



**5001/01/EN/Final
WP 41**

Opinion 4/2001

On the Council of Europe's Draft Convention on Cyber-crime

Adopted on 22 March 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.
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100-6/136
Internet address: <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Opinion:

Introduction

Cyber-crime is part of the seamy side of the Information Society. The use of new technologies bring not only enormous benefits for societies. They also provide the opportunity to commit new kinds of crimes or traditional crimes using new means. States and various instances are conscious of this issue which is therefore dealt with for example in the European Union², the G8³, the OECD, the United Nations and the Council of Europe. The objective of these initiatives is to create an information society where citizens can enjoy freedom and security.

The Council of Europe has a longstanding experience and tradition both in international co-operation in criminal matters as well as in Human Rights. It is working since 1997 on a draft convention on cyber-crime. The committee of experts on crime in cyberspace (PC-CY) has finished its work in December 2000 and the Parliamentary Assembly of the Council of Europe will have to give its opinion (expected for Spring 2001) before the text is to be submitted to the Committee of Ministers of the Council of Europe for adoption. Depending on the opinion of the Assembly, a drafting group will be mandated to modify the text accordingly.

This draft Convention can be signed by countries which are not members of the Council of Europe. The United States, Canada, Japan and South Africa are already actively participating in the drafting process.

¹ Official Journal no. L 281 of 23/11/1995, p. 31, available at:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

² See Communication from the European Commission to the Council and the European Parliament "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" (adopted on 26th January 2001, available at <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html>).

³ See Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes. Adopted on 7 September 1999. WP 25, available at http://europa.eu/comm/internal_market/en/media/dataprot/wpdocs/index.htm

Since April 2000, different versions of the draft Convention have been made available to the public on the web site of the Council of Europe. The draft Explanatory memorandum was published for the first time only recently in February 2001. The drafting process on both documents is continuing. This Opinion only comments on the text of the draft convention as published on 22nd December 2000 (version 25 public⁴), not on the explanatory memorandum.

The Working Party notes the efforts being made in many areas to combat cyber crime and supports the general objectives of these efforts in the way they can contribute to improve the security level for all citizens and in particular for the processing of personal data. It would nevertheless like to give a strong message that a fair balance must be struck between anti cyber crime efforts and the fundamental rights to privacy and personal data protection of individuals as regards the extent to which measures are proposed in the whole of the draft convention. These rights are notably enshrined in the Council of Europe's European Convention on Human Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the field of telecommunications services, in particular as regards telephone services, the EU Charter on Fundamental Rights, the EU Data Protection Directives and the 1966 United Nations International Covenant on Civil and Political Rights.

For these reasons the Working Party offers the following observations on the current draft of the Council of Europe's cyber crime convention.

The Draft Convention

The content of this draft Convention as regards harmonisation of procedural measures (Chapter II) and international mutual assistance (Chapter III) results in the exchange of personal data (traffic data, content of communications and all other kinds) in the course of international co-operation in criminal matters which are not exclusively linked to cyber-crime.

Chapter III concerns international co-operation "for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence". Most obligations for mutual assistance laid down there may concern any crime for which they are sought, be it computer-related or not. The obligations include mutual assistance regarding extradition, spontaneous information, preservation of computer data and traffic data, disclosure of and access to computer and traffic data, transborder access to stored data as well as real-time collection of traffic data and interception of communications. This chapter also provides for possibilities to make requests for mutual assistance by expedited means of communications including fax and e-mail. Formal confirmation has only to follow if requested by the requested Party.

The draft Convention (Chapter II section 2) also requests the Parties to harmonise their procedural law with a view to ensuring that the following measures are available:

⁴ See <http://coe.fr>

expedited preservation of stored computer data, expedited preservation and disclosure of traffic data, order a person to submit computer data under his control and a service provider to submit subscriber information under his control, search and seizure of stored computer data, real-time collection of traffic data and interception of content data.

Concerning the substantive penal law, the draft Convention (Chapter II section 1) requests parties to consider specific acts as crimes with all consequences, in particular the exercise of specific investigative powers that usually exist for criminal investigations. This is for example the case for illegal access to computer data, illegal interception, misuse of devices such as computer programs or passwords, computer related forgery and fraud, offences related to child pornography or infringements of copyright and related rights. The Working Party regrets that no provision is made on the incrimination of violation of data protection rules.

Human Rights, Privacy and Data Protection

The preamble of the draft Convention refers to the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), to the 1966 United Nations International Covenant on Civil and Political Rights, (in brackets) to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and (in brackets) to Recommendation N° R (87) 15 regulating the use of personal data in the police sector.

However, the draft Convention does not harmonise the safeguards and conditions that shall apply to the measures envisaged on the basis of the texts referred to. Though the draft convention (article 15) mentions in the context of procedural law that the “establishment, implementation and application of the powers and procedures provided in this section (Chapter II section 2), shall be subject to the conditions and safeguards provided for under the domestic law of each Party concerned”, it does not require such safeguards and conditions effectively being in place.

Council of Europe countries are obliged to implement the ECHR (granting the right to privacy and data protection, secrecy of correspondence, fair trial, no punishment without law, freedom of expression and imposing precise conditions in clear legal texts to lawfully limit those rights) and other relevant instruments. They must therefore have safeguards and conditions in place, though the concrete nature and scope of those may not be identical in all member countries. However, since the draft Convention is intended to be signed also by non-Council of Europe countries, those countries are not subject to the same obligations as the Council of Europe members and this draft convention does not oblige them to introduce safeguards and conditions in accordance with International Human Rights texts.

Furthermore, the formulation in article 15 of the draft Convention could create the impression that the protection of human rights shall only be considered when it is “due” and shall only be “adequate”. Furthermore, considerations on the proportionality of the powers or procedure to the nature and circumstances of the offence are not referred to as a matter of principle but only “where applicable”. If this could be interpreted as limiting the safeguards and procedures, it would considerably lower, if not fully undermine, the protection of fundamental rights.

In Chapter III on International Co-operation, there is a similar lack of harmonisation of the conditions and safeguards. Some of the obligations to help the requesting party are subject to the conditions and safeguards provided for under national law (real-time collection of traffic data and interceptions of content data)⁵. The other obligations are not subject to any further conditions. This means that a Council of Europe member could not refuse co-operation. It could only do so in the two cases where violation of its “*ordre public*” is recognised as a ground for refusal⁶. And the requirement of dual criminality (another very important safeguard) can only be invoked in limited cases⁷. As a result, in general and irrespective of national or wider concepts on safeguards and conditions, the requested party shall deliver the information, material etc. as requested by the other party. This is a desirable objective in terms of effective law enforcement and fight against crime. However, it may not pass the test of necessity, appropriateness and proportionality as required by Human Rights instruments implemented into constitutional and specific national law.

In this context, the Working Party also notes that throughout the draft Convention⁸, reference is made to “law and *other measures*” that the signatories are obliged to take in order to implement the Convention. The Working Party would like to draw the attention of the Council of Europe, in particular its instances currently dealing with the draft, and all potential signatories to the fact that these terms have to be interpreted in the light of the jurisprudence of the European Court of Human Rights if the measures based on them are to be lawful limitations of the fundamental rights and freedoms.

Several EU Member States implement Directive 95/46/EC also in the “third pillar”, i.e. for processing of personal data in criminal matters. Their national laws thus require that personal data can in principle only be sent to non-EU countries if this country does provide an adequate level of protection of individuals with regard to the processing of their personal data. These countries therefore need to be able to check the adequacy of the level of protection in the third country. In case no adequate protection is found, a transfer of personal data may nevertheless be necessary to fight against crime. National law may have provided for this by allowing exceptions to the principle of adequacy. The same need to set conditions may arise in other countries on the basis of their constitutional and procedural laws. Therefore, the draft Convention should, as a bare minimum, provide for the possibility to reconcile both objectives by allowing the requested party to impose specific safeguards and conditions in order make the transfer happen. Otherwise, conflicts could arise between the obligation to assist and the obligation to respect fundamental rights as granted by the European instruments and relevant jurisprudence.

Apparently Article 27bis together with Article 27(6) are intended to address this issue, but it is not fully clear how. Article 27bis as such does not explicitly mention personal data protection but “confidentiality and limitation on use” concerning “information or material”. It provides only for the possibility (“may”, no obligation) that the requested party subjects the furnishing of information or material to confidentiality or use

⁵ see articles 33 and 34 of draft convention.

⁶ See article 27 (4b) in case no mutual legal assistance treaty applies but this chapter of the draft convention. See article 29 (5b) for expedited preservation of stored computer data and article 30 (2b) for expedited disclosure of preserved traffic data.

⁷ See article 29 (3) and (4) regarding expedited preservation of stored computer data and article 30 on expedited disclosure of preserved traffic data.

⁸ See articles 14, 16, 17, 18, 19, 20 on real time collection of traffic data (i.e. without a warrant or similar basis), 21 on interception of content data, 23 and 26 of the draft Convention.

limitations. At the same time, these possibilities seem to be substantially restricted: as footnote 48 indicates, confidentiality may not be granted if procedural law requires publication. Footnote 49 explains that Article 27bis is without prejudice to Article 27 on mutual assistance in the absence of international agreements. Article 27 (4) allows to refuse mutual assistance for the reasons enumerated there such as if the execution of the request is likely to prejudice its “*ordre public*”, sovereignty, security or other essential interests. Before refusing or postponing assistance, the requested party shall consider whether the request may be granted partially or subject to conditions (Article 27 (6)). However, it is unclear whether data protection conditions could be based on this provision since it is related to the grounds for refusal enumerated in Article 27 (4) which do not necessarily include data protection.

The Working Party is of the opinion that these provisions and their limitations are not sufficient to fully safeguard the fundamental rights to privacy and personal data protection. Citizens may not be able to foresee when and how their fundamental rights are to be restricted. The draft Convention should therefore contain at least data protection provisions outlining the protection that must be afforded to individuals who are subject of all the measures envisaged in the draft Convention. In addition, signatories should be requested to sign up to the Council of Europe’s Convention 108⁹ which is open for non-Council of Europe countries.

In particular Article 27bis and its relation to Article 27 (4) and (6) should be clarified in light of the preceding comments. In view of the fact that Directive 95/46/EC is typically implemented in a seamless way, i.e. including the processing of personal data in the “third pillar”, there are strong arguments to conclude that the notion of “*ordre public*” may also cover situations where an inadequate level of protection of individuals with regard to the processing of their personal data in a requesting country would jeopardize the rights and freedoms of the persons concerned. In this context, explicit reference is made to the fact that the right to the protection of one’s personal data has recently been laid down in Article 8 of the EU Charter of Fundamental Rights. The existence or non-existence of an adequate level of protection in a third country is also mentioned in the Europol Convention as an important criterion to decide on whether, and if so to what extent, personal data may be communicated by Europol to that third country for law enforcement purposes.

Whilst Article 27bis, if clarified and amended as suggested, may go some way towards addressing confidentiality and purpose limitation issues in the specific context of transfer of personal data to non Council of Europe or non EU countries, it is the Working Party’s view that a signatory commitment to satisfying the requirements of Article 27bis will not necessarily constitute an adequate commitment to privacy (see above). The inclusion of data protection provisions will help to codify and clarify the test to be made regarding necessity, appropriateness and proportionality required by the instruments cited above.

It is also the Working Party’s view that signatories to the convention must satisfy the requirements of data protection provisions prior to being considered to provide an adequate level of protection for the rights and freedoms of data subjects. Such an approach will assist in ensuring harmonisation of the safeguards and conditions that shall apply to the measures envisaged in the draft convention. If a party in a third country is to

⁹ This proposal follows the Schengen model where mutual assistance among police services for specific purposes and the exchange of personal data are based on the adherence to Convention 108 and data protection provision in the Schengen agreement itself.

enjoy the benefits of a transfer of personal data to it, it must accept proper responsibility for ensuring that the fundamental rights of the individuals concerned are adequately protected once the data have been received.

Traffic data

The Working Party welcomes that, contrary to previous drafts, the current version of the Convention (version n° 25) does not include anymore a general surveillance obligation consisting in the routine retention of all traffic data. This is in line with the Working Party's Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, adopted on 7 September 1999¹⁰, which explains the legal arguments¹¹ opposing such general obligation.

Also the EU Data Protection Commissioners at their Spring 2000 Conference in Stockholm took a strong position against such measure. They adopted a resolution expressing that they "note with concern proposals that ISPs should routinely retain traffic data beyond the requirements of billing purposes in order to permit access by law enforcement bodies. The Conference emphasises that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights. Where traffic data are to be retained in specific cases, there must be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law."

The views on this issue are converging. Other institutions and groups such as the International Working Group on Data Protection in Telecommunications in its Common Position on data protection aspects in the draft convention¹² have also expressed substantial reservations.

Nevertheless, the provisions in the draft Convention concerning traffic data raise serious concerns: Articles 29 and 30 on expedited preservation and disclosure of traffic and other data do not provide for the possibility for the requested party to refuse such assistance for data protection reasons, but only for the similar general grounds as discussed above ("*ordre public*" etc.). At the same time, the obligations that stored computer data and traffic data are to be preserved upon request for at least 60 days in order to allow a decision being taken on why they are needed and how they should be used, present a considerable burden on business (telecommunications operators, internet service providers and all others) and private persons. Similar concerns apply to Article 20 which obliges service providers to collect or record within their technical capability traffic data in real-time.

Generally speaking, business may need more legal security as to their obligations and their concrete implementation. They may fear that consumers cannot have sufficient trust and confidence in their products and services in case it is not clear who and when does access confidential information and communications.

¹⁰ Available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

¹¹ Referring in particular to Directive 97/66/EC.

¹² International Working Group on Data Protection in Telecommunications, Common Position on Data Protection aspects in the Draft Convention on Cyber-crime of the Council of Europe, adopted at its 28th meeting on 13/14 September 2000 in Berlin,. Available at: http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm.

Conclusions

The Working Party emphasises the Council of Europe's important role as efficient guardian of fundamental rights and freedoms for decades. The Working Party takes the view that the Council of Europe, in promoting international co-operation in matters of cyber-crime outside its own membership, needs to pay particular attention to the protection of fundamental rights and freedoms, especially the right to privacy and personal data protection.

The Working Party therefore sees a need for clarification of the text of the articles of the draft convention because their wording is often too vague and confusing and may not qualify as a sufficient basis for relevant laws and mandatory measures that are intended to lawfully limit fundamental rights and freedoms. Explanations in the explanatory memorandum cannot replace legal clarity of the text itself.

Most of the provisions of the draft Convention have a strong impact on the fundamental rights to privacy and personal data protection. As described above, the choices expressed in the current text of the draft Convention do, to a certain extent, anticipate the result of the examination necessary if the fundamental right to privacy (Article 8 of ECHR) and others are to be restricted¹³. One of the basic questions in this respect is whether a measure is necessary in a specific case, if so, whether it is appropriate, proportionate and not excessive. Some of the elements of the draft Convention are completely new and their impact on the fundamental rights, in particular the right to privacy and data protection, may not have been sufficiently evaluated by the committee of experts on crime in cyber-space (PC-CY). The Working Party sees a need to improve the justification of the measures envisaged in terms of necessity, appropriateness and proportionality as required by the Human Rights and Data Protection instruments referred to above.

The Working Party strongly recommends that the draft Convention should contain data protection provisions outlining the protections that must be afforded to individuals who are subject of the information to be processed in connection with all the measures envisaged in the draft Convention. Article 27bis should also be included (thus delete the brackets) and improved as indicated. The inclusion of data protection provisions will help to codify and clarify the requirements of necessity, appropriateness and proportionality required by the 'acquis' of the Council of Europe and EU Member States.

The Working Party is furthermore of the opinion that the reference to Convention 108 should be included into the preamble (thus the brackets to be deleted), though this has no binding effect, and signatories to the Cyber crime Convention should be invited to sign up to Convention 108 on the Protection of Individuals with regard to Automated Processing of Personal Data.

Furthermore, the Working Party regrets that no provision is made in the draft Convention on the incrimination of violations of data protection rules.

The Working Party sees a discrepancy in treatment of Council of Europe countries and others because Council of Europe members have to respect their obligations following from the European Convention Human Rights, Convention 108, relevant Council of

¹³ For example interception of communications and traffic data fully break the secrecy of correspondence (see Malone judgement of the European Court of Human Rights).

Europe Recommendations, the EU Charter on Fundamental Rights, the EU Data Protection Directives and relevant national legislation whereas non Council of Europe countries have, on the basis of the current draft convention, not the same or similar obligations.

The Working Party furthermore takes the view that signatories to the Convention must accept proper responsibility for ensuring that the fundamental rights of individuals are adequately protected once the data concerning them have been received from the European Union and Council of Europe member countries.

The position proposed in the current draft convention (public version 25) not to oblige signatories to compel service providers to retain traffic data of all communications should in no way be revised.

The Working Party regrets the very late release of relevant documents. The Working Party considers it highly desirable that the public debate be prolonged involving all parties concerned (human rights organisations, industry etc.) before the Parliamentary Assembly of the Council of Europe debates and decides.

The Working Party is of the view that a large number of the deficiencies highlighted before in this opinion, apparently result from the fact that the Council of Europe has not made the best possible use of the available expertise in data protection matters. The Working Party therefore invites the Council of Europe, and especially the EU Member States, to consult their data protection experts before finalising their position on the draft Convention, and to make the best possible use of their contributions.

The Working Party invites the Council of Europe, the European Commission, the European Parliament and Member States to take into account this opinion.

The Working Party reserves the possibility to issue further comments.

Done at Brussels, 22nd March 2001

For the Working Party

The Chairman

Stefano RODOTA