TEN/072
Information society/
Computer-related crime

Brussels, 12 September 2001

OPINION
of the
Economic and Social Committee
on the
Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime
(COM(2000) 890 final)

_____

On 31 January 2001, the Commission decided to consult the Economic and Social Committee, under Article 262 of the Treaty establishing the European Community, on the

> *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*
> (COM(2000) 890 final).

The Section for Transport, Energy, Infrastructure and the Information Society, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 17 July 2001. The rapporteur was **Mr Dantin**.

At its 384th plenary session of 12 and 13 September 2001 (meeting of 12 September 2001), the Economic and Social Committee adopted the following opinion unanimously.

1. Introduction

1.1 The development of the information society is causing profound changes which affect a number of activities: work, education, leisure, industry, trade, etc.

1.2 The Commission launched the *e*Europe initiative in 1999 to enable the EU to reap the benefits of the new technologies and ensure that these would be socially inclusive. In June 2000, the Feira European Council adopted a comprehensive *e*Europe Action Plan and called for its implementation before the end of 2002[1]. The Action Plan highlights the importance of network safety and the fight against cybercrime.

1.3 This decision follows a number of measures already adopted to fight harmful and illegal content on the Internet, protect intellectual property and personal data and promote electronic commerce, among other things.

1.4 This Communication is part of an ongoing reflection process. In 1998 the Commission presented the Council with the results of a study on computer-related crime (the so-called "COMCRIME" study). In October 1999, the Tampere European Council concluded that high-tech crime should be included in the efforts generally to agree on common definitions and sanctions.

1.5 The Commission Communication discusses the need for and possible forms of a comprehensive policy initiative.

---

1 ESC opinion on "*e*Europe 2002 - An Information Society For All - Draft Action Plan" - COM(2000) 330 final; OJ No. C 123 of 25 April 2001.

2. The communication

2.1 After analysing the opportunities and risks inherent in the information society, the communication lists the national and international solutions adopted in order to fight computer-related crime. In doing this, it stresses that the main issues addressed basically involve "privacy offences", "content-related offences", "economic crimes and unauthorised access" and "intellectual property offences", which can be defined as follows:

– *Privacy offences*: Such offences violate basic privacy rights through the illegal collection, storage, modification, disclosure or dissemination of personal data.

– *Content-related offences:* These involve the dissemination, especially via the Internet, of pornography, in particular child pornography, racist statements, *revisionist statements concerning nazism* and information inciting violence.

– *Economic crimes, unauthorised access and sabotage:* These are related to unauthorised access to computer systems (e.g. hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery and computer fraud) and new forms of committing offences (e.g. computer manipulations).

– *Intellectual property offences:* Such offences endanger the legal protection of computer programmes and databases, copyright and related rights.

2.2 In order to approach useful ways and means of proposing a legal provision aimed at approximating national laws on computer-related crime, the communication considers "substantive law issues" and "procedural law issues" (interception of communications, retention of traffic data, anonymous access and use, practical co-operation at international level etc.).

2.3 The communication then looks at all the non-legislative measures needed to complement the legislative measures. These basically involve the creation of "specialised national units", "specialist training", "co-operation between the various actors", "direct industry actions" and EU-supported "RTD projects".

2.4 As far as the "security of information infrastructures" is concerned, this is largely the user's responsibility.

2.5 In its conclusions and proposals the communication, as it did in its development, also falls into two parts that it specifies and enlarges upon:

– non-legislative proposals; and
– legislative proposals.

2.5.1 Non-legislative proposals

Action is proposed in a number of areas:

– creation of a European forum bringing together law-enforcement agencies, service providers, network operators and consumer groups, with the aim in particular of enhancing co-operation at EU level;

– continuation of action to promote security and trust in the context of the *e*Europe initiative, the Internet Action Plan, the IST programme and the next framework programme for RTD[2];

– promotion of other projects under existing programmes; and the

– provision of funding for improving the content and usability of the database of Member States' national laws provided by the COMCRIME study.

2.5.2 **Legislative proposals**

Under Title VI of the European Union Treaty the Commission will put forward legislative proposals designed to:

– approximate Member States' laws in the area of child-pornography offences[3];
– further approximate substantive criminal law in the area of high-tech crime; and
– apply the principle of mutual recognition to pre-trial orders associated with computer-related criminal investigations involving more than one Member State.

The need to take any measures, in particular of a legislative nature, on the question of retention of traffic data will be assessed by the Commission amongst other consultations, on the basis of the outcome of the work that will be done by the proposed EU Forum in this area.

3. **General comments**

3.1 The ESC agrees with the Commission on the importance of the distribution and use of new digital technologies, particularly the Internet, because data processing and communication infrastructures have become an essential link in our economies. In some sectors this link is so important that part of the economy is "computer-dependent".

2 ESC opinion on the Proposal for a Decision of the European Parliament and of the Council concerning the multiannual framework programme 2002-2006 of the European Community for research, technological development and demonstration activities aimed at contributing towards the creation of the European Research Area, and the Proposal for a Council Decision concerning the multiannual framework programme 2002-2006 of the European Atomic Energy Community (EURATOM) for research and training activities aimed at contributing towards the creation of the European Research Area - COM(2001) 94 final - 2001/0053 (COD) - 2001/0054 (CNS) currently in preparation.

3 Proposal for a Council framework decision on combating the sexual exploitation of children and child pornography - COM(2001) 854 final - CNS 2001/025; OJ No. C 062 E of 27 February 2001.

3.2 The ESC also shares the Commission's view on the risks arising from generalised use of these technologies and the precautions that need to be taken because *"as societies become increasingly reliant on these technologies, effective practical and legal means will have to be employed to help manage the associated risks"*.

3.3 The ESC is therefore pleased that the Communication draws up a very comprehensive list of security problems in the information society and that it puts forward proposals aimed at framing an overall security policy. But the ESC thinks it is necessary to define computer-related crime better, in order to distinguish properly between the two types of crimes and offences: on the one hand, the "new computer crimes" (virus diffusion, software or file destruction, etc.), which must be the subject of new legislation, and on the other hand the traditional criminal activities which are easier to carry out today because of the use of computers and networks (child pornography, money laundering and copyright violation) and which need to be the subject of a more thorough harmonisation of the existing texts in each Member State. These different types of offences require different legal measures to combat them. Combating these various offences, which are committed by people who are good at controlling technologies ("white collar crime"), requires different measures.

3.4 The Commission Communication proposes a number of repressive measures. The ESC thinks that computer-related crime must be combated not only by a policy of repression but also by broader measures involving prevention, training and combating exclusion of all kinds (economic and cultural). The ESC urges that the role of the various actors, in particular public-sector actors at all levels, in implementing this broader policy to prevent and combat computer-related crime be clearly defined : the role of the EU, the states, the regions, the cities, of companies and of all the authorities in "civil society" (schools, associations, libraries , etc.).

3.5 But the ESC feels that some important aspects have been under-estimated in the analyses. The Communication's title suggests that two main issues will be tackled: infrastructure security and cybercrime. The ESC would stress that the Communication is concerned above all with fighting crime: infrastructure security is analysed in much less detail. However, security, and especially the security involved in the technical operation of networks, is far from satisfactory. With the big rise in the number of users and volume of data sent, and the constant introduction of techniques which have still not been stabilised (high volume, Internet on mobiles, etc.), there is a risk of this security being compromised. For example, the problems of overloads or breakdowns of telecommunications networks are hardly mentioned at all[4]. One must realise that as economic activities become more computer-dependent, the technical reliability of networks becomes more and more essential.

3.6 As regards the technical safety of networks, it would be interesting to consider the responsibility of telecom operators and the effects of deregulation. A number of studies show the economic benefits of telecom deregulation (lower prices, contract diversification, new services etc.), but none analyse the effects of this deregulation on the quality and security of infrastructures. The

4 Such breakdowns are spectacular on mobile telephone networks (because all the users are aware of them quickly), but they also occur, though less visibly, on the Internet. Unfortunately few statistics are distributed by the operators on this subject.

Commission Communication gives no financial estimate of the losses suffered by users, particularly businesses, following technical breakdowns on networks. However, would it not be important to be able to assess the purely economic costs - in addition to the social and human costs - brought about by "computer-related malfunctions", as opposed to "computer-related crime"?

3.7 The Commission Communication has a very individual and very "laisser faire" approach to security problems, by tending to transfer the handling of all the problems of security and fighting cybercrime to users. It stresses the responsibility of users, individuals or companies, and seems to under-estimate the role of the big players: the telecom operators and the states: *"Security is therefore, to an important extent, a responsibility of the users, as only they can appreciate the value of the bits being sent or received, and can determine the level of protection needed."* Certainly, all users have a role to play in ensuring their own safety, and the ESC agrees that users should be fully informed of the risks run on the Internet and trained to protect themselves and assume their own responsibilities. But it would stress the limits of such an individual approach: while this responsibility may be partially assumed by "heavy or street-wise" users (big business or institutions), can it really be assumed by "smaller or inexperienced" users (small enterprises, individuals and especially children)? This view of security, which is not sufficient in the "real and concrete" world, is surely not more so - and may even be less so - in the virtual world? Is it not an incentive to create illegitimate means of self-defence, such as private militias responsible for security and fighting cybercrime?

3.8 As a complement to the above remarks, the ESC does not deny that the active citizen of today could play an important role, as a user. The user should be well informed and made aware of all the problems concerning the security of cyberspace. This could be done through basic education and by providing constant information on developments in this field. The e-Europe[5] and e-Learning[6] initiatives, as well as lifelong education and training, can help achieve this objective in a positive and creative way.

3.9 It would also be interesting to ponder at greater length about the responsibility of the players in the IT sector: security probably accounts for more than 10 to 15% of the costs of companies and private individuals (purchase of special "firewall" equipment and anti-virus software, updating of this software, etc.)[7]. The push to buy security tools may be debatable for private individuals and SMEs. It is rather a matter for suppliers and manufacturers who must use the currently existing software and materials in order to protect their customers: *"Therefore it is important to encourage innovation and commercial use of security technology and services."* Are we sure that all makers of computer software and hardware really want a fall in the number of viruses, now numbering more than 50,000 and growing by 10,000 a year.

---

5 See note 1.

6 ESC own-initiative opinion on the European dimension of education: its nature, content and prospects - OJ No. C 139 of 11 May 2001.

7 There are big differences in the vulnerability levels of certain systems.

3.10 Moreover, the ESC feels that the power of the European states and of the EU to manage and control the large organisations which manage the Internet networks should be analysed in greater detail[8]. For example, Europe is completely absent from the Internet administration body, the ICANN (Internet Corporation for Assigned Names and Numbers). The ICANN is a private law body formed in 1998 at the initiative of the American government to ensure Internet co-ordination. Among its other responsibilities this private institution manages Internet addresses (to avoid duplication) and the names of website domains throughout the world, and defines the operational rules which apply to all. But the executive board of the ICANN is made up of representatives of American private operators and of some Internet users "elected by universal suffrage on the Internet", including a representative of European Internet users. The Communication is not forthcoming enough about such issues and the ESC thinks there must be acepre8particip nicatioe on tvariouages Internon manernm in

laws and sanctions should concern not only child pornography but also other areas, such as combating religious sects, racist ideas, sexism and, more generally, the promotion of pornography and violence.

4.2 **Need to regulate the interception of communications**

4.2.1 The ESC shares the fears expressed in the Communication that: "Abusive, indiscriminate use of interception capabilities, particularly internationally, will raise human rights' questions and will undermine citizens' trust in the Information Society". But the ESC would supplement this analysis by stressing the need to respect these principles of confidentiality in areas, including companies' internal operations. Human rights and privacy must be respected in all businesses. This includes protecting personal messages sent or received by employees on companies' communication systems (respect for privacy)[11]. It also means negotiating the use of the individual data that has to be compiled if networks are to function properly, but which enables the activities and behaviour of each employee to be monitored. The negotiation of an "IT users' charter" is one way of striking a balance between respect for personal freedom and the operational constraints of business (double e-mail boxes etc.).

The Commission Communication contains only a footnote on the question of the worldwide intelligence interception network known as ECHELON. The ESC approves the efforts of the EP watchdog to throw some light on this network, certain installations of which (equipment, listening centre, etc.) are installed in a Member State. It would be paradoxical to think up detailed procedures for regulating the interception of communications if these rules were constantly broken by a network of states using the alibi of military security as a screen for the less admissible aims of economic espionage. For this reason the ESC asks the Council of Ministers to take firm action on this matter.

4.3 **Need to retain certain traffic data**

4.3.1 The features of Internet crimes are well-known: they are relatively easy to commit (when computer techniques have been mastered), they require few means, they can be committed from a distance without any physical presence, they can concern a large number of Internet users instantaneously and cause considerable damage. On the other hand, they leave traces in the various components of the networks borrowed by the fraudulent data. Technically, everything pushes the various network actors to erase these traces as soon as the billing operations have been carried out, which makes the work of the police almost impossible. The ESC thinks that this problem is one of those most urgently in need of a solution so as to ensure the smooth operation of the Internet, and supports the position of the Commission, which is to *"urge all the parties concerned to discuss in-depth, as a matter of priority, the complex issue of retention of traffic data"*. This discussion should cover both technical matters (what information should be kept, and for how long?) and economic

---

ESC opinion on the Proposal for a Council Recommendation on the protection of minors and human dignity in audio-visual and information services - COM (97) 570 final; OJ No. C 214 of 10 July 1998.

11 For example, an agreement recently signed by Deutsche Telekom guarantees the total confidentiality of messages sent by employees on the company's intranet and the Internet.

issues (who will pay for these new operations?)[12]. The Council of Europe's draft convention on computer crime[13] specifies a number of methods concerning this retention of data. But the deadlines for adopting and implementing this convention are likely to be very long: it is necessary to speed up the adoption of specific measures in the countries of the EU[14].

4.4 **Anonymous access and use**

4.4.1 The Communication points out that the question of anonymity is at the heart of a dilemma: on the one hand, the possibility of remaining anonymous is essential if one wants to preserve fundamental rights to privacy, but on the other hand the possibility of communicating on-line without revealing one's identity makes it impossible to combat certain offences. The ESC approves the Commission position of applying to the Internet the basic legal principles which apply in other fields: *"The Internet is not an anarchic ghetto, where society's rules do not apply."* The ESC thinks that technical and legal solutions have to be sought so that Internet access and navigation do not lead to websurfers' private behaviour being tracked or investigated. The sending of unsolicited anonymous messages to a given[15] individual address, particularly from public places such as webcafes and libraries, should also be prohibited. Indeed, the growth in the number of anonymous messages is a threat not only to each individual, but also to the whole of society. The ESC is aware of the difficulties posed by even a limited ban on anonymity. However, it is advisable to qualify the statement that "the possibility of remaining anonymous is essential if one wants to preserve the fundamental right to privacy and freedom of expression in cyberspace". Granting recognition to such a concept would undermine the rights of message recipients (personal or generic), who - in order to protect their privacy and their interests - should be able to know the exact identity of those with whom they are in contact.

---

12 The problem of funding has already been tackled in some countries: (Belgium, The Netherlands, United Kingdom, etc.) with different answers.

13 Council of Europe - Draft convention on computer crime - Draft no. 25 of 9 January 2001.

14 ESC own-initiative opinion on the impact of e-commerce on the single market (SMO); OJ No. C 123 of 25 April 2001.

15 Messages sent to public or private forums can remain anonymous because all participants accept such anonymity.

4.5 **Role of the specialised national units**

4.5.1 The ESC approves the call for the setting-up at national level of specialised units responsible for such tasks as prosecuting computer-related crimes and developing investigation technologies. The ESC also shares the Commission's view on the need for statistics on cybercrime: *"There is a clear need to gather reliable evidence on the significance of computer-related crime"*. The ESC therefore asks that the tasks of these specialised units be widened to include keeping detailed and pertinent public statistics on cybercrime, so that these statistics are not entrusted to private research organisations, which still have very close links with the computer sector. The combating of security breaches and cybercrime must include estimating the number of punishable acts, their sources and causes, and above all the financial costs borne by private individuals and companies that are due either to security systems or the consequences of various types of fraud and virus attacks.

4.6 **Creation of a European forum**

4.6.1 The ESC approves the Commission proposal to set up a European forum bringing together a large number of actors with the aim of fully enhancing co-operation at EU level, and urges that this forum should be first of all a place enabling exchanges concerning what is and is not specific to the information society. In particular, such a forum should make it possible to justify the need to set up regulation systems and to develop and circulate this idea among institutions and the public. It must be recognised that the Internet has developed partly outside the traditional regulatory framework: that was one of the reasons why it grew so fast. But the Internet has become too important for it to escape any regulation. However, Internet "fans" continue to stress that *"any regulation of the Internet is a brake on Internet development"*. They rest on the associative and libertarian ideal of a number of Internet users to continue developing the idea that the "digital global village" must not be regulated by states and that codes of good conduct of sufficient. It is time that Europe helped to develop ideas on the need for rules and regulations. It must be repeated that the Internet is a tool like any other which has to be regulated like other economic activities. Electronic commerce in the private sector and online procedures in administrative relations will only develop if the consumer and the citizen have confidence in the Internet. This confidence is tied to the rapid adoption of political, economic or tax rules, and not just to the purchase of security systems by companies and private individuals. Such help for the development of ideas, which has to be accompanied by an awareness of the need for any Internet user to keep well away from extreme attitudes (too much naivety or too much paranoia) could be one of the main roles of the European forum.

4.6.2 In view of the interest of this type of exchange for organised civil society, the ESC will participate in this forum.

4.7 **Direct industry actions**

4.7.1 The ESC agrees with the proposal's statement that: *"Many industries, e.g. in the banking, electronic communications, credit card and copyright sectors, and their customers are potential victims of computer-related crime"*. But it thinks that the Communication does not stress enough the enormous risks that security weaknesses on the Internet pose for SMEs. The suppliers of

commercial sites to firms must be encouraged to use the security measures available. Certainly, the major companies have the human and financial resources to ensure a certain level of security, but many SMEs do not. These SMEs can suffer major financial damage (destruction or loss of files, theft of confidential files, etc.) or even a temporary or permanent cessation of activity (viruses in computer systems, etc.). Moreover, some fraudulent practices on the Internet can involve very high "hidden" costs: thus the practice of mass advertising by e-mail ("spam") can cause message recipients financial costs and, above all, a considerable waste of time[16]. For the moment such practices are virtually unpunished. The ESC points out that it is in favour of a system of "prior consent" for e-mail of a commercial nature[17].

4.8 **EU-supported RTD projects**

4.8.1 The ESC approves the broad outline of the RTD programme set out in the Communication. But it stresses the need to continue ideas and research on two topics which it feels are essential.

4.8.1.1 **Topic no. 1 (technical studies):** to what level of complexity can one develop the Internet without it becoming intolerably vulnerable? Everyone agrees that the fragility of a system is linked to its complexity. Given the increasing computer-dependence of economic activity, at what point will a set of inter-connected networks become dangerous because it is too sensitive to technical breakdown and too vulnerable to cybercrime? All human inventions have size limits (aircraft, ships, tunnels, towers, etc.) and giant-sized things are always fragile. Will the Internet and the networks escape these constraints?

4.8.1.2 **Topic no. 2 (psychological, sociological and cultural studies):** what are the specific psychological features of cybercrime in the immaterial world compared with traditional crime in the "real and concrete" world? The absence of "visible" consequences probably plays a major role. How can the effects of cybercrime be made "visible" and easily perceptible so that everyone can feel the negative effects of it? For example, how can stealing software be made to seem reprehensible, even though the user/victim suffers no apparent damage, since he always has software (unlike the victim of a "theft" in the traditional world)? How can virus-induced financial losses, which, in terms of economic sabotage, are often greater than those caused by fire or explosives, be made "visible", even though the physical consequences are not very spectacular (no flames, noise, etc.)? How can one combat computer-related crime when a significant number of economic cybercrimes (particularly the distribution of viruses and acts of intrusion into certain computer systems) are not committed for the traditional reasons (money, power, revenge, etc.) and are often apparently "gratuitous" acts, inspired more by megalomania *("I am stronger than the most sophisticated systems")* and the search for fame

16 According to a recent EU study (February 2001), mass advertising by e-mail accounts for 500 million messages per day worldwide. This extra traffic, paid for by message recipients, is said to cost the Internet users' community more than EUR 10 billion.

17 ESC opinion on the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector - COM(2000) 385 final - 2000/0189 (COD); OJ No. C 123 of 25 April 2001.

than by the lure of gain? What links are there between cybercrime and exclusion? How should prevention policies be conceived?

4.8.2 Confidence in the Internet can only be increased if problems such as these are analysed better and more knowledge is gained so they can be handled better.

5. **Conclusions**

5.1 The ESC shares the point of view of the Commission on the importance of distributing and using the new digital technologies. Their importance - particularly that of the Internet - is such that part of the economy can be said to be "computer-dependent". This "computer-dependence" will continue to increase.

5.1.1 The ESC also shares the Commission's view that increasingly effective practical and legal means will have to be used as the economy becomes more dependent on such technologies.

5.1.2 In this ongoing context the ESC is pleased with the initiatives envisaged by the Commission in its communication. The ESC stresses the urgency of the need to take certain decisions and speed up the adoption of regulations.

5.2 However, in order to widen the debate it would stress the following:

5.2.1 The Commission Communication proposes a number of repressive measures. These must be backed up by broader measures involving prevention, training and combating exclusion.

5.2.2 More emphasis must be put on infrastructure security.

5.2.3 If, as the Commission indicates, security may be partly the responsibility of the user, it is also necessary to define the role of the big players: the telecom operators and the states. While this responsibility may be assumed by "heavy or street-wise" users (big business or institutions), can it really be assumed by "smaller or inexperienced" users (small enterprises, individuals and especially children)?

5.2.4 It is necessary to study in greater detail the power of the Member States and the EU in managing and controlling the large organisations which manage the Internet network.

5.2.5 The approximation of powers under procedural law must be a priority in order to improve "victim protection". The new powers which would be conferred on the authorities responsible for the application of laws must respect the basic rights to the respect of privacy and the protection of data set out in the EU Charter of Fundamental Rights.

5.2.6 It is necessary, as the Commission indicates, to regulate the interception of communications. This approach must be widened by stressing the respect of the principles of confidentiality in all fields, including the working procedures of companies. The ESC approves and

supports the efforts of the European Parliament to shed all possible light on the worldwide intelligence interception network known as ECHELON and asks the Council of Ministers to take firm action on this matter.

5.2.7 The most urgent issues to be dealt with to ensure the smooth operation of the Internet and combat computer-related crime are the need to retain certain traffic data, the regulation of access and user anonymity.

5.2.8 The creation of a European forum bringing together a large number of actors with the aim of enhancing co-operation at EU level creation is a good initiative. The ESC, as a representative of organised civil society, has decided to play an active part in the work of this forum.

5.2.9 It is necessary to underline and analyse to a greater degree than is done in the communication the enormous risk run by SMEs because of security weaknesses on the Internet (destruction and loss of files, theft of confidential files, computer viruses etc.).

5.2.10 The broad outlines of the RTD programme referred to in the communication are a step in the right direction. However two issues appear essential:

– How complex can the Internet become without risking an intolerable degree of vulnerability?
– What are the specific psychological aspects of computer-related crime in the virtual world compared with traditional crime in the "real and concrete" world?

Brussels, 12 September 2001.

The President of the Economic and Social Committee	The Secretary-General of the Economic and Social Committee
Göke Frerichs	**Patrick Venturini**