EU-legislation and Cybercrime
A Decade of European Legal Developments

Erik Wennerström

1 Introduction

Whereas EU-legislation or EC-legislation today encompasses many aspects of private and business activities of European citizens, following a legislative production that started with European integration half a century ago, it is perhaps surprising that while this body of legislation often aimed at taking the political initiative to protect certain desired activities even before they are threatened – by competition or by other activities – when it comes to information technology (IT) the legislative machinery waited until the activities were not only well into dangerous territory, but actually suffering losses in trust as well as in pecuniary terms before action was taken.

When speaking of high tech- or cyber crimes, one normally refers to traditional forms of crime committed in the IT environment, such as fraud or forgery, as well as forms of crime that are unique to that environment, such as *hacking*[1] and *denial-of-service-attacks*.[2] What is perhaps left out in some such references, are the content-related crimes, such as child pornography or racism, and the infringements of intellectual property rights. Regardless of whether a broad or narrow definition is used, it is a form of criminality which often is transnational – every activity adding up to the completed or attempted crime normally leaves traces in more than one jurisdiction and the successful investigation and prosecution of such crimes inevitably will require a transnational response. An effective and well functioning system of international co-operation is vital to that response. Among the efforts that have been initiated to create common rules and mechanisms to protect European society from cyber crimes, several are now moving on from the negotiation and adoption phase to the implementation phase. This article describes some of these efforts.

2 The Council of Europe Deliberations

Following long and intense negotiations, the Council of Europe succeeded in establishing a convention on "crimes in cyberspace",[3] marked by the signing of the Convention on Cybercrime on 8 November 2001 by close to 30 states.[4] The Convention establishes common definitions of crimes in the cyber environment, as well as judicial co-operation facilities between the participating states to improve their fight against cybercrime. The Convention on Cybercrime entered

1 Unauthorized alterations in a computer program or operative system.

2 *DOS*-attacks; flooding a system with useless traffic in order to overburden it thereby making it malfunctioning.

3 Convention on Cybercrime, ETS No. 185, "http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm".

4 All 43 Council of Europe Member States have participated in the negotiations, together with Canada, Japan, South Africa and the United States. The Signatory States are, as of 1 June 2004, Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Switzerland, former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa.

into force following its ratification on 18 March 2004 by Lithuania, thereby reaching five ratifications, which was the requirement for the Convention to enter into force.[5]

2.1 Approximation of Rules on Criminalized Acts

The first part of the convention requires the Contracting States to ensure the criminalization of substantive offences described in Articles 2 – 10 complemented by rules on attempt, aiding and abetting, as well as rules on the liability of legal persons.. The first category of such provisions, in Article 2 – 6, cover crimes against the *confidentiality, integrity and accessibility* of data and systems or computer-crimes (i.e. environmentally unique crime types). This part defines illegal access, illegal interception, illegal damaging and alteration of data, system entry as well as illegal use of certain types of equipment. Article 2 describes the crime of illegally accessing a computer system, in whole or in part. ("In whole or part" is a necessary qualification, as a "computer system", in accordance with the definitions set out in Article 1, is *any* equipment used to treat data automatically.) While Article 3 criminalizes illegal or unauthorized interception of non-public transmissions of computer data, it is worth noting that Article 4 covers the deletion, alteration and suppression of data – a crime referred to as *data interference* – referring i.a. to situations where data is made inaccessible to those authorized to access it. Such situations frequently occur when hackers alter the privileges or authorization levels of computer files. As the article covers alteration of data, most forms of malicious computer viruses will also be covered by it.[6]

Article 5 criminalizes serious *system interference*, resulting in hindering a system from performing the functions it was designed to perform. In order for the interference to be criminal, it must be the result of some form of data manipulation, not mere accident. Unsolicited e-mail advertisement or *spam*, cannot be seen as such interferences *per se*, but the distribution of spam may ultimately result in a system (or server) being overloaded, leading to its malfunctioning. In that situation, it may be argued that a system interference has taken place (based upon a *culpa eventualis* evaluation – the perpetrator had no direct criminal intent, but realized the risk of his behavior and ignored the risk) with results identical to that of a deliberate denial-of-service attack, i.e. the intentional overloading of a system in order to make it malfunction.[7] Article 6 criminalizes the *misuse of devices*, a concept directly imported from the US Federal Criminal Code, Section 1029 "Fraud and related activity in connection

---

5 The starting point of the process that led to the negotiations can be traced back to a series of recommendations adopted by the Committee of Ministers of the Council of Europe – Recommendations No. R (85) 10, R (87) 15, R (88) 2, R (89) 9 and R (95) 13 – as well as to Resolutions 1 (97) and 23 (00) adopted by the European Ministers of Justice.

6 *Convention on Cybercrime (ETS no. 185), Explanatory Report*, p. 61, "http://conventions.coe.int/Treaty/en/Reports/Html/185.htm".

7 Id. p. 69. Wennerström, *Europeiskt arbete mot IT-brottslighet*, Europarättslig Tidskrift, 2001 p. 480.

with access devices".[8] Paragraph 1 of Article 6 criminalizes the production and dissemination of devices, mainly designed to commit the crimes outlined in Articles 2 – 5. This includes the dissemination of passwords and other tools to gain unauthorized access to computer systems, provided there is criminal intent on the part of the perpetrator. Possession of such devices is likewise criminalized, provided there is intent to commit one of the listed offences demonstrated.

As regards *computer-related crimes* (i.e. traditional crime types adapted to the IT environment) the convention defines computer-related fraud and forgery in Articles 7 and 8. Although most States already have criminalized the crimes of fraud and forgery as such, these provisions require States to examine their laws to ensure that they apply to IT-situations. Computer-related forgery and fraud are two specific kinds of manipulation of computer systems or data, and the provisions serve to acknowledge the fact that traditional legal provisions are not always suitably adapted or neutral enough to cover new forms of manipulations.

The Convention also covers some *content-related crimes* and requires States to criminalize i.a. distribution, production and possession of child pornography through the use of computer systems, according to Article 9.[9] This provision criminalizes several aspects of child pornography, which in its offline-form already is criminalized in most States:

- the production of child pornography for the purpose of distribution through a computer system
- the 'offering' and making available of child pornography through a computer system
- the distribution or transmission of child pornography through a computer system
- the 'procuring for oneself or for another' of child pornography, i.e. actively obtaining it through e.g. downloading
- the possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom.

Originally racism and xenophobia was also covered by the Convention's provisions on content-related crimes, but during the finalizing stages of the negotiations it became clear that it would not be possible for some of the negotiating states to agree upon a text that basically criminalized what their constitutional guarantees for freedom of expression were safeguarding.[10] Finally

8 Cf. 18USC1029; *see* U.S. Code Online via GPO Access, "http://www.access.gpo.gov/UScode/title18/parti_chapter47_.html".

9 This Article was later the model for its counterpart in EU legislation, *see* below.

10 That provision was subsequently taken out of the Convention, and negotiated separately as a Protocol to the Convention, and as such signed – by currently 23 states; no ratifications – in early 2003; *see* Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed through computer systems,

we also find among the criminal law definitions infringements of copyright and other intellectual property rights, in Article 10, that states are required to criminalize.

States are required to criminalize these acts through the introduction of penal law sanctions that include custodial penalties. Before it is possible to say whether these provisions actually create a finely woven web of substantive criminal law over the ratifying states, it is necessary to see *how* the ratifying states implement them in their national laws. The states are given room to maneuver in the implementation, as a result of the compromises that lay behind the ultimately adopted text.[11] Article 11 (3) may serve as an example of how much is still at stake, as it makes the obligation to criminalize the *attempt* to commit the crimes described in Article 2 – 10 optional for the ratifying states. This may lead to ulterior difficulties regarding i.a. the requirements for dual criminality.

2.2 Rules on Criminal Procedure

The convention contains rules on criminal procedure such as coercive measures to facilitate investigations of the crimes described above, through a combination of "old" and "new" procedural measures. One such new measure is the "rapid freezing" of data (including traffic data; see below) i.e. an authority with relevant competence shall have the right to order data concerning a crime or a criminal to be stored with an Internet Service Provider (ISP, i.e. a company providing access to internet, e-mail services etc.) in order for it to be deliverable to the investigating authority upon a subsequent formal request for its release. This measure may remain in place for a maximum of 90 days, according to Articles 16-17. Traditional possibilities for search and seizure in order to obtain stored data are provided for in Article 19. Authorities shall have the possibility to secure seized data and to make it inaccessible for unauthorized persons.[12]

Although stopping short of requirements concerning historical traffic data[13] the Convention provides that data shall be presented to the law enforcement authorities at their legally authorized request, in order to identify the operators

---

ETS No. 189.

11 Id. p. 483.

12 *Convention on Cybercrime (ETS no. 185), Explanatory Report*, pp. 200-202, "http://conventions.coe.int/Treaty/en/Reports/Html/185.htm".

13 Traffic data is the data generated at the ISPs as a result of their clients' use of their services; *see* proposed legal definition below. "Historic" or *ex ante*-traffic data refers to traffic data generated up to a point in time at which a search is made retrospectively, i.e. what traffic data has been generated by a particular client account during the past specified number of months. This type of search would require guaranteed *retention* of traffic data and will *not* be possible to conduct with support of the Council of Europe Convention's provisions; only *ex post*-traffic data or data generated in relation to a particular account *from* a specific point in time (the time when the decision to disclose data or granting a request to freeze data, is made) and onwards. The Council of Europe-mechanism is therefore more of a surveillance-mechanism for *preservation* of traffic data, than a useful tool for investigating crimes that have already taken place.

and the route that particular data has taken in transmission. It shall also be possible for authorities to order an ISP to reveal information about its user/client accounts. The Convention stipulates that it shall be possible for authorities to collect traffic data in real time – again: not going back in time, but from a point in time and forwards - that is related to certain data communications and ISPs may be ordered to assist authorities in relation to such measures. Just like in the offline situation, it shall be possible for authorities to use telecommunications-interception in real time in investigation of serious crimes, according to these provisions (Articles 20 and 21). These measures may only be taken under special conditions such as authorization by a judge or another independent authority, subject to the rules on human rights and proportionality in the Signatory States.

2.3 International Co-operation

The Convention's rules on international co-operation aim at making the procedural rules described above enforceable transnationally, by providing possibilities for law enforcement authorities in one state to seize computer-based evidence on behalf of the authorities in another country, Article 31, swiftly and in a less formalized manner in urgent cases, Article 29. The assistance may consist in freezing and seizing certain data in another state that is relevant to an investigation. Central authorities shall be appointed for sending and receiving requests for such assistance, but it shall in urgent cases be possible for authorities to communicate directly with each other. Requests may be refused only under certain circumstances and certain user limitations may come into play as a result of states' rules on data protection. Apart from this, spontaneous and voluntary exchange of information is foreseen.

Pending a formal request for assistance, states shall freeze stored data on request, for at least 60 days. The grounds for refusal are limited. The states naturally have the right to access publicly available information without the permission of other states, should the location of such data be hosted on servers there. On request states shall assist each other with real time collection of targeted traffic data, Article 33 – "targeted" as opposed to "fishing expeditions" where i.a. all traffic data generated at a particular server is monitored indiscriminately - for all crimes falling under the convention, in accordance with the conditions and procedures described in national law. States shall furthermore assist each other with interception of telecommunications as far as is possible with regard to existing treaties and national law, Article 34.

The crimes described in the convention shall be extraditable, according to Article 24, provided that the crimes are punishable with imprisonment of one year or more, with certain exceptions, and that requirements of dual criminality, where applicable, are satisfied.[14] In order to provide support to ongoing investigations, a network of contact points is created, available 24 hours a day,

14 This is not a new rule, but basically just an extension of existing rules on extradition – the Council of Europe Convention of 1957 on Extradition, as well as the two EU conventions of 1995 and 1996 - to this convention, which can also be said about the convention's rules on search and seizure in computer environments.

seven days a week, as outlined in Article 35. This network is modeled on the G8-network (see below) and in reality means that the G8-network is expanded to all ratifying States of the Council of Europe convention.[15]

The Cybercrime convention must like all conventions be ratified, a process that can be time consuming and uncertain - even positive ratifications can be combined with reservations towards certain parts of the agreed text. Herein lays a weakness in the convention as an instrument of legislation, a weakness that is even more evident when compared with EU-instruments (Framework Decisions, Council Decisions, and Directives) that enter into force upon their adoption. According to Article 36, the Convention does not enter into force until it has been ratified by five states – Lithuania became the fifth country to ratify the Convention and subsequently it is now in force between the states that have ratified it; to date it is not in force in any of the states through which the lion share of data – legitimate as well as illegitimate – flows. But apart from this the Council of Europe has created an instrument with broad coverage, legally – covering substantive criminal law, procedural law as well as international co-operation – as well as geographically, which is its main advantage.[16] The Convention has had great influence even well before it entered into force, yes, even before the text of the Convention had been agreed upon in 2001, on national, regional and international negotiations and discussions on cybercrime, which demonstrates its unique nature at the time of adoption, and the high technical quality of its provisions.[17]

3 EU Deliberations

The possibilities for creating and implementing legislation are naturally greater in the EU, consisting of 25 states already linked together by a vast common legal system of Community law, than among a larger and more loosely knitted circle of countries, such as the Council of Europe. In spite of this, the EU refrained from bringing forward solutions of its own concerning cyber crimes, pending the outcome of the Council of Europe-negotiations, and it is not until recently that a series of different initiatives have been issued at EU-level, starting with several "soft law" Recommendations and Council Conclusions, later followed by, as a first legislative proposal, measures against credit card-fraud or fraud and forgery of non-cash means of payment, where the Commission took action as early as 1998, although the Council did not conclude its deliberations until 28 May 2001, when the Framework Decision on Combating Fraud and Counterfeiting of Non-

15 *See* p. 298, Explanatory Report.

16 Albania, Croatia, Estonia, Hungary, and Lithuania were the first five States to ratify the Convention. For these five, the Convention enters into force on 1 July 2004. Romania has since joined the group of ratifying States, and the Convention will enter into force in relation to Romania on 1 September 2004. France, Sweden and the United Kingdom are currently in the process of ratifying the Convention.

17 *See* e.g. references in the explanatory memorandum to the Commission's proposal for a Council Framework Decision on attacks against information systems, COM (2002) 173 final, 19.04.2002.

Cash Means of Payment was adopted.[18] This instrument applies to pre-paid and other paper instruments as well as all electronic instruments and applications. Member States are required to ensure criminal sanctions against fraud and counterfeiting of such instruments, when the acts are offences related to

- payment instruments
- computers
- specifically adapted devices.[19]

During this period of relative inertia in the EU, the Council of Europe negotiations held centre-stage, closely followed by the G8. If the Council of Europe was taking the lead concerning judicial co-operation in this field, the same could be said about G8 (USA, Canada, Japan, United Kingdom, Germany, France and Italy - and Russia) when it came to practical co-operation. In 1997 agreement was reached within G 8's crime fighting activities (the co-operation that is commonly known as the Lyon-group, where the Commission takes part as a representative of the EU as such) on an action plan on high-tech and computer-related crime. This action plan contains several of the actions that have later been transposed into provisions of the Council of Europe Convention (such as the 24/7-network) and into Commission initiatives (such as encouraging special police capabilities for fighting this type of crime; see 3.1 below).[20] The most

18 Council Framework Decision 2001/413/JHA.

19 *See* Article 6 of the Cybercrime Convention above. It is the same US Code Article that has influenced European legislation here.

20 The G8 1997 Action Plan on Combating Cybercrime contains the following points:
- use established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis;
- taking appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other states;
- reviewing G8 legal systems to ensure they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes;
- considering issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements;
- continuing to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; trans-border searches; and computer searches of data where the location of that data is unknown;
- developing expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally;
- working jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence;
- ensuring that G8 can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required;

tangible result of the G8 action plan is the establishment of a network of law enforcement contact points for combating cyber crime, accessible 24 hours a day, seven days a week. This network makes it possible to swiftly and without bureaucracy request the assistance from other participating states, in investigations with links into other countries. From the outset the idea was to expand the membership of the network beyond the G 8-states, and the network now holds over 30 participating states.[21]

When G8 met in October 1999 to follow up the action plan, one could, apart from the progress made above all in relation to the network, note that the greatest challenge consisted in identifying and tracing criminals in the on-line environment. For this reason certain principles were adopted, on trans-border access to stored data, amounting to rapid freezing of data at the request of another state, simplified mutual assistance and a general permission to access publicly available material in another state, without specific permissions. These principles can now also be found in the Cybercrime Convention, which demonstrates how much cross-fertilization took place between these processes.[22]

3.1 The Policy behind EU Action

Inspired by the progress in the Council of Europe negotiations[23] and no longer feeling the need to hold back its own ambitions, the Commission issued a Communication to the Council and the European Parliament,[24] 26 January 2001, on *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (referred to as the Cybercrime Communication). It contains policy proposals as well as indications on planned legislative proposals from the Commission. In the Communication, the Commission notes that approximation of penal law is necessary for establishing common minimum levels of protection in the EU. An important chapter concerns the procedural law aspects of cyber crime-fighting, where the Commission notes that the issues that need to be addressed are interception of communications, retention of traffic data, anonymity on the

- encouraging internationally recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies;
- developing and employing compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

21 EU Member States that had not joined the G8-network have been encouraged to do so, through statements and formal Council Recommendations of the EU. *See* Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime. OJ C 187/5, 3.7.2001.

22 The Commission also noted the concrete measures promoted within the G8, as it formulated its own ambitions in this field.

23 For a comparison between different instruments, *see Network security and crime fighting – coordinated instruments (Nätsäkerhet och brottsbekämpning – Samordnade instrument),* Sandberg, C., Stockholm 2003.

24 COM (2000) 890.

Internet, practical co-operation at international level, jurisdiction in procedural issues and the evidence-value of computer processed information.

The Commission drew the conclusion that there was a need for EU-legislation leading to

a) the approximation of Member States' penal legislation on child pornography,

b) the further approximation concerning crimes against system integrity [e.g. hacking], racism and xenophobia and drugs trafficking via the Internet,

c) the mutual recognition of judicial decisions, covering measures such as search and seizure,

d) the evaluation of the need for a special initiative on traffic data retention.

Non-legislative proposals were also brought forward:

a) the establishment of an EU Forum where the actors in all fields of society can gather to exchange views and experiences, trying to find solutions to common problems, related to cybercrime.[25]

b) encouraging the security development through Community initiatives (such as *e*Europe)[26] and programmes (such as the research programs),[27]

c) promotion of training in security of relevant staff,

d) support for a data base on the legal development of Member States in this field.[28]

The most concrete proposals focus on material criminal law - as regards procedural law the ambitions are less definite in the Communication, with the exception of mutual recognition of judicial decisions. On the issue of preservation and retention of traffic data the Commission subsequently proposes nothing more than a continued dialogue between all actors involved. The reasons for this relate to the continuous debate between advocates of civil liberties and law enforcement representatives, where the scales leaned in favor of the former in early 2001. The Commission confirms that traditional mutual assistance takes

25 This Forum held its 1st plenary meeting on 27 November 2001, hosted by the Commission, with representatives of the industry, law enforcement authorities, data protection authorities and civil liberties organizations, to discuss the topic of retention of traffic data. The discussions held sofar have been rather inconclusive. For more information, *see* "http:// europa.eu.int/information_society/topics/telecoms/internet/crime/forum/index_en.htm".

26 *See* "http://europa.eu.int/information_society/eeurope/2005/index_en.htm".

27 *See* "http://europa.eu.int/comm/research/fp6/index_en.html".

28 A follow-up to the study conducted in 1998 on behalf of the Commission by Prof. Ulrich Sieber: *Legal Aspects of Computer-Related Crime in the Information Society:COMCRIME Study* (1998), prepared for the European Commission by Dr. Ulrich Sieber, University of Würzburg, Germany.

too long to meet the challenges of the on-line environment and suggests that faster and more effective means for co-operation has to be found.

Apart from the initiatives directly launched as a result from the Communication, the policy ambition of the Commission gradually started to influence *all* initiatives that the Commission and the Member States were taking in the field of criminal law. When the mandate of EUROJUST, the unit for cooperation between prosecution services, was formulated, it came to include cybercrime,[29] and when the *European Arrest Warrant* (EAW) – one of the most revolutionizing instruments in the history of European judicial cooperation – was drafted, cybercrime was in the list of crimes (together with non-cash fraud and forgery) for which the EAW could be used.[30] Other EU bodies have been inspired by this ambition and it should be noted that EUROPOL, the European police office, has taken steps to establish a High-tech Crime Observatory.[31]

Another important policy contribution from the Commission was the Communication on Network and Information Security of 6 June 2001.[32] It contains an analysis of the issues and threats that the Commission considers to be the challenges to *information and network security*. It mostly concerns intentional threats, such as system intrusions, viruses, DOS-attacks and other interferences. But it also covers unintentional threats such as those caused by the human factor and natural causes. Just like the Cybercrime Communication it contains a series of proposals for responding to network security challenges at EU level:

a) measures to increase awareness of problems,

b) a European warning and information system,

c) technical support measures,

d) support for market oriented standardization and certification,

e) a stronger legal framework,

f) increased security in the public sector's use of information technology,

g) improved international co-operation.

Most measures fall in the category of "soft law" but on the basis of reactions from the Member States, industry and organizations, the Commission proposed in 2003 the creation of the *European Network and Information Security Agency*,

29 *See* Article 4 in Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. OJ L 63/1, 6.3.2002.

30 *See* Article 2 in Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. OJ L 190, 18.07.2002.

31 *See* EUROPOL Annual Report 2002, Council doc. 8578/03 EUROPOL 15, together with EUROPOL Work Programme 2004, Council doc. 8580/03 EUROPOL 17.

32 COM (2001) 718.

ENISA.[33] The purpose of ENISA is to develop expertise to stimulate cooperation between the public and private sectors, provide assistance to the Commission and Member States in their dialogue with industry when addressing security-related problems in hardware and software products. ENISA will also follow the development of standards, promote risk assessment activities as well as interoperable risk management routines and produce studies on these issues.

The policy ambitions of the Commission were outlined in the two Communications, triggering other initiatives by Member States and the Commission, and also influencing other initiatives in the fields of criminal law, judicial cooperation, police cooperation and information security. With these ambitions clear, the inertia of the late 1990s was overcome and sharp tools, tools that the Council of Europe did not possess, could be engaged in the fight against cybercrime.

3.2 Content-related Crime gets first Attention

It is worth repeating that the legal framework emerging in the EU following these policy statements was very much inspired by the Council of Europe Cybercrime Convention. It was partially based upon those experiences that the EU initiated the legislative process on child pornography in 2001, when the Commission presented a proposal for a *Framework Decision* (equivalent to a Directive) *on Sexual Exploitation of Children and Child Pornography*.[34] The Framework Decision, which was finally adopted on 22 December 2003,[35] contains rules for harmonizing national criminal law provisions that are directly applicable to the on-line environment. Member States are required in to ensure that the following acts are punishable, when committed intentionally, by physical as well as legal persons:

a) production of child pornography,

b) distribution, dissemination or transmission of child pornography,

c) making child pornography available,

d) acquisition or possession of child pornography.[36]

---

33 The legislative instrument for establishing ENISA is a Regulation (460/2004) adopted on 10 March 2004, on the basis of a proposal of the Commission, doc. COM (2003) 63. *See* "http://www.enisa.eu.int".

34 COM (2000) 854, O.J. C62 E/327, 27.2.2001. The proposal for a Framework Decision, a more directive-like instrument for cooperation and approximation in the area of justice and home affairs, that had been introduced with the Amsterdam Treaty on 1 May 1999, actually followed a Joint Action on the same substance that had been presented in November 1998. Some of the cooperative provisions of that proposal were brought forward in a Council Decision 2000/375/JHA of 29 May, 2000.

35 Council Framework Decision 2004/68/JHA, O.J. L13/44, 20.1.2004.

36 Cf. Article 9 of the Cybercrime Convention above.

As regards physical persons the offences shall carry deterring sanctions, including prison sentences. All provisions shall be incorporated in Member States' national law by 20 January 2006.

Again inspired by the Council of Europe negotiations, the Commission presented a proposal[37] on 28 November 2001 for a *Framework Decision on Combating Racism and Xenophobia*, aiming at harmonizing Member States' criminal law on such offences and to ensure closer judicial cooperation. The proposal also aims to ensure that racist or xenophobic content hosted outside the EU is subject to criminal sanctions inside the EU. The offences include racism and xenophobia through publicly

- inciting violence or hatred,
- insulting or threatening individuals or groups,
- condoning crimes of genocide, crimes against humanity and war crimes,
- disseminating or distributing such material,
- directing, supporting or taking part in activities of groups active with these offences.

The adoption of this Framework Decision, having been the subject of a lengthy and difficult negotiation, is expected during 2004.

3.3 Getting to the Computer-crimes

In 2002, the Commission proposed a *Framework Decision on Attacks Against Information Systems*,[38] containing common definitions of crimes in this pertinent area, as well as rules on criminal procedure, which brings cybercrime-fighting within the general procedural assistance regime developed in the third pillar of the EU. The Framework Decision is expected to be adopted during 2004, and contains common definitions of *illegal access to information systems*, and *illegal interference with information systems* through sending viruses or deliberately overwhelming an information system (denial of service-attacks).[39]

The purpose of the Framework Decision is to approximate (i.e. harmonize) the Member States' legislation concerning attacks against information systems and to improve cooperation between judicial authorities. The Framework Decision covers areas also covered by the Council of Europe Convention, but is not as extensive in scope. Article 1 defines technical terms, such as "computer data", which coincides entirely with the Convention. Instead of "computer system", which is the term used in the Cybercrime Convention, the Framework Decision uses "information system"; both terms cover individual or connected

37 COM (2001) 664.

38 COM (2002) 173.

39 Cf. Articles 2 – 6 of the Cybercrime Convention above.

computing devices, but whereas *computer systems* (Cybercrime Convention) treat data in any form, *information systems* (Framework Decision) are limited to handling computer data, which in its turn is defined in Article 1 (b). The provisions on illegal access to information systems in Article 2, matches Article 2 of the Convention. Paragraph 2 provides Member States with the option to limit criminal activity to the intrusion through a security device, which is an option also found in the Convention. Articles 3 and 4 on illegal system interference and illegal data interference largely correspond to Articles 5 and 4 in the Convention, see chapter 2 above. Article 5 penalizes the dependent forms of crime, instigation, aiding, etc. (The Convention covers some of these forms, but has no provisions on instigation.)

Article 10 deals with Member States' jurisdiction: a Member State has jurisdiction over crimes committed on the territory of that State or by one of its citizens abroad. Acts committed on the territory of a State shall also include acts directed towards information systems in another State, as well as acts directed towards information systems in the State by an attacker elsewhere. The jurisdiction provisions state that Member States shall be competent to prosecute

- persons physically present on their territory who attack information systems located in another country,

- persons physically present in another country that attack an information system located on their territory.

Provisions for conflicting jurisdictions and the traditional *aut dedere aut judicare*-provision one normally finds in EU-instruments are also covered in Article 10.

Member States shall use available cooperation networks for the exchange of information concerning the investigation of the crimes concerned, according to Article 11. For cooperation purposes, Member States shall establish a permanent operational point of contact to facilitate exchange of information on cybercrime attacks. The article refers to "contact points" which is a way of linking the networks together along the same lines as the Convention does through Article 35, i.e. the G8-inspired 24/7-network. (see above.) Illegal interception, misuse of devices, content-related crimes, computer-related fraud and forgery, as well as rules on criminal procedure and cooperation are not found in the Framework Decision. Whereas there was a need for such provisions in the Convention, the EU already has a regime in place covering some of those provisions, in the mutual legal assistance instruments.[40]

40 Most notably in the largely unratified, but most influential Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union, hereinafter MLA Convention 2000. OJ C 197, 12.07.2000. For a full picture of the mutual legal assistance regime, *see* e.g. *Internationell rättslig hjälp i brottmål inom EU. Effektivitet v. rättssäkerhet (International Judicial Assistance in Criminal Matters within the EU. Efficiency v. Legal Certainty)*, Thunberg Schunke, M., Iustus Förlag AB, Uppsala 2004.

3.4 Traffic Data –the Endangered Fingerprints in Cyber space

Just as the Commission in its Cybercrime Communication attempted to strike a balance between crime fighting and data protection, the greatest challenge today for the EU is still to introduce far-reaching rules on data protection, while simultaneously increasing the efforts to fight cybercrime. The Commission published a proposal on 12 July 2000 for a *Directive on the treatment of personal data and the protection of privacy in the field of telecommunications*.[41] Until then, the treatment of personal data and protection of privacy had been regulated through a general data protection Directive (95/46/EC) and a special telecommunications Directive (97/66/EC) that deals with issues specific for this sector. Through the new Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector,[42] which was adopted on 12 July, 2002, the "old" telecommunications Directive was updated in accordance with developments in the field of communications and technology. The new Directive is accordingly not limited to telephony and computer networks, but also covers satellite, ground carried and digital TV, regardless of which information is going through the systems. The Directive requires service providers to take measures to guarantee the security of their services, as well as the confidentiality of communications and traffic data. Member States are required to ensure that illegal interception, storage or surveillance of communications or traffic data is prohibited. Furthermore, the Directive contains rules on location data, i.e. data indicating a terminal's geographical location. Such data may only be treated with the user's consent or when the data has been anonymised.

The most important issue in this context concerns traffic data, i.e. the data generated when transferring messages and information between two addresses on the networks. According to the main provision in Article 6 of the Directive, traffic data must be erased or made anonymous as soon as the transmission of data has been concluded, except when it is needed for billing purposes or, with the consent of the subscriber, value added-services. In the latter situation the service provider must inform the subscriber of the types of traffic data that will be treated and how long the treatment will go on. The thrust of the article is that all information about the addresses between which communication has taken place are erased the moment transmission is concluded, which means a period of a few minutes at most.

Article 15 permits exceptions from the main rule in Article 6 i.a. for purposes linked to national security and law enforcement. National interception rules can subsequently be used, as they will break through the data protection rules. Articles 6 and 15 could, however, create a situation, if used in isolation, where traffic data could be observed *ex post* only, from the moment a decision is taken that certain communications shall be intercepted - all relevant traffic data before that point in time would have been erased or made anonymous. Should a denial of service-attack take place, all communications preceding the attack would be out of sight and what happens after the attack has been discovered (i.e. when the

41 COM (2000) 385.

42 Directive 2002/58/EC.

system has collapsed) is presumably of little relevance. The possibilities for the police to seek the assistance of a service provider in tracking a picture containing child pornography figuring in a chat room on the Internet, would likewise be reduced to nil, since there are no longer any traces of the communication from the moment the picture has been sent to the chat room; we would know that the picture is there but not how or from where it got there. All will depend on how these national rules of exception are formulated.

The implementation of the Directive into national laws will require co-ordinated action of the national measures concerning crime fighting - should the Directive be implemented in different ways in this respect in the different Member States, it will create a situation where some Member States will be able to co-operate to fight certain crimes, whereas others will find that they have sacrificed the safety of their citizens on the altar of data protection, turning ISPs on their territory into havens for computer criminals.

Following the adoption of Directive 2002/58/EC[43] on the processing of personal data and the protection of privacy in the electronic communications sector, the Member States were required until 1 July 2003 to implement its provisions, whereas the optional possibility for Member States in article 15 to limit that obligation for purposes of i.a. national security and law enforcement, can be utilized at any time after that implementation deadline as well. (Needless to say, a Member State having once permitted its ISPs to *not* retain traffic data, will face a steeper challenge when later introducing such obligations, than a Member State with such provisions already in place.)

The possibility in article 15 comes with a qualification, namely that any restrictions of the application of article 6 must be such that they are "necessary, appropriate and proportionate measure within a democratic society ....". Ultimately only the European Court of Justice can interpret the scope of this qualification, and it is likely to do so only if and when a Member State or a body of the EU - normally the Commission - brings a charge of infringement against a Member State or the Council before it. When Member States make use of the exception in article 15, the Member States will not know beforehand if the Commission will charge them with infringement of the EC Treaty, on the grounds that the exception made was too far-reaching in scope (the data to be retained or the purposes for which it should be retained) or in time (the length of the retention periods), in order to qualify as a measure "necessary, appropriate and proportionate measure within a democratic society...." in the eyes of the Commission and, later, the Court. The only way for Member States to avoid having such a sword of Damocles hanging over their rules of data retention, is for the Member States to agree, by means of an EU instrument, on a uniform set of minimum rules regarding the retention of traffic data. During the Danish Presidency, difficult negotiations in the Third Pillar finally resulted on 19 December 2002 in a set of Council Conclusions[44] on information technology and the investigation and prosecution of organized crime. These conclusions call for such a joint effort by the Member States to agree upon common definitions of minimum scope and time for traffic data retention for law enforcement purposes.

43 OJ L 201, 31.7.2002, p. 46.

44 Council doc. 15763/02.

Following intense and substantive consultations, a *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism,* was proposed to the Council on 28 April 2004, by France, Ireland, Sweden and the United Kingdom.[45] Article 1 of this instrument outlines the scope and aim of the Framework Decision, which is to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of data processed and stored by Internet and other telecommunications service providers, for the purpose of prevention, investigation, detection and prosecution of crime or criminal offences including terrorism. The Article underlines that its provisions do not apply to the content of communications, nor to the interception and recording of telecommunications. Article 2 sets the legal definitions of the technical terms figuring in the legislative text. The most important definition concerns "data" which refers to data necessary to

- trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.
- identify the routing and destination of a communication.
- identify the time and date and duration of a communication.
- identify the telecommunication.
- identify the communication device or what purports to be the device.
- identify the location at the start and throughout the duration of the communication.

The main provisions of the Framework Decision are found in Article 3, which creates an obligation for the Member States of the EU to ensure that data is retained by ISPs, and Article 4, which defines the length of the retention period to at least 12 months and not more than 36 months. (According to Article 4, Member States may have longer periods for retention of data dependent upon national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.) A Member State may apply other retention periods as regards Short Message Services (SMS), Electronic Media Services (EMS) and Multi Media Messaging Services (MMS), and concerning Internet Protocols including Email, Voice over Internet Protocols, world wide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice over broadband and subsets of Internet Protocols numbers - network address translation data, but for telephony services excluding SMS, EMS and MMS, the retention period suggested in the proposal is non-derogable. Negotiations are in their early stages as this is written, and difficult to predict, but the fact that the Heads of State and Government, meeting in the

45 Council doc. 8958/04 CRIMORG 36/TELECOM 82.

European Council in Dublin, 25-26 June 2004, expressed strong support for the draft instrument indicates the political pressure behind the continued negotiations.

4 Conclusions

A schematic comparison between the efforts of the two main institutionalized European legislative and cooperative processes, reflects how the EU is gradually not only catching up with the Council of Europe's extensive convention, but also surpassing it in scope and in strength, utilizing the stronger framework for both legislation and for cooperation that the EU provides.

Crime-type or measure	***Council of Europe Cybercrime Convention***	***EU instruments on criminal law and judicial cooperation***
Criminal law		
Computer-crimes	Art. 2 – 6	Framework Decision (FD) on Attacks against information systems
Computer-related crimes	Art. 7-8	FD on fraud and counterfeiting of non-cash means of payment
Content-related crimes	Art. 9 on child pornography	FD on the sexual exploitation of children and child pornography
	Protocol on racism and xenophobia	FD on combating racism & xenophobia
Crimes against intellectual property rights	Art. 10	–
Criminal procedural law		
Ex post traffic data retention	Art. 16-17	MLA Convention of 2000, Art. 17-20
Real-time traffic data retention	Art. 20-21	MLA Convention of 2000, Art. 17-20
Ex ante traffic data retention	–	Draft FD on traffic data retention

Cooperation, mutual assistance		
Measures for rapid assistance	Art. 16-17, 19, 25-26, 33, etc.	MLA Convention 2000, Art. 6-7, etc.
Dual criminality	Art. 25	Restrictions on application of the principle in MLA Convention 2000, Art. 3, and other EU instruments.
Institutions for cooperation	24/7-network, Art. 35	24/7-network EUROPOL, EUROJUST, ENISA

Summing the initiatives up, these are ambitious legislative projects that have been launched in order to provide protection for the developing technology, the market where it operates and the actors in this environment. Nevertheless, it is impossible to reach the goal (a safer information society) unless the same importance is given to the procedural law issues as has been given to the issues of substantive criminal law. This is the dilemma that the EU finds itself in, having addressed one problem after the other which inevitably leads focus on to crimes and criminalization efforts, instead of taking the global grip on the problem, as the Council of Europe did, which took some time and had little political appeal in the process. The distance between full protection[46] and the edge of the ongoing legislative processes, oscillates and will continue to do so. If we look at the development in substantive criminal law, we see legislation in place or being prepared (child pornography, racism, hacking etc.) that provides the EU with common definitions that can be put on top of the definitions gained through the Council of Europe convention. This is clearly raising the common level of protection. But if we turn to criminal procedural law, however, we see how the Council of Europe convention introduces an arsenal of important tools for enforcing the law against criminals, albeit not in the most crucial area of traffic data retention, while the EU is still struggling with the paralysis that its data protection regime has had and still has, which is almost moving in the opposite direction, or at least was until 11 September 2001. This also affects the possibilities for international co-operation and this is a *sine qua non* for any effective fight against cybercrime.

European initiatives, in the Council of Europe and the European Union, have succeeded in bringing the substantive criminal laws of the States therein closer together, so that sanctions are at the disposal of all European courts, or will be soon. Measures have also been taken to ensure more effective judicial and police cooperation between the European states. But as long as there is still a question

46 Which naturally is an illusion and which should not even be *see*n as desirable; *this* is where the Big Brother society lies, *not* in balancing the needs of law enforcement against the interests of personal integrity, as the recent traffic data initiative demonstrates.

mark over the issue of "fingerprints" – will or will not traffic data be available when a serious cybercrime is investigated? – we will not be sure whether cases will ever reach a court. Likewise, as long as the bulk of all communications, data, publications online, etc., are carried over American networks – even those that originate and terminate in Europe – investigations may come to a halt for want of a solid foundation for Transatlantic cooperation on the law enforcement side, stronger than the G8-network. Again the EU data protection regime could prove a spanner in the works, but the Cybercrime Convention may at least go some way; when President Bush urged the U.S. Senate in 2003 to process the ratification of the Cybercrime Convention with speed and in a positive spirit[47] this raises the hopes that not only the American but also the European efforts will achieve durable results in the global fight against cybercrime and that the remaining challenges can be met from both sides of the Atlantic.

47 *See* "http:77www.whitehouse.gov/news/releases/2003/11/print/20031117-11.html".