5074/01/EN/final
WP 51

Opinion 9/2001

on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"

Adopted on 5 November 2001

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

The European Commission, Internal Market DG, Functioning and impact of the Internal Market. Coordination. Data Protection.
B-1049 Bruxelles/B-1049 Brussels - Belgium - Office: C100-6/136
Internet address: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

The Working Party on the protection of individuals with regard to the processing of personal data

Established by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;

Having regard to Articles 29 and 30 of that Directive;

Having regard to its Rules of Procedure;

Has adopted this opinion.

1. GENERAL OBSERVATIONS

In January 2001, the European Commission addressed a Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on creating a safer information society by improving the security of information infrastructures and combating computer-related crime.

In general, the Working Party welcomes this text, which attempts to accommodate in a balanced manner the different interests in this area. These interests are principally to combat computer-related crime (which can in itself contribute to improving the protection of personal data) and to respect the basic rights and fundamental freedoms of individuals, especially regarding the right to privacy and the protection of personal data. The challenge is to reconcile these two interests, so that measures adopted in the legitimate interest of combating computer-related crime nevertheless respect the requirements resulting from the protection of

basic rights and fundamental freedoms[1]. More particularly, any restriction of these rights and freedoms must be duly justified, necessary and proportionate to the objective pursued. The increasing importance attached to the phenomenon of computer-related crime must not serve as an excuse to set up major citizen surveillance techniques without having given proper consideration to alternative strategies for combating computer-related crime.

The Working Party is pleased to note that the Commission's Communication provides for an EU Forum to be set up, mainly to give a voice to experts of its designation and to representatives from data protection authorities. It is crucial that this Forum should start its activities as soon as possible to enable each initiative associated with combating computer-related crime to be debated openly and transparently, so that these issues are addressed in all their aspects and the interested parties are able to express their points of view before the implementation of any of the measures proposed in the Commission's Communication.

2. SECURITY OF PERSONAL DATA

The Working Party is of the opinion, however, that, although the Communication contains some references to preventive measures, the Commission could have placed more emphasis on the importance of effective preventive measures, and in particular security measures, rather than concentrating on repressive measures[2]. A general improvement in security levels would contribute to reducing the risks of any compromise to network and data security. In this regard, the Working Party would like to recall the obligations ensuing from the directives on data protection.

For example, Article 4 of Directive 97/66/EC stipulates that "the provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented".

The same article stipulates that in the event of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

[1] As are guaranteed, in particular, by Directives 95/46/EC and 97/66/EC, the Charter of Fundamental Rights of the European Union (in particular Articles 7 and 8), the European Convention on Human Rights (in particular Article 8), Council of Europe Convention No 108 of 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Recommendation R (87) 15 regulating the use of personal data in the police sector, Council of Europe Recommendation R (95) 4 on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services.

[2] The Working Party is aware of the existence of a further communication from the Commission that deals specifically with the issue of security, entitled "Network and Information Security: Proposal for a European Policy Approach" (COM(2001) 298, 6 June 2001. The Working Party reserves the right to comment on that text at a later date.

In addition, Article 17 of Directive 95/46/EC, stipulates that "the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of the implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected".

As a last comment on this subject, the Working Party reiterates that Article 24 of Directive 95/46/EC specifically obliges Member States to adopt suitable measures to ensure the full implementation of the provisions of this Directive and, in particular, to lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to that Directive.

3. THE CONCEPT OF COMPUTER-RELATED CRIME

There is no universally accepted concept at European Union level of what constitutes computer-related crime. It can range from both new forms of crime (denial of services etc.) to traditional forms of crime using the new technologies. The Working Party would also like to draw the Commission's attention to the fact that the Communication uses a concept of computer-related crime that is extremely wide-ranging, including crimes for the mere reason that at a given moment use was made of information and communication technologies.

In fact, the range of the concept of computer-related crime is undoubtedly of importance. In particular, this concept will be used as the basis for the procedures referred to in the Communication. It is important to avoid the situation where conduct whose investigation off-line would not involve intrusive procedures becomes the object of such measures simply because of the use of information and communication technologies.

Furthermore, the Working Party points out that the concept of computer-related crime may be found in the annex to the Europol Convention and in the draft Eurojust decision delimiting these bodies' areas of competence. In terms of coherence and legal certainty, it is important that care should therefore be taken to ensure that these different processing methods within different bodies are covered by equivalent and appropriate guarantees[3]. It would be particularly harmful if the distinct areas of competence of these different bodies led to a situation where the data processed in the context of combating computer-related crime were treated with a different level of protection.

4. POSITIVE LAW ISSUES

The harmonisation of positive law provisions will necessarily lead to common offences being defined. In this regard, the Working Party would like to make two observations. Firstly, regarding the content of substantive law, a distinction must be drawn between infringements associated with computer crime (e.g. illegal access or interception etc.)

[3] This would legitimise the increase in the processing of personal data within these bodies.

and infringements relating to the application of legislation on the protection of privacy or personal data (e.g. illegal access to personnel data and infringement of communications secrecy, etc.), in order to avoid contradictions and overlapping that could be deleterious to legal certainty. Furthermore, punishable behaviour in the area of computer-related crime will have to be precisely defined to be able to be subject to prosecution. When defining the factors needed to establish the existence of such infringements, there must be perfect coherence with the existing rules on data protection. Thus, the consent of a person other than the data subject is not necessarily a valid criterion for removing the criminal character from behaviour involving a breach of personal data.

Furthermore, the Working Party wishes to draw the Commission's attention to the need to carry out an evaluation of the work of the Council of Europe that has resulted in the draft Convention on computer-related crime. The Working Party stresses that numerous criticisms of that text have been made, particularly concerning its lack of balance[4]. On this issue, the Working Party would refer, in particular, to its opinion 4/2001.

In addition, the Working Party insists on the need to define the substantive law on conduct that is to be considered criminal in a coherent manner with regard to the legal framework on data protection.

5. PROCEDURAL LAW ISSUES

The Working Party is particularly sensitive to procedural law issues that go hand-in-hand with collecting copious personal data on individuals suspected of having committed offences.

The Working Party would, in particular, like to emphasise that the procedural law measures referred to in the Commission Communication could end up being very wide in scope, to the extent that they could potentially be applied to all sorts of crime and not just computer-related crime.

The Working Party emphasises the need to define the procedural measures in such a way as to ensure compliance with the fundamental rights and freedoms of the data subjects and, in particular, in a manner that is coherent with the legal framework for data protection. For example, the fact that personal data are made accessible to the public, or that the person physically holding them agrees to their disclosure, does not mean that these data can be used completely freely in the fight against crime. Moreover, where the law enforcement authorities are authorised to consult data available from Internet service providers which relate to an individual's connections, only those connections associated with an inquiry into specific activities should be able to be processed by those authorities. To give an example, data on the connections relating to illegal access to a company's Intranet network should be able to be processed, but not data on the surfing habits of the individual responsible for the illegal access that are unrelated to the crime. Similarly, the fact that individuals leave traces on the networks and that personal data are

[4] See, for example, the Common Position of the International Working Group on Data Protection in Telecommunications on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe of 13/14 September 2000: "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", available at http://datenschutz-berlin.de/doc/int/iwgdpt/cy-en.htm, and the report of the European Parliament of 17 July 2001 on the strategy aimed at creating a safer information society by improving the security of information infrastructures and combating computer-related crime.

stored, sometimes without the knowledge of the individual concerned, does not mean that all these data can automatically be used in a particular inquiry. More generally, the Working Party is aware that, when computer data are seized, it can be difficult to determine immediately what data are relevant and what are not. However, it is important that only the former should be stored.

The adoption of each procedural measure and of international cooperation mechanisms should be subject to conditions and safeguards.

The Working Party is of the opinion that the following issues, in particular, should be taken into account:

- the legal basis authorising each measure in a manner that is accessible, not arbitrary, and whose effects are foreseeable, should be determined in advance;

- in a democratic society there is an onus to justify the need for each measure. This justification implies that there should be an overriding social need, an absence of less invasive alternative measures to establish the facts and excludes any general or exploratory surveillance measures.

- the measures should be able to be implemented only if there is clear evidence indicating that someone is planning, committing or has committed certain specific criminal acts. A proportionality test should be performed in each case, covering the nature, circumstances and gravity of the offence;

- all measures should be limited in time and space, sufficiently specific (a specific person, the categories of data that can be seized, the specific computer, the specific data) and associated with a particular criminal inquiry;

- for each case of this kind, implementation of the procedure should be justified and accompanied by an explanation of how less invasive measures are unable to establish the facts;

- if non-relevant data (data concerning third parties, data that are not relevant to the crime, etc) are obtained by the procedures, there should be specific guarantees and, in particular, measures to delete such data;

- informing the person concerned of the implementation of these procedures should be considered from the moment at which this information does not or would no longer hinder the investigation;

- the democratic transparency of the procedures should be effectively applied, for example in the form of criminal policy reports;

- implementing the measure should be conditional upon an authorisation issued by a judicial authority, or an equivalent competent authority, subject to independent control;

- a right to legal appeal[5] should be provided for individuals affected by these measures;

- specific guarantees should be adopted for regulated professions (lawyers, doctors, etc.)[6].

[5] See Article 47 of the Charter of Fundamental Rights of the European Union.

[6] In this regard, refer to the case law of the European Court of Human Rights, which requires premises housing documents covered by professional secrecy to benefit from increased protection, and all relevant searches to be proportionate and targeted so as to avoid accessing documents covered by professional secrecy that are irrelevant to the inquiry.

In addition, the Working Party would like to refer to its previous work on certain specific issues, namely Recommendation 2/99 on the respect of privacy during interceptions of telecommunications and, in particular, the need for national law to define the conditions for intercepting communications rigorously and in compliance with all the above-mentioned provisions, Recommendation 3/99[7] on the preservation of internet traffic data and Recommendation 3/97 on anonymity on the Internet[8].

6. Codes of conduct

The Commission's Communication makes reference at various points to codes of conduct. The Working Party would like to draw the Commission's attention to the fact that any limitation of individuals' fundamental rights must be founded on a legal basis, mainly for reasons of democratic control[9].

Conclusions

The Working Party emphasises the balanced nature of the Commission's communication.
The Working Party recommends the greatest vigilance to ensure that all the measures introduced to combat computer-related crime are also consistent with the requirements of protecting fundamental rights and freedoms and, in particular, the rights to the protection of personal data and to privacy.
The Working Party emphasises the need for a transparent and public debate to start as soon as possible and be continued so as to give all the parties concerned an opportunity to make themselves heard, and in particular experts in data protection.
The Working Party suggests to the Commission that it should assess whether it is genuinely desirable to take as a basis the work undertaken by the Council of Europe that has resulted in the draft convention on computer-related crime.
The Working Party invites the Commission, the Member States and the European Parliament to give this opinion due consideration.
The group reserves the right to comment on the concrete initiatives that will be taken in the area of combating computer-related crime.

Done at Brussels, 5 November 2001

For the Working Party

The Chairman

Stefano RODOTA

[7] See also the European Commissioners' Resolution on Data Protection on the same subject issued in Stockholm in spring 2000.
[8] See Council of Europe Recommendation No R (95) 4, Article 2(2)(2)
[9] As interpreted by the European Court of Human Rights.