ARTICLE 29 Data Protection Working Party

**00451/06/EN**
**WP 118**

# Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services

**Adopted on 21 February 2006**

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

**set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],**

having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

having regard to its rules of procedure, and in particular Articles12 and 14 thereof,

**HAS ADOPTED THE PRESENT OPINION**:

## I. INTRODUCTION

The Working Party 29 is aware of the expansion of different on-line based communication services, including free web-based email services and related services. With the expansion of the e-communication services, concerns about the protection of the privacy of the communications have arisen, in particular because of existing practices to inspect communications in order to eliminate spam and viruses as well as to detect any predetermined content.

The Working Party 29 is aware that most of internet service providers and email service providers ("ISP" and "ESP") use filtering tools to protect networks and machines as well as, in fewer cases, to inspect communications for commercial reasons. However the Working Party 29 considers that, in some cases, using such filtering tools may not be in compliance with the existing data protection legislation described below. This may be due, among others, to the fact that the application of the legislation to these new types of services is not always clear.

The main purpose of this paper is to provide guidance on the question of confidentiality of email communications and, more specifically, on the filtering of on-line communications. In particular, a question has arisen as to whether the scanning of communications in which ISPs and ESPs are commonly engaged in order to carry out a variety of purposes constitutes an interception of communication and whether and how such interception can be justified.

To this end, this paper analyses, among others, the provisions on confidentiality of the e-communications as defined in Article 5 paragraph 1 of the 2002/58 Directive on privacy and electronic communications as well as other relevant provisions that are part of the *acquis communautaire* and national laws implementing it.

## II. LEGAL FRAMEWORK FOR DATA PROTECTION AND PRIVACY IN EMAIL COMMUNICATIONS

### A) European Convention for the Protection of Human Rights and Fundamental Freedoms

Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") and the constitutions of the Member States. It is also guaranteed by the two EU directives described below.

Article 8 of the ECHR provides everyone with the right to respect for his private life and his correspondence and lays down the conditions under which restrictions of this right could be acceptable. The European Court of Human Rights ("the Court") has applied Article 8 to regular mail communication on various occasions.

---

[1] Official Journal L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

Interception, opening, reading, delaying reception of letters or putting up barriers to the sending of letters have all been considered to be interfering with Article 8 of the ECHR[2]. From the case law of Commission and the Court of Human Rights, it may be concluded that email communications almost certainly will be covered by Article 8 ECHR, by combining both the notions of "private life" and "correspondence"[3]. Communication partners that use emails may reasonably expect that their communications will not be inspected by third public or private parties.

The right to respect for "correspondence" not only includes confidentiality but also the right to send and receive such correspondence[4]. Thus, it may be concluded that a general prohibition of sending or receiving email will conflict with Article 8 of the ECHR.

Everyone within the jurisdiction of one of the contracting ECHR States is entitled to the right to respect for his private life and correspondence. This includes all parties involved in a communication. In the A *v* France case (1993) the Court held that the recording of a telephone conversation with the consent of only one party was an interference with the right to respect for correspondence of the other party involved in the communication.

Under the ECHR, the contracting ECHR States can carry out lawful interception of correspondence including electronic communications or take other measures, if necessary for any of these purposes and in accordance with the ECHR, as interpreted by the rulings of the European Court of Human Rights. An interception can be defined as a third party acquiring access to the content and/or traffic data related to private communications between two or more correspondents, including traffic data concerning the use of electronic communication services that constitutes a violation of an individual's right to privacy and to confidentiality of correspondence. Such interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the ECHR and the ECHR's interpretation of this provision:

*"… a legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention.…"*

In private relationships, however, the most relevant mechanism for the application of the Convention rights is the doctrine of the positive obligations of the Contracting Parties. The Contracting Parties do not only have the obligation to refrain from interference but also to take positive measures to ensure that these rights can actually be exercised, not only with respect to the public power but also in the sphere of the relations of individuals between themselves. This includes the obligation to provide for an adequate legal framework for the exercise of these rights.

[2] In Niemitz (1992) the Court ruled that letters that were already delivered to the addressee are covered by Article 8 of the ECHR. In that decision the Court also stated that not merely private communications but also business correspondence is to be protected. In Klass (1978), Malone (1984) and Huvig (1990) the Court stated that telephone conversations are covered by Article 8 as well. With regard to other means of communication the Mersch-case of the Commission (1985) is relevant; where the Commission considered that the tapping of any form of communication would constitute an interference with Article 8.

[3] This conclusion is supported by the fact that in most Member States inspection of email messages is prohibited and that both on the international and national levels specific powers have been created to intercept email communications.

[4] Golder (1975), consideration 43: *"Impeding someone from even initiating correspondence constitutes the most far-reaching form of 'interference' (paragraph 2 of Article 8) with the exercise of the 'right to respect for correspondence'; it is inconceivable that should fall outside the scope of Article 8 while mere supervision indisputably falls within it."* Withholding of received mail will constitute interference also (Schöneberger & Durmaz, 1988)

Article 6 (2) of the Treaty on European Union states clearly that the Union shall respect fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, as general principles of Community law. According to Article 52 (3) of the EU Charter, the meaning and scope of rights contained in the Charter shall be the same as those laid down by the ECHR. This provision shall not prevent the Union law from providing more extensive protection.

**B) Specific provisions that apply to the confidentiality of email communications**

As mentioned above, the confidentiality of communications is further guaranteed by two EU Directives. When assessing the question of confidentiality of communications, the provisions of such Directives must be interpreted in conjunction with the ECHR as well as with the case law of the Court of Human Rights, described above.

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive") sets forth a horizontal legal regime for the protection of individual rights to data protection. With regard to the processing of personal data, the Data Protection Directive makes reference to the right to privacy as recognized in Article 8 ECHR[5]. The right to receive and impart information is also recognized as included in the freedom of information as guaranteed in Article 10 ECHR[6]. Furthermore, according to recital 47, the person from whom an email message that contains personal data originates must be considered to be the controller of that personal data, whereas the email service provider will normally be considered controller in respect of the processing of the additional personal data necessary for the operation of the service.

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector ("e-Privacy Directive") applies to the processing of personal data in connection with the provision of publicly available electronic communications networks in the Community. The provisions of this Directive particularize and complement the Data Protection Directive. The confidentiality of communication is protected, in particular, by Article 5 of the e-Privacy Directive which reads as follows:

*"…Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other then users, without the consent of the users concerned, except when legally authorised to do so…"*

Moreover, Article 4 of the e-Privacy Directive provides 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".*

---

[5] Recital 10: *"whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law"*

[6] Recital 37: *"Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiviovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms"*

Also relevant is the e-Commerce Directive, in particular the provisions regarding the liability of providers of internet/email services according to which Member States may not endorse general monitoring obligations to ISPs and ESPs. Such an obligation would constitute an infringement to the freedom of information as well as to the confidentiality of correspondence (Article 15 e-Commerce Directive[7]).

## III. SCANNING OF EMAIL CONTENT

In light of this legal background, a question arises as to whether the scanning of communications in which ISPs or ESPs are commonly engaged in order to carry out a variety of purposes is compatible with EU law.

Most of ISPs and ESPs do scan emails. They do this routinely for purposes such as spam filtering, virus detection, search and spell checking as well as forwarding, auto-responding, flagging urgent messages, converting incoming emails into cell phone text messages, automatic saving and storing into folders, converting text URLs to clickable links.

Below we will review the legal framework that governs the screening carried out for the following reasons: (A) for detecting virus, (B) for the purposes of filtering spam (C) for the purposes detecting any predetermined content.

### A) The screening of emails for purposes of detecting virus

Virus scanning consists of the process of checking files to see if they contain known viruses. In some cases, virus scanning is followed by virus cleaning which is the process of removing the detected virus from the file so that the file can be used securely. Such scanning occurs generally speaking when the email first hits the email provider's servers. Most email service providers include virus scanning as part of their service in order to protect themselves and the users from harmful viruses. In most cases, users cannot turn off automatic scanning as it comes by default as a part of the service.

In assessing the legal grounds that legitimise this practice, the Working Party 29 is of the opinion that the setting up and use of filtering systems by email providers for the purposes of detecting virus might be justified by the obligation to take appropriate technical and organisation measures to safeguard security of their services as foreseen in Article 4 of the e-Privacy Directive quoted above.

Indeed, given that the delivery of emails containing virus may shut down the email service providers system (besides damaging other documents and software stored in the end-user terminal equipment), and thus impair the transmission of further email communications, the Working Party 29 considers that performing such screening is a security measure aimed at protecting the data controller's (email service provider's) system, which as outlined above is a binding obligation for electronic communications service providers per application of Article 4 of e-Privacy Directive.

The Working Party 29 considers that using filters for the purpose of Article 4 can be compatible with Article 5 of the e-Privacy Directive.

The Working Party 29 wishes to underline in particular that such measures mentioned above shall be in accordance with the general principles of Community law.

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Furthermore, the Working Party 29 considers that by setting up filtering systems, email providers can also be considered as ensuring the performance of the service contract with their customers, who expect to receive and send emails with a certain degree of security. Accordingly, the processing of data in which email service providers are engaged when they set up filtering systems may also be legitimised under Article 7 b of the Data Protection Directive which foresees the processing of data "*necessary for the performance of a contract to which the data subject is a party*".

Given that in accordance with the above, virus filtering might be justified for safeguarding the security of services under Article 4 of the e-Privacy Directive and/or for the mere performance of the contract in accordance with Article 7 b of the Data Protection Directive, without prejudice to confidentiality of the communication, the Working Party 29 recalls the need for email providers to ensure compliance with the following:

(a) the content of emails and the attached annexes has to be kept secret and must not be disclosed to anyone but the addressee(s);

(b) if a virus is found, the installed software must offer sufficient guarantees regarding confidentiality;

(c) if a virus scan is carried out in the form of content scanning, it should be set up automatically and only for this purpose, i.e. the contents must not be analysed for any other purpose.

Information should also be provided on the screening (see specific section, below)

**B) The screening of emails for the purposes of filtering spam[8]**

ISPs and ESPs use various techniques to prevent unwanted (not necessarily only commercial) emails, i.e. spam, from reaching their intended addressees.

One of them consists of using the so-called blacklisting by which IP addresses of certain servers and dynamic IP ranges allocated to certain ISPs are blacklisted[9] Blacklisting is not further analysed in this paper.

Filtering out spam has in fact become a necessary practice. If email services did not use email filtering for spam purposes, spam would increasingly be part of their incoming mail stream and the systems would probably be very slow and inefficient, making email services practically unusable for their users. This would obviously cause consumers dissatisfaction and would probably impose limitations to the possibility of providing a trustworthy and reliable email service.

[8] The OECD Document entitled "Anti Spam Regulations" carried out by the Spam Task Force in March 2005 (DSTI/CP/ICCP/SPAM(2005)1 in describing the concept of spam states the following: "*The term "spam" is commonly used in the international media and in policy announcement made by different countries, however there is no commonly held definition of the term. Although broadly referring to the same phenomena, different countries define spam in a manner that is most relevant to their local environment. In developing an anti-spam policy, it is essential that the nature of spam be clearly understood and defined, and that spamming be differentiated from legitimate practice.*"

[9] By using this technique, the email provider does not engage in filtering, it simply blocks (i.e. refuses to accept) the emails that come from blacklisted servers or IP ranges, without screening its content. Whereas this blacklisting practice is in principle less privacy intrusive than content-based filtering, it can raise the question of freedom of speech and of freedom of expression as well as the right to free correspondence and to receive such correspondence as recognised in Article 8 of the ECHR, further interpreted by the Court.

Whereas spam may not be per se a threat for the security of the ESPs' services, but rather for the general performance of the network and the email service in particular, spam may nevertheless trigger the ESP inability to provide the email service itself. The Working Party 29 considers that Article 4 of the e-Privacy Directive requiring email providers to take appropriate technical and organisational measures to safeguard security of their services, is concerned about the security of the ESP and network services *per se* but also about the general performance of the email and network services. Security of the ESP is a problem insofar as it affects the ESP service. For this reason, the Working Party 29 considers that Article 4 might also apply to this situation. In other words, threats to the general performance of email and network services can justify ISPs and ESPs to engage in filtering for anti-spam purposes. If one takes into account the effects that spam produces, even in those cases where the spam sender distributes only few information via emails per day, but those information are sent to a very huge number of recipients, it reinforces the argument in favour of the application of Article 4 of the e-Privacy Directive because even in these cases, the sending of such limited number of emails might block the internet traffic and seriously harm the reliability, the security and the efficiency of email services in general. Furthermore, for the same reasons, the Working Party 29 also considers that such filtering could be legitimized on the basis of Article 7 (b) of the Data Protection Directive, on the basis that filtering for spam is necessary for the email provider to be able to perform properly the service contract to which the data subject, i.e. recipient is a party.

On the other hand, the Working Party 29 is concerned by the fact that filtering results sometimes in "false positives", i.e. legitimate "wanted" messages are not delivered because they are deemed to be spam. The Working Party 29 considers that the action of filtering and withholding received mail supposedly unwanted may entail not only an invasion to the freedom of speech but also, a violation of Article 10 of the ECHR and constitute an interference of private communications[10]

In light of the above, notwithstanding the application of Article 4 of the e-Privacy Directive, and in order to safeguard the principle of freedom of communications, as recognised by Article 10 of the ECHR as well as the confidentiality of the communications provided in Article 5 of the e-Privacy Directive and recognised by Article 8 of the ECHR, the Working Party 29 strongly recommends email providers to take into account the following recommendations, which mainly aim at giving recipients of emails control on the communications that are in principle addressed to them:

(a) the Working Party 29 encourages the practice consisting of giving subscribers the possibility to opt out of scanning their emails for spam purposes, the possibility to check emails deemed as spam in order to ascertain whether they were indeed spam and the possibility to decide what "kind" of spam should be filtered out. Furthermore, the Working Party 29 also welcomes the activity of some of ESPs that offer subscribers an easy way of opting back into the scanning of their emails for the purposes of filtering spam;

(b) the Working Party 29 also encourages the development of filtering tools that end users can install or configure either in the terminal equipment or in third party servers or in the provider's email server and which enable them to control what they want to receive and what they do not want to receive, also in order to reduce the costs inherent in downloading unsolicited electronic mail as recalled in Recital 44 to Directive 2002/58. The Working Party 29 also welcomes the research of other tools to fight spam that may be less privacy intrusive.

[10] As recognised by the Court in Schöneberger & Durmaz, 1988.

In addition to the above, the Working Party 29 reminds email service providers engaged in screening emails for spam purposes of their duties, under Article 10 of the Data Protection Directive, to inform subscribers of their policy as far as spam is concerned in a clear and unambiguous way, as further described under section IV of this Opinion. The email provider must also ensure the confidentiality of the filtered emails that should not be used for any other purpose.

**C) The screening of emails for the purposes of detecting any predetermined content**

The Working Party 29 notes that some email providers reserve the right to screen and even to remove any predetermined content[11], for example, such content could include alleged unlawful material or material that is unwanted by the recipient, user of this particular service. The technique used for this type of screening is very similar to the one used for the detection of viruses and spam.

Unlike the screening for viruses, the screening of emails for detecting predetermined content, even if considered as alleged unlawful material, cannot be considered as necessary technical and organisational measures to safeguard security of email services as foreseen in Article 4 of the e-Privacy Directive. The email service provider is not under threat of being harmed and communications stopped because of the material contained in emails. Therefore, the scanning for the purpose of detecting this material is not legitimised on the email provider's need to safeguard the security of the service. The Working Party 29 is also concerned that in exercising such type of filtering, email service providers become censors of private email communication, by for example blocking communications whose content may be completely lawful, raising fundamental questions of freedom of speech, expression and information. The Working Party 29 would like to emphasize that service providers have no general obligation to monitor predetermined or alleged harmful content, but, as further developed below, this kind of service might be offered by a service provider as an added value service.

Accordingly, the Working Party 29 is of the opinion that, in accordance with Article 5.1 of the e-Privacy Directive, the email providers are prohibited from engaging in filtering, storage or any other kinds of interception of communications and the related traffic data for the purposes of detecting any predetermined content without the consent of the users of the services or they must be legally authorised to engage in such screening in accordance with Article 15 of the e-Privacy Directive as implemented by Member States legislation.

## IV. OBLIGATION TO INFORM

In addition to Article 5 of the of e-Privacy Directive, the processing of personal data for the purposes of acquiring knowledge of the content and/or traffic data relating to private communications must also comply with various requirements of the Data Protection Directive.

---

[11] See TOS yahoo: You acknowledge that Yahoo! may or may not pre-screen Content, but that Yahoo! and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or move any Content that is available via the Service. Without limiting the foregoing, Yahoo! and its designees shall have the right to remove any Content that violates the TOS or is otherwise objectionable. You agree that you must evaluate, and bear all risks associated with, the use of any Content, including any reliance on the accuracy, completeness, or usefulness of such Content. In this regard, you acknowledge that you may not rely on any Content created by Yahoo! or submitted to Yahoo, including without limitation information in Yahoo! Message Boards, and in all other parts of the Service. You acknowledge, consent and agree that Yahoo! may access, preserve, and disclose your account information and Content if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to: (a) comply with legal process; (b) enforce the TOS; (c) respond to claims that any Content violates the rights of third-parties; (d) respond to your requests for customer service; or (e) protect the rights, property, or personal safety of Yahoo!, its users and the public.

Among others, the Data Protection Directive sets forth an obligation to inform individuals about the processing of their personal data. In particular Article 10 *"Information to be given to the data subject"* imposes upon data controllers the obligation to provide data subjects from whom personal data is collected with certain information, which includes the identity of the data controller as well as the purposes for which the data will be processed. Furthermore, Article 6 paragraph 1, letter (a) of the Data Protection Directive establishes that data must be processed fairly and lawfully, which reinforces the obligation on data controllers to be completely transparent regarding the conditions of the processing of individuals' data.

As far as filtering for the purposes of screening virus and spam is concerned, the Working Party 29 considers appropriate the ESPs practice consisting of informing subscribers as part of the contractual conditions of the service.

In addition to the above, ESPs must also comply with Article 4 of the e-Privacy Directive which requires providers of a publicly available electronic communication service to inform subscribers of particular risks of breaches of the security of the network. Where the security lies outside the scope of possible remedies by the service provider, the service providers should inform their users and subscribers of measures they can take to protect the security of their communications.

## V. OTHER EMAIL RELATED SERVICES

The Working Party 29 notes the development of a new kind of software products and services such as for example the so-called *"Did they read it?"* service, aiming at tracking email opening.

This kind of service allows anybody subscribing to it, to know if an email sent by the subscriber (a) has been read by the addressee(s), (b) when it was read, (c) how many times it has been read (or at least opened), (d) if it has been transferred to others and (e) to which email server, including its location. Finally, it also allows knowing which type of web navigator and operating system the recipient of the email uses.

The data processing is secretly performed, i.e. no information about the data processing is provided to the email recipients from whom the data is retrieved. Furthermore, email recipients are not given the possibility to accept or refuse the retrieval of the information described above. In sum, differently from classical acknowledgement email systems, with these new products, the recipient of emails has no possibility to accept or refuse the acknowledgment information processing towards the software user.

The Working Party 29 expresses the strongest opposition to this processing because personal data about addressees' behaviour are recorded and transmitted without an unambiguous consent of a relevant addressee. This processing, performed secretly, is contradictory to the data protection principles requiring loyalty and transparency in the collection of personal data, provided by Article 10 of the Data Protection Directive.

In order to carry out the data processing activity consisting in retrieving from the recipient of an email, whether the recipient has read it and when and whether it has forwarded it to third parties, unambiguous consent from the recipient of the email is necessary. No other legal grounds justify this processing. Therefore, the data processing that is performed secretly is contradictory to the data protection principles requiring unambiguously given consent, laid down by Article 7 of the Data Protection Directive.

## VI. CONCLUSION

Given the perceived uncertainty on the compatibility of the filtering of email communications and the request from guidance from stakeholders, the Working Party found it helpful to publish the present opinion.

The Working Party 29 wishes to encourage email service providers to take into account the guidelines and recommendations contained in this opinion in the provision of their services. Furthermore, as part of its policy to promote technology which incorporates data protection and privacy requirements in the building up of the infrastructure and the information systems including terminal equipment, the Working Party 29 would like to encourage developers of email software to devise and develop privacy compliant systems in such a manner as to reduce the processing of personal data to the very minimum; limiting it to what is absolutely necessary and proportionate to achieve the purposes of the processing.

Done at Brussels, on 21 February 2006

*For the Working Party*

The Chairman
Peter Schaar