effects of its order and must terminate it as soon as the circumstances which justified the order change.

2. Article 39*bis* § 3 CCP allows the Prosecutor to use all technical means to make data inaccessible that "are the subject of the offence or have been produced by the offence and if they are contrary to public order or good morals or constitute a danger to the integrity of computer systems or data stored, processed or transmitted through such system". This power is, for example, used by prosecutors to impose an ISP to delete from their copy of DNS (Domain Name Server) the domain name of a site that violates the law, such a site distributing child pornography (See above A.1: Specific legal interests deemed to be in need of protection by criminal law).

3. The new Act of 2010 on gambling, updating the 1999 Act in view of gambling on the Internet services, provides a similar mechanism but an administrative decision of the Commission on Gambling.[97] Gambling games on the Internet can now legally be held, but only by legal institutions holding the same type of games "in the real world." The Commission on Gambling has the power to order to access providers to block access to illegal sites. The law is now also applicable to "game media" (primarily television sets). (See above: 2.6. Other innovative criminal prohibitions in the area of ICT and internet).

Privacy (or "data protection") Offences: See above A.2.1 (Attacks against IT systems).

3. Self-protection by ICT users

- e.g., by encryption of messages, using passwords, using protective software?
- Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password?
- Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

There are no sanctions for a lack of reasonable self-protection. Yet, Luc Beirens, Head of the Federal Computer Crime Unit (FCCU) at the Federal Judicial Police, allocates responsibility to ICT users to use protective software like antivirus software and firewalls.[98]

In civil proceedings, the lack of reasonable self-protection can provide a defense. In criminal proceedings, however, it is very unlikely for a defendant to successfully raise (the prohibition of) provocation resulting from a lack of reasonable self-protection. This shows from the above-mentioned Google Street View-case in which the even unintentional interception of communication data from non-secured WiFi-networks by Google Street View-cars violated the Act of June 13th, 2005 on electronic communications (see above A.2.1: Attacks against IT systems; D.1 Role of criminal law in relation to other ways of combating abuse of ICT and the internet).

E. LIMITING ANONYMITY

1. Laws or regulations obliging internet service providers to store users' personal data

Preservation orders: See above B.3 (Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation).

➢ Obligation for providers to provide such data to law enforcement agencies

Liability of Internet Service Providers/User and Traffic Data: See above A.4 (Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims).

2. Laws or regulations obliging an internet service provider to register users prior to providing services

No. Yet, as discussed above (A.2.5: Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities), users that create an email account in the name of someone else can be found guilty on the charge of having committed 'computer forgery' as set forth in Article 210bis CC.

3. Laws or regulations limiting the encryption of files and messages on the internet

➢ Can suspects be forced to disclose passwords they use?

No. The use of encryption is free according to Article 48 of the Act of June 13th, 2005 on electronic communications (see above A.2.1: Attacks against IT systems). Article 88quater CCP allows the public prosecutor to impose the obligation to certain individuals to co-operate during an investigation. These individuals are described as persons whom the Investigative Judge thinks they have special capacities concerning the computer system, which has been the object of an investigation, or of services used to store, process, encrypt or transfer data. This production order or obligation to co-operate cannot be given to a suspect (nemo tenetur principle).

F. INTERNATIONALISATION

1. Application of domestic law to data entered into the internet abroad

- Requirement of "double criminality" with respect to entering data from abroad?

Extra Territorial Jurisdiction: Next to the crimes committed on Belgian territory, the Belgian courts also have the competence to judge (under certain conditions) about offences, which were committed abroad.[99] Article 4 CC states that crimes committed outside Belgian territory by nationals or foreigners are not punishable unless in cases determined by law. These cases are laid out in article 6-14 of the preliminary title of the CCP. The jurisdiction of the Belgian courts over crimes committed abroad can be based on different basics: the Belgian nationality of the offender (active personal jurisdiction), the Belgian nationality of the victim of a crime (passive personal jurisdiction), the protection of the Belgian state (protective principle) and the international character of a crime (universal jurisdiction).[100]

The requirements for Belgian jurisdiction based on the principle of "active personal jurisdiction" are contained in Article 7 of the preliminary title of the CCP. Belgian criminal law applies, to crimes and offences committed outside the Kingdom by Belgian nationals and any person having his principal place of residence in Belgium, when the facts are punishable both under Belgium law and the law of the place where the crime is committed (art. 7, §1)

This requirement of dual criminality in respect of acts committed abroad (i.e., the act must be a criminal offence in the place where it was committed as well as in Belgium), is complemented in Article 7 §2 of the preliminary title of the CCP with a second requirement in cases where the crimes were committed against foreigners: in these cases the prosecution is reserved to the public prosecutor,[101] and requires either a prior complaint by the victim or an official opinion given to the Belgian authorities by the authorities in the country where the offence took place.

Prosecution of human trafficking and sex tourism abroad on the basis of universal jurisdiction is made possible by Article 10*ter* of the preliminary title of the CCP.[102] This provision was inserted in the CCP by article 8 of the Act of April 13th, 1995 concerning the suppression of human trafficking and child pornography and subsequently amended by the article 34 of the Act of November 28th, 2000 on Protection of Minors by Criminal Law and article 23 of the Act of August, 10th, 2005 amending several provisions with a view to the strengthening of the fight against human trafficking and smuggling. Double incrimination is not requested in order to prosecute a person who committed one of these crimes outside Belgium. The presence in Belgium of the person who is accused of it, however, is obligatory (art. *10ter juncto* 12 of the preliminary title of the CCP)[103].

A law of February, 6th 2012 added to the exceptions of this presence requirement very serious crimes as manslaughter and infanticide.

International net searches (See below G.1: Current trends of legislation and legal debate concerning ICT and internet crime): When the investigative judge commands a search of a computer system or part of it, this search can be expanded to an interconnected system that is situated in another place than the place where

the search has been conducted (Article 88*ter*, §1 CCP):
- If the expansion of the search is necessary to bring the truth concerning the investigated offence to the surface;
- If other measures would be disproportional or if there is a risk that without expanding the search, evidence would disappear or be lost.

This expansion of the search in an information science system is limited to those systems, area's or parts of it that the rightful operators are allowed to use or have specific access to (Article 88*ter*, §2 CCP).

However once those conditions taken into account there is no geographical limit to the search. The provisions are very clear: when the data are not situated on Belgian territory only copying is allowed. In that case the investigative judge reports immediately the extra-territorial search to the Minister of Justice, who will consequently inform the competent authority of the related State. Indeed, when the data found during the search are needed to carry the investigation further, the rules provided for in Article 39*bis* CCP apply. The investigative judge informs the responsible person for the remote system of the search, unless his identity or his address cannot be discovered (Article 88*ter*, § 3 CCP).

This possibility to search at least virtually abroad goes much further than the provisions of the Cybercrime Convention,[104] that only speak about this possibility in case of open sources on the Internet or with the consent of the user of the computer [105]. When elaborating the law, the Council of State already reminded that, for the European Council, "*as concerning the data stored in another member State (…), most of the member States tend to consider a cross-border search on the web carried out by the competent authorities entrusted with the inquiry without the authorization of the competent authorities to be a violation of their sovereignty and of international law*".[106]

2. Influence of international legal instruments on criminal law in the area of ICT and internet

Computer Crime Act of 2000 (See above A.6: Specific differences between the definition of cyber crimes and "traditional" crimes): The provisions introduced by the Computer Crime Act of 2000 have seen a single update of scale[107] with the Act of May 15th, 2006 amending Articles 259bis, 314bis, 504quater, 550ter and 550bis of the Penal Code.[108] The aim of this law is to put Belgian law in compliance with the Convention of the Council of Europe Convention on Cybercrime, signed in Budapest, November 23rd, 2001[109] and its Additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through Computer Systems, signed in Strasbourg, January 28th, 2003 and also with the EU Framework Decision 2005/222/JHA on attacks against information systems. The EU Framework Decision 2005/222/JHA on attacks against information systems is legally binding for Belgium even without ratification. Belgium has signed the Cybercrime Convention and the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts, but it has only ratified the first text (see below G.1: Current trends of legislation and legal debate concerning ICT and internet crime). It has also signed but not yet ratified the Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201). The reasons for the delay in ratification are not clear.

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The new Article 550*bis*, § 5 CC is much more faithful to Article 6.1a, 1° of the Cyber Convention by addressing not only hacking 'data' but also hacking 'devices'.

Illegal interception (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 2 and 3 of the Computer Crime Act of May 15th, 2006 complement Article 259*bis* CC and Article 314*bis* CC, again as a reaction to the provisions with regard to "misuse of devices" in the Cyber Crime Convention. The Belgian legislator in 2006 was of the opinion that Belgian law lacked incriminations to combat use of devices and data with the purpose of carrying out illegal interceptions.[110]

Computer fraud (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Article 4 of the Computer Crime Act of May 15th, 2006 does away with the vague and confusing term ' deceptive profit' in Article 504*quater* CC. The main consequence of this change, prompted by Article 8 of the Cybercrime Convention, is that for the crime to apply it is not necessary to have acquired a financial gain. It is enough to act with the intention to obtain gain. [111]

Data and system interference (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Again, like with *hacking* (Article 550*bis* CC), we see in the first and fourth paragraph of Article 550*ter* CC a more faithful phrasing, made necessary by Article 6.1a,1° to the Cybercrime Convention, and obliging the Belgian legislator to address not only data and system interference using 'data' but also using 'devices'.[112] The list of incriminated actions in the fourth paragraph is longer compared to the original and is again more in line with the Cybercrime Convention. The incrimination of attempt in the sixth paragraph was made necessary by Article 11 of the Cybercrime convention and by Article 5 of the EU Framework Decision of the Council of the European Union on attacks against information systems that requires the criminalization of attempts to undermine the integrity of data.[113]

Infringements of Copyright and Related Rights (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): The Belgian Copyright Act of June 30th, 1994 was amended by the act of May 22nd, 2005,[114] which transposed the EU Copyright Directive.[115] The reform is a faithful copy of this Directive. The new Act introduces *inter alia* an exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction, an exclusive distribution right and an exclusive right of communication to the public for interactive on-demand distribution. Article 79*bis* implements article 6(1)-(3) of the Directive. The protection of the databases and the right of the producers of the databases is regulated by the Act of August 31st, 1998 which transposes the European directive from March 11th, 1996 on the juridical protection of databases.[116] This law foresees criminal sanctions for fraudulent or malicious breach of rights or the name of the producer of the databases.

Liability of Providers of Electronic Payment (See above A.4: Limitation of criminal liability for certain cyber crime to particular groups of perpetrators and/or victims): The Act of July 17th, 2002 on the electronic transfers of

funds, -which transposes into Belgian law the European Recommendation 97/489/EC of July 30th, 1997.

3. Participation of Belgium in discussions about the harmonisation of cybercrime legislation

United Nations

UN intergovernmental expert group on cybercrime

International Telecommunication Union

Global Cybercrime agenda

Council of Europe

Cybercrime Convention

European Union

- EU- US Working Group on Cybersecurity and Cybercrime
- Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA[117]

G. FUTURE DEVELOPMENTS

1. Current trends of legislation and legal debate concerning ICT and internet crime

Hacking (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Some reforms are indispensable because of the on-going technical progress. From the perspective of the prosecution there are demands for more powers to 'hack' into systems to be able to respond adequately to frequent use of encryption and of communications in 'voice over IP' (VoIP).

Ratification of Conventions: Belgium, though amongst the first countries to sign the Cybercrime Convention and the Additional Protocol to the Cybercrime Convention on racist and xenophobic acts, waited until August 20th 2012 to ratify the first text (see above F.2: Influence of international legal instruments on criminal law in the area of ICT and internet). Yet, the only serious adaptation of our substantive law that remains to be done is in effect the introduction of the mechanism of the freezing order (article 16 and 17 Cybercrime Convention). Belgium has signed but not yet ratified the Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse (CETS 201). The reasons for the delay in ratification are not clear.

International net searches (See above F.1: Application of domestic law to data entered into the internet abroad): An adaptation of internal law will also have to focus the discussion on the compatibility with the Convention of the Belgian power to execute a computer search abroad, beyond the Belgian borders (art. 88 CCP). The Convention does not provide for this extra-territorial searching power of a computer system without the agreement of the person authorized to have access to this system.

Identity Theft (See above A.1: Specific legal interests deemed to be in need of protection by criminal law): Under A.2.5 (Crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities), we discussed crimes related to virtual identities of users. Under B.1 (Specific problems with respect to the principle of legality), we referred to a legislative proposal aimed at the sanctioning of identity theft within the context of an electronic communications network, but that did not make it. In a recent report, the Working Group on Information Technology and Liberties of the Belgian Senate considers to propose new criminal legislation for online identity theft, including false profiles on Facebook.[118]

Preservation order (See above B.3: Avoidance of criminal legislation becoming obsolete in light of rapid technological innovation): Article 126 of the Act of June 13th, 2005 on electronic communications will be further elaborated in a Royal Decree.

Netiquette (See above B.1: Specific problems with respect to the principle of legality): Under B.1 (Specific problems with respect to the principle of legality), we discussed a legislative proposal aimed at obliging ISPs to contractually impose netiquette and related sanctions on their customers.

H. SUMMARY TABLE

The table below gives an overview of those criminal laws that fall under more than one of the above-mentioned categories of criminal laws (see above A.2), and that cover mere preparatory acts and data possession.

Criminal law/category	Attacks against IT systems	Violation of IT privacy	Forgery and manipulation of digitally stored data	Distribution of computer viruses	Crimes related to virtual identities of users	Preparatory acts	Data Possession
Hacking	X					X	X
Illegal interception	X	X				X	X
Data and system interference	X	X	X	X		X	X
Computer fraud	X		X		X		
Computer Forgery and Use of Forged Computer Data	X		X				
Spamming or Stalking	X		X			X	
Privacy (or "data protection") Offences	X	X			X	X	X
Act of June, 13th 2005 on electronic communications	X	X	X				X

I. REFERENCES

[1] Criminal Court Brussels, January 21st, 2004, *Computerrecht*, 2004, pp. 21 and f.

[2] Act of June 30th, 1994 protecting privacy against the interception of communication and telecommunication, *Belgian official journal*, January 24th, 1995, p. 1542.

[3] De Hert, P., 'De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?', *Tijdschrift voor Strafrecht*, 2001, Vol. 2/6, pp. 316-317.

[4] Criminal Court of. Dendermonde, November 28th, 2005, *Nieuw Juridisch Weekblad (N.J.W.)*, No. 138, 2006, p. 229 and note J. Deene (who does not agree with this theory); *R.A.G.B.*, 2007, p. 427. Criminal Court. Dendermonde, May 14th, 2007, *T. Strafr.*, 2007/6, pp. 404-407, annotation by E. Baeyens.

[5] Board of General Prosecutors, Circulaire COL1/2002 of February 14th, 2002, 'relative à la criminalité informatique', p. 7.

[6] See for a detailled analysis on the limits of the power of the public authorities Degrave E. 'L' article 22 de la Constitution et les traitements de données à caractère personnel', *Journal des Tribunaux*, 2009, pp. 365-371 and for an analysis of the interaction between the public sector and the private sector regarding to the processing of personal data with new technologies: Degrave E. & Poullet Y., 'L'externalisation de l'adminsitration, les nouvelles technonlogies et la protection de la vie privée', *Journal des Tribunaux*, 2008, pp. 277-285.

[7] See Art. 44/1 until 44/11 of the Act of August 5th, 1992 'on the Police function' about the rules of dealing by a police force of datas and informations introduced by Art. 1991 of the law of December 7th, 1998 organising an integrated police force on two levels, *Belgian official Journal*, January 5th, 1998.

[8] Article 39 punishes with a fine of one hundred to one hundred thousand francs 1° any controller, his representative in Belgium, appointee or agent who processes personal data in violation of the principles and requirements imposed in Article 4 § 1 (finality principle, proportionality principle, etc.); 2° any controller, his representative in Belgium, appointee or agent who processes personal data in cases other than those permitted in Article 5 (consent, contract, legal ground); 3° any controller, his representative in Belgium, appointee or agent who processes personal data in violation of the Articles 6, 7 and 8; (these regard the so called sensitive data); 4° any controller, his representative in Belgium, appointee or agent who has failed to comply with the obligations laid down in Article 9; (duty to inform the data subject); 5° any controller, his representative in Belgium, appointee or agent who fails to communicate the information referred to in Article 10 § 1 within forty five days upon receipt of the request, or who knowingly communicates inaccurate or incomplete data; 6° any person who resorts to acts of violence or threat with the purpose to force another person to disclose information that is obtained through the exercise of the right as defined in Article 10 § 1 or to give his consent for the processing of personal data relating to him; 7° any controller, his representative in Belgium, appointee or agent who starts, manages, continues to manage or terminates an automatic processing operation of personal data without compliance with the requirements of Prior notification to the National Data Protection Authority (Article 17); 8° any controller, his representative in Belgium, appointee or agent who communicates incomplete or inaccurate information in the notifications prescribed in Article 17; 10° any controller, his representative in Belgium, appointee or agent who, in violation of Article 19, refuses to communicate to the Commission the information relating to the non-automatic processing of personal data that are contained in a filing system or that are intended to be contained therein; 12° any person who transfers personal data, brings about or permits such transfer to a country outside the European Community that has been entered on the list referred to in Article 21 § 2 in violation of the requirements of Article 22; 13° any person who prevents the Commission, its members or the experts who have been deployed by it from making the verifications referred to in Article 32.

[9] See for a detailed analysis of the interaction between the Data Protection Act and the Computer Crime Act: De Bot, D., 'The (missing) link between the Processing of Personal Data and Computer Crime' in *A Decade of Research @ the Crossroads of Law and ICT*, Dumortier, J., Robben, F. & Taeymans, M. (eds.), Brussels, Larcier & De Boeck, 2001, pp. 35-51.

[10] De Villefagne, F. & Dusollier, S., 'La Belgique sort enfin ses armes contre la cybercrimininalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique', *Auteurs & Media* 2001, pp. 60-81.

[11] Court of Appeal Antwerp, May 28th, 2008, (via http://www.juridat.be).

[12] Act of January 10th, 2010 'modifiant la loi du 7 mai 1999 sur les jeux de hasard, les établissements de jeux de hasard et la protection des joueurs, en ce qui concerne la Commission des jeux de hasard', *Belgian Official Journal*, February 1st, 2010. The Act updates the Act of May 7th, 1999 on games of chance and protection of players, *Belgian Official Journal*, December 30th,

2009, p. 50040. See Dauwe, L., 'Act on games of chance amended in order to restrict online gambling', *Stibbe, ICT Law Newsletter*, No. 37, February 2010, p. 4

[13] Belgian Law of May 22nd, 2005 implementing Directive 2001/29/EC of 22 May 2001, *Belgian Official Journal*, May 27th , 2005. See Derclaye, E., 'The Belgian Copyright Act finally revamped with the implementation of the Copyright Directive (2001/29): the good, the bad and the ugly', *Euro. C.L*, 2005, vol. 12, xi-xv.

[14] Directive 2001/29/EC of the European Parliament and the Council of 22 May 2001.

[15] For a study about the different ways to repair the damage caused by such an infringement, see A. Berenboom, 'Contrefaçon sur l'Internet – réparation du dommage, www.droit-technologie.org/dossier-182.

[16] See for a discussion in the case law about the extent of this provision and its conformity with the EU Copyright Directive: Wijckmans, E., 'Court of Appeal of Brussels asks preliminary question to the European Court of Justice in the Sabam v. Scarlet case', *Stibbe, ICT Law Newsletter* No. 37, February 2010, p. 5-6.

[17] *Belgian Offical Journal*, November 14th, 1998, p.36914.

[18] *Belgian Offical Journal*, September, 9th, 2003.

[19] See O. Leroux, '*Criminalité informatique*', *loc. cit.,* p. 416.

[20] F. Verbruggen & C. Fijnaut, 'Belgium. The criminal justice system facing the challenge of organized crime', *International Review of Penal Law*, 1998, vol. 68, pp. 630 and 642.

[21] Act of March 21st, 1991 on the reform of certain economic public enterprises, *Belgian Official Journal* March 27th, 1991. An English translation of the Act is available via http://www.itu.int/ITU-D/treg/Legislation/Belgium/law.pdf

[22] See for one of these studies: De Schutter, B., Spruyt, B., Blontrock, P. & De Hert, P., *Informaticagebeuren en strafvorderingsrecht* [Criminal Procedure in a Digital Environment], Antwerp-Deventer, Kluwer rechtswetenschappen, 1992, 149p.

[23] See for a lengthy discussion: De Hert, P., 'De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?', *Tijdschrift voor Strafrecht*, 2001, Vol. 2/6, pp. 286-335.

[24] Koops, E.J., 'Cybercrime Legislation in the Netherlands', 2010, report written at the occasion of the Cybercrime Section of the 2010 International Academy of Comparative Law Congress, p. 2.

[25] De Hert P. & Gutwirth, S., 'Informatie: wel beschermd, doch niet vatbaar voor diefstal. Op het grensvlak van strafrecht en intellectueel recht en voorbij', in K. Byttebier, E. De Batselier & R. Feltkamp (Eds.), *Tendensen in het economisch recht*, Antwerp, Maklu, 2006, pp. 85-116.

[26] Court of Appeal Antwerp, February 14th, 1990, *R.W.*, 1989-90, 1294; Court of Appeal Liège, February 26th, 1992, *J.L.M.B.*, 1992, 1346.

[27] For a study about the Belgian legislation on computer forgery see O. Leroux, 'Le faux informatique', *Journal des Tribunaux*, 2004, pp. 509 and f.

[28] Constitutional Court, Judgement No. 198/2011 of December 22nd, 2011, n° 5147, http://www.const-court.be/

[29] Constitutional Court, Judgement No. 55/2007 of March 28th, 2007, n° 4119, via http://www.const-court.be/. See De Hert, P., Millen J. & Groenen A., 'Het delict belaging in wetgeving en rechtspraak. Bijna tot redelijke proporties gebracht', *Tijdschrift voor Strafrecht*, 2008, vol. 9, No. 1, pp. 3-9.

[30] Belgian National Data Protection Authority, Opinion no 10/2000 of April 3rd, 2000 that estimated that art. 314*bi*s CP cannot be applied on the only consultation of stored data.

[31] Belgian Data Protection Authority, Recommendation no 08/2012 of May 2nd, 2012 on the control by the employer of the use of electronic communication instruments at work, 11, http://www.privacycommission.be

[32] Labour Court of Appeal of Gent, May 9th, 2005 *Computerrecht, Tijdschrift voor informatica, telecommunicatie en recht*, 2006, n° 2, pp.107-110 with note P. Van Eecke & B. Ooms; *Chron. Droit social*, 2006, p. 158. also reported by Verlinden, M., 'Ghent Labour Court of Appeal rules that an employer may monitor employees' Internet use', *ICT Law Newsletter*, No. 23, February 2006, 7.

[33] Criminal Court of Leuven, December 4th, 2007, *Tijdschrift voor Strafrecht*, 2008, p. 223 and note L. Ceulemans; also reported by Debusseré, Fr., 'Correctional Court of Leuven rules that IT managers must respect privacy of e-mail boxes, *Stibbe, ICT Law Newsletter* No. 29, February 2008, p. 2-3

[34] The IT manager was, however, acquitted from the crimes enumerated in Article 124, 1° and 2° requiring 'fraudulent intent', because this mens rea was not proven. Article 124, 1°: "with a fraudulent intent, taking note of the existence of signs, signals,

writings, images, sounds or data of any nature that originate from and are addressed to others" and Article 124, 2°: "with a fraudulent intent, modifying or deleting this information by any technical means or identifying the other persons".

[35] Labour Court of Appeal of Antwerp, September 2nd , 2008, reported in Debusseré, Fr., 'Labour Court of Appeal of Antwerp finds that an employer lawfully dismissed an employee for violation of the company's IT policy', *Stibbe, ICT Law Newsletter*, No. 33, March 2009, p. 5-6.

[36] Court of Appeal Antwerp, September 6th, 2007, reported by Costermans, S., 'Supreme Court finds that the confidentiality of communications applies to both the existence and the content of an e-mail', *Stibbe, ICT Law Newsletter*, No. 37, February 2010, p. 5.

[37] Supreme Court, October, 1st, 2009, via http://jure.juridat.just.fgov.be. See Costermans, S., *l.c.*, p. 5.

[38] Valgaeren, E., 'Bill sanctioning identity theft', *Stibbe ICT Law Newsletter*, No. 25, September 2006, p. 5. The Bill can be found on http://www.senaat.be under No. 3-1779.

[39] We rely on E. Kindt, E. Lievens, E. Kosta, Th. Leys & P. De Hert, 'Constitutional Rights and New Technologies in Belgium', in R. Leenes, E.J. Koops & P. De Hert (eds.), *Constitutional Rights and New Technologies. A Comparative Study*, The Hague, T.M.C. Asser Press, (Information Technology & Law Series, vol. 15), 2008, 11-56.

[40] However, press crimes inspired by racism or xenophobia do not have to be brought before a jury.

[41] The Act can be found on http://www.dekamer.be, No. 52-610. See Debusseré, Fr., 'Bill to oblige ISPs to impose netiquette and sanctions on customers', *Stibbe, ICT Law Newsletter*, No. 30, May 2008, p. 4.

[42] Supreme Court, January 18th, 2011, via http://jure.juridat.just.fgov.be., *T.Strafr.* 2011, No. 2, pp. 120-122, annotated by P. Van Linthout.

[43] Supreme Court, September 4th, 2012, A.R. P.11.1906.N/18; See P. De Hert & G. Boulet, 'De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten' [The Yahoo-sage: the choice between national investigation methods and international mutual assistance instruments], to be published in the next edition of *Computerrecht*, 2012.

[44] Beirens, L., 'De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace' [The police, your virtual friend? Thinking about a policy-oriented approach of criminality in virtual communities in cyberspace], *Orde van de dag*, 2010, Vol. 49, pp. 66.

[45] Koops, E.J, 'Cybercrime Legislation in the Netherlands', 2010, report written at the occasion of the Cybercrime Section of the 2010 International Academy of Comparative Law Congress, p. 2

[46] In Dutch: 'informatica systeem'.

[47] De Hert, P., 'De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?', *Tijdschrift voor Strafrecht*, 2001, Vol. 2/6, (pp. 286-335), p. 316.

[48] Exposé des motifs, *Chambre des Représentants de la Belgique*, *Doc. Parl.*, Sess. Ord. 1999-2000, n°50213/001, p. 12 (The preparatory works can be consulted at http://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&rightmenu=right&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=50&dossierID=0213).

[49] Act of November 20th, 2011 'modifiant la législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité', *Belgian Official Journal*, January 20th, 2012.

[50] Rapport fait au nom de la Commission de la Justice par M. MAHOUX, *Le Sénat de Belgique*, 2011-2012, no. 5-1248/1, March 7th, 2012, 72 (at http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=nl).

[51] Data Protection Authority, Opinion No. 29/2008 of September 3rd, 2008 on a draft Royal Decree which obliges telecommunications operators to cooperate with law enforcement agencies in case of judicial inquiries ('Royal Decree on Cooperation'), via http://www.privacycommission.be. See Dauwe, L., 'Privacy Commission issues Advice on the obligation of network operators to cooperate in judicial inquiries', *Stibbe ICT Law Newsletter*, No. 32, December 2008, p. 4

[52] Translation found at http://www.stopchildporno.be/en/child-pornography/belgian-law/

[53] Supreme Court (cass.), February 3rd, 2004, n° P031427N, www.juridat.be

[54] Poulet, Y., 'La lutte contre le racisme et la xénophobie sur Internet', *J.T.*, 2006, pp. 1-12.

[55] De Villefagne, F. & Dusollier, S., 'La Belgique sort enfin ses armes contre la cybercrimininalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique', *Auteurs & Media* 2001, pp. 60-81.

[56] See Baeyens, E., 'Informatica en strafrecht: oude griffels – nieuwe leien', anotation of Criminal Court Dendermonde 14 May 2007, *T. Strafr.*, 2007/6, pp. 404-407.

[57] See Baeyens, E., 'Informatica en strafrecht', *l.c.*, pp. 404-407.

[58] See Court of Appeal Antwerp, September 13th, 1984, *R.W.*, 1985-1986, Court of Appeal Brussels May 10th, 1990, *Pas.*, 1990, II, 1-6; Criminal Court of Brussels, June 24th, 1993, *J.L.M.B*, p. 44.

[59] F. Lugentz, 'Les vols et les extorsions', in *Les infractions contre les biens*, Bruxelles, Larcier, p. 70-71. According to this author the use, for instance, of a stolen or false magnetic badge to have access to a building can still be considered as a 'false' key and thus as aggravating circumstance of a theft that is more severely punished than a computer fraud.

[60] Coesemans, C., 'Hacker ReDaTtAck convicted under Cybercrime Act', *Stibbe ICT Law Newsletter*, No. 13, January 2004, p. 8.

[61] Criminal Court Ghent, December 1st, 2003, not published but reported in Coesemans, C., *l.c.*, p. 8.

[62] Court of Appeal Antwerp, May 28th, 2008, (via http://www.juridat.be).

[63] Court of First Instance Brussels, March 2nd, 2000 (with comment of Marc Isgour), *Auteurs & Media* 2001, 151-157.

[64] Supreme Court, March 6th, 2012, No. P.11.1374.N/1 and No. P.11.0855.N/1, via http://jure.juridat.just.fgov.be; See D. Voorhoof, 'Weblogs en websites zijn voortaan ook 'drukpers''[Henceforth, weblogs and websites are press], *De Juristenkrant*, 2012/246, pp. 4-5; See also P. Lemmens, 'Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid' [Abuses of the freedom of expression via internet: is the law 2.0-compatible? Plea for a technology-neutral protection of the freedom of expression], *Orde van de dag,* 2010, Vol. 49, pp. 15-22.

[65] Court of First Instance of Brussels, February 19th, 2004, via http://www.droit-technologie.org. See Rosier, K., 'Court qualified on-line defamation as a press delict', *Stibbe, ICT Law Newsletter No. 17* – November 2004, p. 6.

[66] Court of First Instance of Brussels, October 15, 2009, *Jurisprudence de Liège, Mons et Bruxelles*, 2010/ 3 pp. 128-136, and note C. Donny, 'Le presse, une notion que le Constituant tard à (re)définir… ' , pp. 137-142; also reported by Dauwe, L.; 'Court of First Instance of Brussels qualifies online defamation as a press delict', *Stibbe, ICT Law Newsletter No. 37* – February 2010, p. 9.

[67] Court of Appeal of Mons, May 14th, 2008, via http://jure.juridat.just.fgov.be ; also reported by Costermans, S., 'Court of Appeal of Mons qualifies online defamation as a press delict' *Stibbe, ICT Law Newsletter*, No. 33 – March 2009, p. 5.

[68] Criminal Court of Brussels, June 23rd, 2009, reported by Leitner, L., 'Criminal Court of Brussels finds that online publications can qualify as a press delict and that purely technical webmasters cannot be held liable for a press delict if the website editor can be identified', *Stibbe, ICT Law Newsletter*, No. 37, February 2010, p. 8.

[69] Supreme Court, February 3rd, 2004, via http://www.juridat.be. See Coesemans, C., 'www.illegalwebs.com Case: hyperlinks to child pornography', *Stibbe ICT Law Newsletter*, No. 16, September 2004, p. 4-5. A more general analysis can be found at http://www.stopchildporno.be/en/faq-en/

[70] Court of appeal of Brussels, January, 23rd, 2009, *R.D.T.I.*, 2009, No. 37, pp. 105-117. See Docquir, P.-F., 'N'ayons plus peur de la liberté d'expression sur Internet: à propos d'une définition stricte des discours de haine' , annotation of Brussels, January, 23th, 2009, *R.D.T.I.*, 2009, No. *37*, pp. 118-127; Costermans, S., 'Court of Appeal of Brussels finds that the administrator of an online discussion forum can be held liable for publishing or preserving unlawful videos and articles', *Stibbe, ICT Law Newsletter*, No. 37, February 2010, p. 8.

[71] Criminal Court of Brussels, November 27th, 2009, *Jurisprudence de Liège, Mons et Bruxelles*, 2010/1, p. 10-17. Also reported by Leithner, L., 'Criminal Court of Brussels finds that online publications can qualify as a press delict and that the person responsible for a website can be held liable for racist and xenophobic content on his website', *Stibbe, ICT Law Newsletter*, No. 37, February 2010, p. 8-9.

[72] Exposé des Motifs, *Chambre des Représentants de la Belgique*, Session 51, 2003-2004, 1284/001, p. 6.

[73] *Belgian Official Journal*, July 27th, 1994, p. 19315. This Act. was modified by the Act of May 15th, 2007 about the repression of the counterfeit and the piracy of intellectual property rights, *Belgian Official Journal*, July 18th, 2007, p. 38734.

[74] We rely on http://www.stopchildporno.be/en/faq-en/. Pornography as a whole is not prohibited in Belgium. The prohibitions that exist are grounded on vague general norms and are only applied to punish the more extreme sexual 'crimes' that society considers to be scandalous, such as bondage, zoophilia or the use of other paraphinalias. Judges are to rule on what is to be considered prohibited pornography on a case by case basis, as no specific criterion is set out by the law. In this respect, the criteria often used are that the material must shock "the morality of the ordinary citizen", so that it is "resented by the collective

conscience of the moment". Thus, no equivocal rule is drawn out; so, it is left up to judges to determine what the average citizen would consider to be unlawful pornography.

[75] *Belgian Official Journal*, April 25th , 1995, p. 10822.

[76] *Belgian Official Journal*, March 17th, , 2001, p. 8495.

[77] For some French authors the use of peer-to-peer network often used for exchange of child pornography can be considered as organized criminality This point of view can also be applicable in Belgium as illustration of the circumstance described Article 383*bis* § 3 CC. See A. Jaber, 'Reflexion sur l'assimilation des réseaux peer-to-peer d'échanges non-autorisés à une bande organisée', www.droit-technologie.org.

[78] Act of November 30th, 2011 'modifiant la législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité', *Belgian Official Journal*, January 20th, 2012 ; See on this L. Huybrechts, 'De wet tot verbetering van de aanpak van seksueel misbruik en pedofilie binnen een gezagsrelatie' [La législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité], *RW* 2011-12, pp.1150-1166.

[79] Supreme Court, April 20th, 2011, via http://www.juridat.be.

[80] See on this C. Falzone & F. Gazan, 'La pornographie enfantine en Belgique', *Journal des Tribunaux*, 2008, pp. 357-365.

[81] http://www.stopchildporno.be/en/faq-en/

[82] *Belgian Official Journal*, August 8th, 1981. A fundamental revision was carried out by the Act of May, 10th 2007 amending the Act of July 30th, 1981 to punish racism or xenophobia by certain acts, *Belgian Official Journal*, May 30th, 2007.

[83] *Belgian Official Journal*, March 30th, 1995.

[84] Act of March 11th, 2003 '*sur certains aspects juridiques des services de la société de l'information*', *Belgian Official Journal*, March 17th, 2003, p. 12962 and Act of March 11th, 2003 '*sur certains aspects juridiques des services de la société de l'information visés à l'article 77 de la Constitution*.', *Belgian Official Journal*, March 17th, 2003, p. 12960.

[85] See E. Montero, M. Demoulin & Lazaro C., 'La loi du 11 mars 2003 sur les services de la société de l'information', *Journal des Tribunaux*, 2003, pp. 81 and f.

[86] *Belgian Official Journal*, August 17th, 2002, p. 35337. See GOFFARD, O., 'Status questionis: risques et responsabilités en cas de transfert électronique de fonds sur Internet ou : des risques encourrus par le titulaire et l'émetteur d'un instrument de transfert de fonds, lorsque l'instrument est utilisé sans présentation physique et sans identification électronique: application au paiement sur Internet", *RDC*, 2005/1, pp.5-19.

[87] *Belgian official Journal*, January 15th, 2010, p. 1906.

[88] *Belgian Official Journal*, July 29th, 2005.

[89] With regard to subscriber data: See article 14 of the Computer Crime Act on the preservation order.

[90] See Royal decree of January, 9th regarding the execution of Art. 46bis §2, alinéa 1er, 88bis §2, alinéas 1er et 3 et 90 quater §2 alinéa 3 CCP and of Art. 109ter, E, §2 the Act of March 21st, 1991 on the reform of certain economic public enterprises, *Belgian Official Journal,* February, 10th 2009. Following the Board of the General prosecutors :: « *Etant donné que les articles de base sur lesquels cet arrêté est fondé ont subi une modification et compte tenu de l'évolution technologique actuelle et de l'adoption de normes techniques européennes, des initiatives ont été prises dans l'intervalle en vue de modifier l'arrêté royal.* », see circulaire n° COL 14/2009 du Collège des Procureurs généraux près les Cours d'appel du 17 décembre 2009, p. 4.

[91] Royal Decree of February 8th, 2011 regarding the legal duty to cooperate with judicial requests regarding electronic communication, *Belgian Official Journal*, February 23rd, 2011; Article 1 of this Royal Decree changes the title of Royal decree of January 9th, 2003 regarding the execution of Art. 46bis §2, alinéa 1er, 88bis §2, alinéas 1er and 3 and 90 quater §2 alinéa 3 CCP and of Art. 109ter, E, §2 the Act of March, 21st, 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, February 10th, 2003.

[92] OECD Directorate For Financial And Enterprise Affairs, *Belgium: Phase 2*, *o.c.*, p. 22. This discretion is limited by the power of the general prosecutor and the Minister of Justice to overrule this decision and to order a prosecution. Also there exists the often used possibility for the injured person to bring a case directly before the courts or to file a complaint before the investigative judge, thus setting in motion the prosecution.

[93] Article 84 of the Act of April 14th, 2011 'portant des dispositions diverses', *Belgian Official Journal,* May 6th, 2011; Act of July 11th, 2011 'amending Articles 216*bis* and 216*ter* of the Code of Criminal Procedure and of Article 7 of the Act of June 6th, 2010 on the introduction of the Social Criminal Code', *Belgian Official Journal,* August 1st, 2011.

[94] OECD Directorate For Financial And Enterprise Affairs, *Belgium: Phase 2*, *o.c.*, p. 22.

[95] Data Protection Authority, *Annual Report* 2011, 5, http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2011.pdf

[96] These authorities are listed in the Royal Decree of May 7th, 2003 'fixant les modalités selon lesquelles la libre circulation de la société de l'information peut être restreinte', (*Belgian Official Journal,* July 7th 2003, p. 36295). Another Royal Decree of May, 10th, 2005 fixes the level of administrative fees that can be proposed in case of infringement to the law (*Belgian Official Journal,* May 10th, 2005). A third Royal Decree April 4th, 2003 rules the sending of publicity via e-mail (Belgian Official Journal, May 28th, 2003, p. 29292).

[97] Act of January 10th , 2010 'modifiant la loi du 7 mai 1999 sur les jeux de hasard, les établissements de jeux de hasard et la protection des joueurs, en ce qui concerne la Commission des jeux de hasard**,** *Belgian Official Journal*, February 1st, 2010. The Act updates the Act of May 7th, 1999 on games of chance and protection of players, *Belgian Official Journal*, December 30th, 2009, p. 50.040.

[98] Beirens, L., *o.c.*, pp. 56 and 59; For an interview (in Dutch) with Luc Beirens, watch: "Cyberwar", Documentary of May 31st, 2012 at Canvas channel, via http://www.canvas.be/programmas/panorama/server11668bf33:136e8606961:-6fa4

[99] See in general Franchimont, M., Jacobs, A. & Masset, A., *o.c.*, 1255 – 1277.

[100] See in general Franchimont, M., Jacobs, A. & Masset, A., *o.c.*, 1255 – 1277.

[101] In Belgian law, the prosecution can in principle be instituted either by the public prosecutor or by an individual joining in the proceedings to make a civil claim.

[102] The principle of universal jurisdiction has been founded on the international criminal character of a crime: on the basis of this principle, all states have the right, and even the obligation, to prosecute and punish certain international crimes irrespective of the place where they were committed and irrespective of the nationality of the offender and the victim. See in general Henzelin, M., *Le principe de l'universalité en droit pénal international. Droit et obligation pour les Etats de pursuivre et juger selon le principe de l'universalité*, Brussels, Bruylant, 2000, 527.

[103] Supreme Court (cass.), May 30th, 2007, *Nullum Crimen*, 2009, No. 6, pp. 387-379: 'The condition of the presence of the suspect in Belgium has to be fulfilled at the moment of the starting of the penal procedure'. See also Art. 11 of the preliminary title of the CCP: "The foreigner who is a co-author of or an accomplice to a crime, which has been perpetrated outside Belgium by a Belgian national, can be prosecuted in Belgium, together with the suspected Belgian national or after the latter's having been condemned". On Article 11 and 12 of the said preliminary title, more in detail, see Demeyere, Br., *l.c.*, p. 54-57.

[104] See F. Van Leeuw, 'Criminalité informatique. Entre objectif et objection d'ubiquité: Quelques pistes de la procédure pénale belge face aux acteurs du « *cyberworld* », European Lawyers Union, *VI Convegno di Studi*, Brussel, Bruylandt, 2010, pp. 414-418.

[105] See Art. 32 of the Cybercrime Convention.

[106] Opinion of the Council of State, *Doc.Parl.*, Ch., 1999-2000, projets de loi 213/1-214/1, pp.45-46.

[107] For a study about Belgian cybercrime legislation after the Act of 2006, see O. Leuroux, 'Criminalité informatique' in *Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 365-453.

[108] *Belgian Official Journal*, September 12th, 2006, pp. 46332-46333.

[109] Council of Europe, Convention on Cybercrime, ETS No. 185, November 23rd, 2001, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[110] Exposé des Motifs, *Chambre des Représentants de la Belgique*, Session 51, 2003-2004, 1284/001, p. 6 (via http://www.dekamer.be/FLWB/pdf/51/1284/51K1284001.pdf).

[111] Exposé des Motifs, *Chambre des Représentants de la Belgique*, Session 51, 2003-2004, 1284/001, p. 6.

[112] Exposé des Motifs, *Chambre des Représentants de la Belgique*, Session 51, 2003-2004, 1284/001, p. 6.

[113] Exposé des Motifs, *Chambre des Représentants de la Belgique*, Session 51, 2003-2004, 1284/001, p. 7.

[114] Belgian Law of May 22nd, 2005 implementing Directive 2001/29/EC of 22 May 2001, *Belgian Official Journal*, May 27th, 2005. See Derclaye, E., 'The Belgian Copyright Act finally revamped with the implementation of the Copyright Directive (2001/29): the good, the bad and the ugly', *Euro. C.L*, 2005, vol. 12, xi-xv.

[115] Directive 2001/29/EC of the European Parliament and the Council of May 22nd, 2001.

[116] *Belgian Offical Journal*, November 14th, 1998, p.36914.

[117] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, September 30th, 3010, 2010/0273, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

[118] Rapport fait au nom de la Commission de la Justice par M. MAHOUX, *Le Sénat de Belgique*, 2011-2012, no. 5-1248/1, March 7th, 2012, 72 (at http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=nl).