5042/00/EN/FINAL
WP36

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

Opinion 7/2000

On the European Commission 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 of 12 July 2000 COM (2000) 385

Adopted on 2nd November 2000

set up 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 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12, 13 and 14 thereof,

has adopted the present Opinion 7/2000:

1. Introduction

In the context of the 1999 review of the Community's telecommunications regulatory framework[2], the Commission has adopted on 12 July 2000 proposals for new Directives in the area of electronic communications, intended to replace the existing regulatory framework. One of the five envisaged proposals concerns a revision of Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector.

Following its Opinion 2/2000 concerning the general review of the telecommunications legal framework[3], the Working Party now wishes to contribute to the discussions on the draft directive in the European Parliament and in the Council.

2. Analysis of the draft directive

The Working Party's main concerns relate to personal data processing over and via the Internet that needs to be addressed in a more specific way as well as to new issues arising from the liberalised telecommunications market.

Article 1 - Objective and Scope and Article 3 – Services concerned

The Working Party understands that no change is proposed as to the scope and services concerned. The specific provisions of the new directive would thus apply to the provision of *publicly* available electronic communications services in *public* communication networks in the Community. Personal data processing for the use of closed/private

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

[2] The 1999 Review was launched by a Commission Communication in November 1999 followed by a broad public consultation. The results of this consultation were summarised in a second Communication adopted by the Commission on 26 April. All documents concerning the review and the draft directives are available at: http://www.ispo.cec.be/infosoc/telecompolicy/review99/Welcome.html

[3] All documents adopted by the Working Party are available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

networks would fall solely under the general Directive 95/46/EC. This is regrettable because private networks are gaining an increasing importance in every day life and communications of citizens, for example in the context of their work, and the risks to privacy that such networks are raising are accordingly increasing and becoming more specific (e.g. monitoring of employee behaviour by means of traffic data, lack of confidentiality of communications).

Processing of personal data in connection with the delivery of *services* using public communication services and networks[4] such as the content of broadcasting transmission and Information Society services is not covered either by the proposed new directive. This means that data processing in the latter case is subject only to Directive 95/46/EC as are all matters not covered by the specific privacy directive (see recital 9 which is identical to the relevant recital of the present Directive 97/66/EC).

However, interactive television services would be covered.[5]

These points could usefully be clarified either in the text of the relevant articles of the various directives or in the recitals.

Article 2 – Definitions

The Working Party welcomes the effort to clarify terminology. It notes that the proposed directive accommodates the view the Working Party had taken in its Working Document: Processing of Personal Data on the Internet that both Data Protection Directives fully apply to data processing on the Internet[6].

Traffic data are defined as *« any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network*". This definition does not contain a "necessity" clause. The Working Party welcomes this approach which leads to the result that all traffic data generated during a communication, whether they are necessary to establish the communication or not, have to be erased as soon as the communication is transmitted (see Article 6 paragraph 1). The definition includes location data generated during the transmission of a communication. It also includes "navigation data " (such as URLs/Unique Resource Locator) which might reveal an individual's personal interests (e.g. web sites visited that give indications about an individual's religious beliefs, political opinions, health or sex life). Because they show precisely which pages on a web site have been visited they effectively reveal the actual content that the individual has accessed.

[4] This follows from *Article* 3 of this draft directive and *Article* 2 of the draft directive on the general framework. The Working Party notes that "public communications service" is not defined in either document and that the definition of "electronic communications service" in the draft directive on privacy is not complete compared to the one in the framework text.

[5] It would also be useful to know whether text messaging in mobile phones is covered.

[6] See Article 2-definitions, draft recital (5), Article-3 services concerned, as well as definition of "electronic communications networks "in the document on a framework where "IP networks" could be added to the examples given.

Since traffic data might include this kind of personal information on the individual, they should in addition enjoy the confidentiality provided for communications (see Article 5 and below).[7]

The Working Party understands that the proposed definition of "call" does not cover voice telephony over the Internet but only traditional circuit switched voice telephony.

Although the Working Party welcomes the way in which the proposed directive defines "call", it emphasises that it will continue to take the view that in the existing Directive 97/66/EC "call" includes use of the Internet. This view seems to be shared by the European Commission as follows from the explanatory memorandum to the draft directive.

The Working Party notes that the term "subscriber" is not defined anymore though it is used throughout the draft directive. Instead the term "user" is defined, but excludes legal persons. The Working Party would like to know the reasons for these changes.

The draft directive no longer refers to "telecommunications services", but to "electronic communications services". The explanatory memorandum to the proposal mentions that this change was necessary to align the terminology with the proposed directive establishing a common framework for electronic communications services and networks[8].

The term "electronic communications services" is not defined in the proposed privacy directive but in Article 2 b) of the proposed directive establishing a common framework for electronic communications services and networks.

The new definition reads as follows: *Electronic communications services means services provided for remuneration which consist wholly or mainly in the transmission and routing of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.*

The new definition is actually based on the same core idea as the previous one (the transmission and routing of signals on electronic communications services) but the inclusion of a list of examples of services included and excluded from the definition is very helpful as it sheds light on the discussions outlined in the previous sections.

It can be concluded from the list included in the new definition that those who provide content transmitted using electronic communications networks and services will not fall within the scope of application of the privacy draft directive. This is confirmed by the preamble to the proposed directive establishing a common framework for electronic communications services and networks (recital 7) in which it is stated that *it is necessary to separate the regulation of transmission from the regulation of content.* It is, however, stated that this separation should not overlook the links existing between them.

The main consequence of this separation is that additional services such as those which provide content to a *portal* or a web site (but not host them) are covered not by this

[7] An additional aspect that would need further discussion is that some of these data could also be considered as sensitive data in the sense of Article 8 of the general Data Protection Directive 95/46/EC, the processing of which is in principle prohibited.

[8] COM (2000) 393.

directive, but only by the general data protection directive. It also means that *Internet Service Provider*s are covered by the specific directive insofar as they act as Access Providers and provide connection to the Internet, and are only covered by the general directive when acting as content providers.

The advantage of the clear separation between regulation of content and transmission is the clarity that it brings with it. In practice, however, it will be less easy to work with such a separation (for example in case an *Internet Service Provider* that also provides content, by hosting its own *portal site.* This *ISP* will then have to apply the general directive to all its activities and the specific directive (which entails specific obligations) to the activities in which it plays the role of access provider.

Another interesting aspect of the new definition of "electronic communications services" is the reference to the fact that the service should be provided for remuneration. Neither the preamble nor the explanatory memorandum refer to the inclusion of this term or give any guidance as to how to interpret it. This could be interpreted as meaning that Free Access Providers would fall outside the scope of application of the revised privacy and telecommunications directive, as they do not receive remuneration (or at least not financial) from Internet users.

This interpretation is however not correct since it has been made clear in the jurisprudence of the European Court of Justice, when dealing with services in the sense of article 50 (ex article 60) of the EC Treaty[9], that the remuneration does not necessarily has to be paid by the recipient of the service. It can for instance also be paid by advertisers.

In the case of the Free Access Providers, those who place advertisements or banners in the Internet pages are the ones who in fact offer a remuneration to the providers. It is therefore clear that these services fall under the definition of electronic communications service and therefore under the scope of the directive.

It would however be desirable to clarify this issue in the text of the directive since no every reader of the text is aware of the interpretation of this term given by the European Court of Justice.[10].

Article 4 – Security

The Working Party welcomes the explanation in recital (13) as regards security measures such as encryption. It proposes to consider the need for more specific obligations on network operators and service providers on the basis of an analysis of national laws implementing security requirements with a view to facilitating free flow of data and equipment (software and hardware). It would also be useful to indicate more specifically the risks at stake, and this not only concerning the Internet, but also other communication environments since the security obligations are imposed on all network and service providers.

Article 5 – Confidentiality of Communications

The Working Party recalls the commonly shared view that confidentiality of communications is part of the most important elements of the protection of the

[9] Case C-109/92 Wirth [1993] ECR I-6447 , 15.

[10] This could be done for instance by adding the word "*normally* against remuneration" in the text of the definition and to explain in the respective recital the meaning of these terms in the sense of the jurisprudence cited above.

fundamental right to privacy and data protection as well as of secrecy of communications. Any exception to this right and obligation should be limited to what is strictly necessary in a democratic society and clearly defined by law in accordance with the conditions set out in Article 15 and Article 13 of Directive 95/46/EC.

Since the wording of the proposed Article 5 par. 2 is too vague and thus allows exemptions to confidentiality without respecting the basic conditions, this paragraph should be deleted.

In this context, the Working Party recalls its Recommendation 2/99 emphasising that "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."

Confidentiality of communications (including behaviour on the Internet) must be the rule, not the exception.

Article 6 – Traffic data and billing data

The Working Party is of the opinion that the opportunity should be used to review the provision on traffic data more thoroughly. Given the wide definition of traffic data it should be made clear that it is not necessarily acceptable to treat all items of traffic data in the same way. It should be clear for what purposes and to what extent particular types of traffic data (in the sense of the new wider definition) may be generated, collected, stored at all, and for what purposes they might be further used. The Working Party would like to stress that, in case processing be allowed for a specific purpose on the basis of the subscriber's consent, the subscriber does not give up his/her rights to privacy and data protection once and for all. The Working Party also recalls that the level of protection granted by the present Directive 97/66/EC should in any case be maintained, if not strengthened.

Concerning Article 6 (2): On the basis of the current text proposal allowing processing of traffic data which are necessary for billing purposes, the Working Party notes that the draft directive does not propose any harmonisation of the period during which the bill may lawfully be challenged. The Working Party wishes to know how the Commission intends to follow up the Working Party's Recommendation 3/99 which recommended to the European Commission to harmonise this period in order to set a limit to the storage of traffic data for this specified billing purpose with a view to strengthening the fundamental right to privacy of citizens. The Working Party invites the European Parliament and the Council to set a clear time limit which should be the shortest possible. Any processing of traffic data for additional purposes creates new risks to the fundamental right to privacy. It can only be considered provided appropriate safeguards are in place. The Working Party therefore recommends to include a " necessity" test in Article 6 par.3 for the possibility to process traffic data for the provider's own marketing.

As regards the proposal to allow processing of traffic data for the provision of "added value services", the Working Party considers that this term is not clear enough with a

view to guaranteeing the limitation of the purpose. Neither definition nor indications in the recital are given as to the full range of such services. Since the context compared to marketing of the provider's own services is different, different safeguards may be needed.

The Working Party supports the new provision in Article 6 par. 4 concerning the information to be given to the individual. It proposes to add in the relevant recital that the individual also be informed about his right to object to the processing (Article 14 of Directive 95/46/EC).

Article 7 – Itemised billing

The Working Party welcomes the explicit reference to alternative privacy enhancing modalities for itemised billing in the relevant Article. At the same time, it regrets that one of these modalities (deletion of the digits, recital 18 of Directive 97/66/EC) is not mentioned any longer in the draft recital. The Working Party wishes confirmation in the sense that this continues to be a lawful means and recommends its integration into the recital.

Article 9 – Location data

Since more clarity about added value services is needed (see above), the use of location data (traffic data) for such purposes should be examined in the light of the in-depth review of the rules on traffic data as proposed above. In principle location data should not be processed for the provision of added value services. They may be processed exceptionally for clearly specified purposes which technically require that location data are used and provided that safeguards appropriate to the privacy risks are provided.

Without anticipating the Working Party's final view on the substance concerning processing of location data for added value services[11], it considers that the proposed technical possibility to deny the processing of location data as proposed in Article 9 (2) is not a satisfactory solution. Given the sensitivity of location data with respect to freedom of movement and the fact that the location data covered here are not necessary to establish the communication, the user/subscriber must have full control over their processing. The rule should thus be the inverse: the subscriber must have the possibility, via simple means, to freely allow the processing of location data for each delivery of an added value service (including if necessary connection to the network or transmission or a communication). The technical implementation of this right must be embedded within the equipment of the user/subscriber, not in the network (contrary to calling line identification).

Article 10 – Exceptions

The Working Party considers that this Article may need additional safeguards in order to avoid circumvention of the stricter rules in Article 15 together with Article 13 of Directive 95/46/EC. Since the "old" terminology of "call" is maintained here, the Working Party understands that this Article only covers voice telephony over fixed and mobile networks, but excludes voice telephony over the Internet, IP addresses and e-mails.

[11] Or more generally concerning the disclosure of location data to users of the networks.

(a) As regards the proposed possibility to override the choice of the subscriber not to be identified[12]) at subscriber requests in order to trace malicious or nuisance calls, a procedural safeguard should be provided for that guarantees to check whether a call was indeed malicious or nuisance.

(b) The overriding of elimination of CLI and the use of location data against the wish of the subscriber/user or without him/her knowing is not specific enough: firstly it should be clarified which kind of location data (traffic data) are meant here. Secondly, in order to avoid a circumvention of Article 15, the law enforcement agencies that are authorised to respond emergency calls should be specified and the obligation to delete the data after the objective of help is achieved should be laid down.

In this context, the Working Party notes that *Article 22 (3) of the draft directive on universal service and users' rights*[13] obliges "Member States to ensure that network operators make caller location available to emergency services authorities, where technically feasible for all '112' calls." Though there is no doubt that the services ready to rescue persons in emergency situations shall have all the information they need to identify the caller, the Working Party draws the attention of the Commission to the need to ensure coherence with data protection principles. The understanding and definition of "emergency services authorities" should be the same in both texts. And the obligation to provide location data to these authorities should be limited to what is necessary to identify the person in trouble. But given the sensitivity of location data (see comments on Articles 2 and 9 above), it may be worth considering to some extent that the "112" emergency feature should be classified as a service with the consequence that the necessary location data only of those callers who have consented to this service are provided to the "112" emergency number.

Article 12-Directories of Subscribers

The Working Party supports the proposed choice of subscribers to decide whether or not they want to be included in directories in electronic or paper form. In addition, given the dimension of electronic directories in particular in today's information society, subscribers should be informed about possible uses of directories and the data they can include should be limited to what is necessary in order to identify them, but not to reveal more private information.

This requirement is linked to an issue, which is not yet addressed in the draft directive : several Data Protection Authorities are currently handling cases of reverse searches in directories. These are new services in the liberalised telecommunications market and they consist in offering easily and at a low cost extended capabilities for the processing of all information contained in telephone directories. It is for example possible to find out by means of the telephone number the name and address of a given person or the names and telephone numbers of all people living in the same street by means of the name of the street. It is possible to learn much more about an individual than he/she would imagine when accepting to have his/her telephone number in the telephone directory. As much information as usually appears on a business card (full name, address, profession, job) can be found. Moreover, the simple knowledge of a citizen's itemised billing, where only called telephone numbers appear, would allow to get a list of the names and addresses of

[12] Elimination of calling line identification (CLI) means that the subscriber can choose to remain anonymous vis à vis the person receiving the call. Overriding this right means that the caller's line can be identified even against his/her wish. As regards emergency calls, it is proposed that this also applies to location data even in case the subscriber has not given consent to any processing of such data.

[13] Available on the web site indicated in footnote 2.

all persons called by him/her during a specific period of time. Other search products contain geographical information ("location data", see comments above on Articles 2 and 9) such as city maps and databases with photographs of all the dwellings of a city. This information could easily be associated to the address appearing in the telephone directory that allows for multi-criteria search.

This is a new purpose of the directories. which is not compatible with the initial purpose. It is furthermore not legal unless the data subject has given his/her consent to process his/her personal data for such new purposes. The Working Party has adopted a common position on this subject and considers it important that the draft directive explicitly addresses this issue in the sense that the informed consent of the data subject for inclusion of his/her data in public directories for reversed searches is required.

Another important aspect is that directories can be edited by everybody. It is therefore necessary to ensure that transmissions of data from a provider/operator for the purposes of directories or other uses of the data contained therein respect the choices expressed (free of charge) by users/subscribers to the initial provider/operator. The initial provider/operator has to inform the user/subscriber about these uses (commercial use, reverse directories etc.) before the subscription.

Furthermore, the cession of data in form of CD Roms raise an additional problem in some cases as regards the duration of the licence: the duration of the licence should be determined in a way that does not allow the use of data which are outdated as regards the choices made by the persons concerned.

Article 13 – Unsolicited Communications

Spamming is the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact. Spam constitutes a specific form of privacy violation: the user has no human interface, supports the costs of the communication and normally receives spam within the protected area of his private home.

Not surprisingly consumers prefer solicited and targeted commercial communications instead of spam which is annoying, time consuming to read and to delete, and costs money. Nuisance caused by junk e-mailers undermines customer's confidence in e-commerce.

But industry also requests legal certainty: unsolicited e-mail puts ISPs in the unacceptable position of being forced to provide the bandwidth and equipment to deliver junk e-mail that the huge majority of its customers do not want. Removing spam from the servers and dealing with angry customers also involves considerable costs. Systems sometimes collapse under the sheer bulk of unsolicited commercial e-mail that is sent, thereby blocking and delaying legitimate traffic. Most ISPs try to filter out spam and have clauses in their contracts with subscribers that the latter shall not send or relay spam. Registers exist of suspect servers, which are known as source of junk e-mail. But the filters, which they use, are not 100% accurate and they also cause legitimate traffic to be blocked if it is sent from a server which happens to be on the black list. However, since there is no legal ban on spam, this practice puts ISPs in a difficult legal position. A legal ban would facilitate more targeted action against junk e-mailers.

Recent market trends suggest that leading on-line direct marketers in the US operate on the basis of "permission based marketing" (opt-in) because the data provided on that

basis are of better quality and the level of positive responses is significantly higher. Some practice even "double opt-in": though the individual had agreed to receive commercial communications (for example by indicating this wish on a web site), in the following first (solicited) e-mail contact he is again asked to confirm his wish to the marketer

The Internet offers ample opportunities to collect e-mail addresses of users who are interested in receiving commercial communications by e-mail on specific topics and willing to give their consent for that purpose. Any mailings, which are based on consent, are likely to reach far more potential customers than Spam.

In five Member States (Germany, Austria, Italy, Finland and Danemark) it is unlawful to send unsolicited commercial communications . In the other Member States, either an opt-out system exists or the situation is not fully clear. Companies in opt-out countries may target e-mail addresses not only within their own country but as well to consumers in Member States with an opt-in system. Moreover, since e-mail addresses very often give no indication of the country of residence of the recipients, a system of divergent regimes within the internal market does not provide a common solution for the protection of consumer's privacy.

Opt-in is a well-balanced and efficient solution in order to remove obstacles to the provision of commercial communications whilst protecting the fundamental right of privacy of consumers.

The Working Party thus welcomes and supports the proposal to address unsolicited electronic mail in the same way as automatic calling machines and facsimile machines. In all these situations, the subscriber has no human interface and supports parts or the whole of the costs of the communication. The degree of invasion into privacy and the economic burden are comparable (see Opinion 1/2000).

Article 14 – Technical features and standardisation (and recital 22)

The Working Party welcomes and supports the proposal to develop specific measures at Community level if necessary in order to ensure a harmonised implementation of the data protection rules.

Since technology develops in a "bottom up" way, it could be useful to recall industry their interest in integrating privacy-compliant and even privacy-enhancing features right from start into the design of software and hardware. The Working Party takes the view that technology must comply with the legal requirements and facilitate their implementation, in particular the data minimisation principle following from Articles 6 and 7 of Directive 95/46/EC, and the exercise of the data subject's rights. Taking into account experience in various Member States as well as the Working Party's Recommendation 3/97 on Anonymity on the Internet and its Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, it is proposed to add a paragraph along the following lines:

The design and selection of data processing technologies, including hardware and software, shall conform to the objective of processing no or as less personal data as possible and shall facilitate the exercise of the data subject's rights. Where possible and not disproportionate with a view to the protection intended, anonymous and pseudonymous data should be used.

Transparency

The Working Party is of the opinion that, though it is clear that the obligations of the general data protection directive to inform the individual apply[14], it would provide added value to explicitly oblige providers to inform the subscriber/user before the subscription/use and also afterwards about their rights and thus give them the opportunity to exercise at any time all options/rights they have in accordance with the data protection directives. This information concerns the purposes of the intended processing, the controller, the recipients in case a third party is involved, the rights of the individual etc.. It is proposed that the providers/operators publish this information in order to enable the subscriber/user to choose at any time all available options to exercise his/her rights. This could be done for example in form of posting a privacy policy on a web site.

3. Conclusions

The Working Party welcomes the revision aiming at ensuring that the same service is regulated in an equivalent manner irrespective of the means by which it is delivered. This also implies that consumers and users should enjoy the same level of protection concerning their personal data and privacy regardless of the technology by which a particular service is delivered. The Working Party shares and fully supports the Commission's view that maintaining a high level of data protection and privacy for citizens is one of the declared aims. The Working Party furthermore recognises that considerable amount of adaptations are proposed to increase the level of data protection in all electronic communications.

The Working Party recommends the Commission, the European Parliament and the Council to take into account its comments. It invites the Commission to clarify outstanding issues so to allow the Working Party to contribute to the ongoing process.

The Working Party suggests that this draft directive be discussed in the Council's working group "economic questions – data protection". This would allow to speed up the process to adopt all directives proposed for the telecom review and it would bring this text to the competent experts.

The Working Party reserves the possibility to comment on the draft directive as it evolves.

Done at Brussels, 2nd November 2000

For the Working Party

The Chairman

Stefano RODOTA

[14] see Articles 10, 11, 12, 14 etc. of Directive 95/46/EC referred to in recital 9 of the draft directive, as well as Articles 4 (2), 6(4), 7, 8, 9, 11, 12, 13 of the draft directive.