5005/99/FINAL
WP 18

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

Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications

Adopted on 3 May 1999

Recommendation on
the Respect of Privacy in the context of Interception of Telecommunications

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

Instituted by Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995[1] ,

Having regard to Articles 29 and 30 paragraphs 1 and 3 of the above-mentioned Directive[2],

Having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

Has adopted the present recommendation:

The purpose of this recommendation is to indicate how the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence, is to be applied to the measures concerning the interception of telecommunications adopted at European level.

This recommendation covers interception understood in a broad sense, i.e. not only of the contents of telecommunications, but also of any related data, particularly any preparatory measures (such as monitoring and datamining traffic data) which may be envisaged in order to determine whether intercepting the contents of a telecommunication is advisable[3].

A. Scope of the provisions on the interception of telecommunications adopted at European level

1. The Council Resolution of 17 January 1995 on the lawful interception of telecommunications[4] lists the technical conditions required for the interception of

---

[1] Directive of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 of 23.11.1995, p. 31.

[2] The three members representing the Registertilsynet (Denmark), the Commission Nationale de l'Informatique et des Libertés (CNIL, France) and the Data Protection Registrar (United Kingdom) respectively, did not take part in the vote on this recommendation, as they consider the topic addressed to be outside the Working Party's remit. Nonetheless, they support the general substance of the recommendation.

[3] Interception understood in this broad sense fits the scope of the Council Resolution of 17 January 1995 on the legal interception of telecommunications, quoted below (Chapter A.1), and the general framework of the relevant legal provisions (see below, Chapter B).
The recommendation also applies to the interception of non-public telecommunications on the Internet. The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data is paying particular attention to the general problem of the processing of personal data linked to the development of the Internet, within the framework of work being done simultaneously by the party's Internet task force.

[4] OJ C 329 of 4.11.1996.

telecommunications, without going into the conditions under which such interception may be permitted. The Resolution requires network operators or service providers to pass the intercepted data on to the "authorised services" in plain text.

The data concern telephone calls, whether from mobiles or conventional units, e-mail, faxes and telex messages, and Internet data traffic, with regard to both content and any data related to telecommunications (this refers particularly to traffic data, but also to any signal transmitted by the person under surveillance – point 1.4.4. of the Resolution).

Data are to be collected both on the target persons and on any persons with whom they enter into communication[5].

The Resolution also provides for law enforcement agencies to have access to data on the geographical location of a mobile subscriber[6].

The Resolution of 18 January 1995 is currently being revised, with one of the main goals being to adapt it to new communication technologies. In particular, the draft text addresses how to apply interception measures to satellite telecommunications[7].

2. The Working Party is concerned about the scope of the measures envisaged by the Council Resolution of 17 January 1995. An unpublished, more recent version of the document referred to above ("declaration of intent" dated 25 October 1995), provides for the signatories to the text to contact the director of the United States Federal Bureau of Investigation about the requirements for the interception of telecommunications. The text also provides, subject to the approval of the "participants", for other States to take part in the exchange of information and in the revision and updating of the requirements.

   The Working Party points out that the legal status of this text is unclear – particularly as regards the actual signing by the countries concerned – and that it does not constitute a measure accessible to the citizen according to the case law of the European Court of Human Rights quoted below, insofar as it has not been published. Secondly, the text notes a desire to develop technical measures for intercepting telecommunications jointly with States which are not subject to the requirements of the European Convention on Human Rights and of Directives 95/46/EC and 97/66/EC.

---

[5] Point 1.4 of the annex to the Council Resolution of 17 January 1995.

[6] Point 1.5, op. cit.

[7] Document 10951/1/98, ENFOPOL 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enfo/6332/1.htm). It seems that a yet more recent version has been agreed by the Council's Working Party on Police Cooperation and has been forwarded to the European Parliament to be adopted or amended. Apparently the new resolution is to be adopted by the Council on 27 and 28 May 1999 (see "Datenschutz-Berater", 15.02.99, p. 5, which refers to a non-public version of 20.02.99). The European Parliament's Committee on Legal Affairs and Citizen's Rights recommended that the Committee on Civil Liberties and Internal Affairs (which is primarily responsible) reject the draft revision of the Council's recommendation under the form it takes in ENFOPOL 98, amongst other things, because of a threat to privacy and because the Treaty of Amsterdam was coming into force soon thereafter (see Mr Florio's report). The Committee on Civil Liberties did not accept this recommendation and will therefore propose that ENFOPOL 98 be approved at the plenary session, according to Mr Schmid's report. The European Parliament should make its decision in early May.

3. The Working Party notes that the Council Resolution aims to settle technical questions on the means of intercepting communications, without affecting the national provisions which regulate phone tapping in legal terms. Nonetheless, certain measures the resolution provides for, which increase the scope for intercepting telecommunications, conflict with the more restrictive national regulations of certain countries in the European Union (particularly point 1.4, access to data concerning calls, including calls from mobile phones, without considering the anonymous prepaid services now available; point 1.5, geographical location of mobile subscribers, and point 5.1, forbidding operators from disclosing interceptions after the fact.)

4. Although the Council Resolution is in line with an aim of "the protection of national interests, national security and the investigation of serious crimes", the Working Party wishes to draw attention to the risks of abuses with regard to the objectives of tapping, risks which would be increased by an extension to a growing number of countries – some of which are outside the European Union – of the techniques for intercepting and deciphering telecommunications.

   A European Parliament resolution of 16 September 1998 relating to transatlantic communications[8] "considers that the increasing importance of the Internet network, and more generally of telecommunications on a world-wide scale and in particular the Echelon system, as well as the risks of their abuse, call for the adoption of measures to protect economic information and effective encoding."

   These considerations highlight the risks associated with telecommunication interceptions which go beyond the strict framework of questions of national security – and thus fall outside the European Union's "third pillar". They raise the question of their legitimacy, in particular in the light of the obligations arising from Community legislation on the protection of the fundamental rights and freedoms of natural persons, particularly their privacy.

5. The Working Party emphasises, finally, that as a result of the Treaty of Amsterdam coming into force, the legal basis of provisions for the interception of telecommunications will change at European level. The basis for the Council to draw up the resolution (currently articles K.1 (9) and K.3 (2) of the Treaty on police and judicial co-operation), will include powers of initiative of the European Commission under the new article K.6 (2).

B. General Legal Framework

6. The Working Party points out that each telecommunication interception, defined as a third party acquiring knowledge of the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunication services, constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows

[8] Plenary session, minutes part II, B4-0803, 0805, 0806 and 0809/98.

that interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950[9], and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention[10].

The legal basis must precisely define the limits and the means of applying the measure through clear and detailed rules which are particularly necessary owing to the continuous improvement of the technical means available[11]. The text of the law must be accessible to the public so that citizens may be informed of the consequences of their behaviour[12].

In this legal context, exploratory or general surveillance on a large scale must be proscribed[13].

7. Within the European Union, Directive 95/46/EC[14] establishes the principle of the protection of the right to privacy enshrined in the legal systems of the Member States.

---

[9] It should be stressed that the fundamental guarantees recognised by the Council of Europe on the interception of telecommunications create obligations for Member States regardless of the distinctions made at European Union level according to the Community or intergovernmental nature of the fields addressed.

[10] Council of Europe Convention No 108 also stipulates that interference may be tolerated only when it constitutes a necessary measure in a democratic society for the protection of the national interests listed in Article 9 (2) of that Convention (NB the national interests listed in Convention 108 and in the Convention for the Protection of Human Rights are not exactly the same), and when it is strictly defined in terms of this purpose.

[11] See below for the obligations under Article 4 of Council of Europe Recommendation No 4 of 7 February 1995 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.

[12] Judgments in the cases of Huvig and Kruslin v. France of 25 April 1990, Series A No 176-A &176-B, pp. 15 et seq.

[13] See especially the Klass judgment of 6 September 1978, Series A No 28, pp.23 et seq., and the Malone judgment of 2 August 1984, Series A No. 82, pp. 30 et seq.

The Klass judgment, like the Leander judgment of 25 February 1987, insists on the need for "effective guarantees against abuse" "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it". (Leander judgment, Series A No. 116, pp. 14 et seq.).

The Court notes in the Klass judgment (paragraphs 50 et seq.) that assessing the existence of adequate and effective guarantees against abuse depends on all the circumstances of the case. In the particular case, it considers that the surveillance measures provided for in German legislation do not permit exploratory or general surveillance and do not contravene Article 8 of the European Convention for the Protection of Human Rights. German legislation provides the following guarantees: surveillance is confined to cases in which there are indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may be ordered only if the establishment of the facts by another method is without prospects of success or considerably more difficult; and even then, the surveillance may cover only the specific suspect or his presumed "contact-persons".

[14] Note that Article 3 of Directive 95/46/EC excludes from its field of application the processing of personal data in the course of an activity which falls outside the scope of Community law and processing

This Directive specifies the principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC[15] gives concrete expression to the provisions of this Directive by specifying the Member States' obligation to ensure through national regulations the confidentiality of communications carried out by means of a public telecommunications network or by means of publicly available telecommunication services.

According to Article 13 (1) of Directive 95/46/EC, Member States may adopt legislative measures to restrict the scope of certain obligations (for example, concerning the collection of data) and certain rights (for example, the right to be informed of data collection) provided for in the Directive[16]. These exceptions are strictly enumerated: the restriction must constitute a measure needed to safeguard the public interests exhaustively listed in paragraphs a) to g) of this article, which include national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

Article 14 (1) of Directive 97/66/EC similarly states that Member States may only restrict the obligation of the confidentiality of communications on public networks when such a measure is required to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.

C. Obligations of Telecommunications Operators and Service Providers

8. It must be stressed that the obligations of the security and confidentiality of data to which telecommunication operators, service providers and Member States are subject on the basis of Articles 17 (1) and (2) of Directive 95/46 and Articles 4, 5 and 6 of Directive 97/66/EC respectively are the rule and not the exception.

The Working Party points out that these obligations also apply to operators in general under Article 7 of Council of Europe Convention No. 108 of 28 January 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data, and Article 4 of the Council of Europe Recommendation No. 4 of 7 February 1995 on the

---

operations concerning public security, defence, State security and the activities of the State in areas of criminal law. Up to now, most Member States who have transposed the Directive do not make any distinction in their national legislation whereby this law would not be applicable to matters not covered by Community law.

In addition, the provisions of Community law are applicable in cases where data are processed according to the directive (for example, a list of calls recorded by an operator for billing purposes) but are subsequently intercepted. Directive 95/46/EC provides for a number of guarantees, detailed below, which must be respected in the event of such interception.

[15] Directive of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30 January 1998, p. 1.

[16] Laid down in Article 6(1) (principles relating to the quality of data), Article 10, Article 11(1) (information of the data subject) and Articles 12 (right of access) and 21 (publicising of processing operations).

Protection of Personal Data in the Field of Telecommunication Services, with particular regard to telephone services[17].

9. These obligations imply that telecommunications operators and telecommunications service providers may not process data on telecommunications traffic and billing except under certain conditions: given that traffic data on subscribers and users must be erased or made anonymous as soon as the communication ends, it follows that the purposes for which the data may be processed, the length of time they may be kept (if at all) and access to them must be strictly limited[18].

10. Telecommunications operators and telecommunications service providers must take the measures needed to make the interception of telecommunications by unauthorised parties impossible, or as technically difficult as the current state of the technology allows.

    The Working Party stresses in this respect that the implementation of effective means of intercepting communications, using precisely the most advanced techniques, must not result in a lowering of the level of confidentiality of communication and protection of the privacy of individuals.

    These obligations take on a special meaning when telecommunications between individuals located on the territory of the Member States pass or may pass outside European territory, in particular when satellites or the Internet are used.

11. Where Directive 95/46 applies, making such telecommunications accessible outside the European Union could moreover constitute a violation of Article 25 of the

---

[17] "4.1. Personal data collected and processed by network operators or service providers should not be communicated, unless the subscriber concerned has given his express and informed consent in writing and the information communicated does not make it possible to identify the subscribers called.

The subscriber may revoke his consent at any time but without retroactive effect.

4.2. Personal data collected and processed by network operators or service providers may be communicated to public authorities when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

4.3. In cases of communication to public authorities of personal data, domestic law should regulate:

a. the exercise of rights of access and rectification by the data subject;

b. the conditions under which the competent public authorities shall be entitled to refuse to give information to the data subject or to defer the issue thereof;

c. conservation or destruction of such data."

[18] See in particular the obligations imposed by Article 6 of Directive 97/66/EC.
These obligations raise questions about some practices which are currently becoming common among telecommunications providers, i.e. examining the overall traffic data of subscribers ahead of time, in order to identify certain subscribers' suspicious behaviour – and possibly allow targeted interception of the content of certain telecommunications.

Directive, insofar as foreign authorities intercepting them may not be able to ensure an adequate level of data protection.

D. Respect of Fundamental Freedoms by the Authorities with regard to Interceptions

9. Taking into account the above-mentioned provisions, it is important for national law to strictly specify:

- ✓ the authorities responsible for permitting the legal interception of telecommunications, those authorised to carry them out and the legal basis for their action,
- ✓ the purposes for which such interception may be carried out, which allow an assessment of whether it is proportionate to the national interests at stake,
- ✓ the prohibition of all large-scale exploratory or general surveillance of telecommunications,
- ✓ the exact circumstances and conditions (for example, facts justifying the measure, duration of the measure) governing the interceptions, without violating the principle of specificity which any interference in the privacy of individuals must respect[19],
- ✓ compliance with the principle of specificity, which is a corollary of forbidding all exploratory or general surveillance. Specifically, as far as traffic data are concerned, it implies that the public authorities may only have access to these data on a case-by-case basis, and never proactively and as a general rule.
- ✓ the security measures for the processing and storage of the data, and the length of time data may be kept,
- ✓ the guarantees concerning the processing of data concerning individuals affected indirectly or by chance[20] by interceptions, in particular the criteria used to justify the conservation of data, and under what conditions these data may be passed on to third parties,
- ✓ that a person under surveillance be informed of this as soon as possible[21],
- ✓ the recourse available to a person under surveillance[22],

---

[19] See above, note 13.

[20] The data concerned refer to individuals who are not under surveillance, but who enter into communication with someone who is. For example, the telephone number of a relative, dialled by the person under surveillance; geographical location of people in contact by mobile phone with a person under surveillance.

[21] It should be possible to inform the person under surveillance if doing so does not hinder the investigation, or as soon as it ceases to do so.

[22] The Leander judgment quoted above points out that the authority to which an appeal may be made "need not necessarily be a judicial authority in the strict sense, but that the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy is effective" (83). This "must mean a remedy that is as effective as can be, having regard to the restricted scope for recourse inherent in any system of secret surveillance for the protection of national security" (84).

- ✓ the arrangements for the monitoring of these services by an independent supervisory authority[23].
- ✓ publication of the policies on the interception of telecommunications as they are actually practiced[24], for example, in the form of regular statistical reports,
- ✓ the specific conditions under which the data may be transmitted to third parties under bilateral or multilateral agreements.

Done at Brussels, 3 May 1999

For the Working Party

The Chairman

P.J. HUSTINX

[23] The Leander judgment refers to democratic supervision of interceptions when it specifies that "The supervision of the proper implementation of the system is, leaving aside the controls exercised by the Government themselves, entrusted both to Parliament and to independent institutions" (64).

[24] The obligation to make the information public, as well as the specific need for an independent authority to supervise interceptions, are mentioned in the "Common position on public accountability in relation to interception of private communications" adopted in Hong Kong on 15 April 1998 by the international working party on data protection in the telecommunications sector.