



# GUIDE FOR THE FIGHT AGAINST SPAM

Agencia Española de Protección de Datos



## ÍNDICE

<u><i>I.- What is Spam.....</i></u>	<u><i>2</i></u>
<u><i>II.- Forms of Spam.....</i></u>	<u><i>5</i></u>
<u><i>III.- Help prevent Spam.....</i></u>	<u><i>7</i></u>
<u><i>IV.- Help reduce Spam.....</i></u>	<u><i>11</i></u>
<u><i>V.-Legislation and texts of interest.....</i></u>	<u><i>14</i></u>
<u><i>VI.-Powers of the Spanish Data Protection Authority.....</i></u>	<u><i>16</i></u>
<u><i>VII.- International solutions to an international problem.....</i></u>	<u><i>21</i></u>
<u><i>VIII.- Glossary of Spam related terms.....</i></u>	<u><i>26</i></u>



## I.- What is Spam?

Nowadays Spam or “junk mail” refers all kinds of **unsolicited** mail sent electronically.

So, Spam is understood as being any unsolicited message and which normally aims to offer, market or try to arouse interest regarding a product, service or company. Though this can be done by various routes, the one most used among the general public is electronic mail .

This conduct is particularly serious when it is done massively.

The sending of marketing messages without prior consent is prohibited by Spanish legislation, both by the Information Society Services Act 34/2002 (the outcome of transposing Directive 31/2000/EC) and by the Data Protection Organic Act 15/1999 of 13 December.

The low cost of sending via the Internet (by means of electronic mail) or via mobile telephones (SMS and MMS), its possible anonymity, the speed with which messages reach their recipients and the possibilities in the volume of transmissions, have allowed this practice to be carried out abusively and indiscriminately.

Article 21.1 of the Information Society Services Act expressly prohibits the sending of **advertising or promotional communications** by email or other equivalent means of electronic communication which has not been previously requested or expressly authorised by their recipients. In other words, communications intended for the direct or indirect promotion of the goods and services of a company, organisation or person who carries out a commercial, industrial, artisan or professional activity is banned, though this prohibition is subject to the exception contained in paragraph two of the article, which authorises the sending when there exists a prior contractual relation and it refers to similar products. The sending of unsolicited marketing communications can thus be regarded as constituting a minor or serious infringement of that Act.



In addition to implying an infringement of the Information Society Services Act, the practice of Spam can signify a violation of the right to intimacy and a breach of the legislation on data protection, since it has to be borne in mind that the email address can be considered as personal data.

The Directive on Privacy in Telecommunications of 12 July 2002 (Directive 58/2002/EC) currently transposed in the Telecommunications General Act 32/2003 which modifies various articles of Act 34/2002 introduced the principle of “*opt-in*” into the European Union, in other words, **prior consent** of the person for sending electronic mail having marketing ends. In this way, any messages sent for advertising purposes become subject to the granting of consent, unless there exists a prior contractual relation and the subject does not state his wishes otherwise.



## **II.-Forms of Spam**

### **- Electronic mail**

Due to the ease, speed and capacity in data transmissions, the reception of marketing communications via this information society service is the most usual one, and the means by which *spammers* send most of their undesired advertising.

### **-Pop-up Spam**

This concerns sending an unsolicited message which pops up when we connect to the Internet. It appears in the form of a dialogue window and a message from Windows titled "message visualisation service". Its content is variable and generally concerns an advertising message.

For this, a functionality of the Windows operating system is used, available on versions Windows NT4, 2000, and XP, and which permits a networks administrator to send messages to other posts in the network.

The simplest solution for preventing it is to disable this service from Windows. Another method is to use a firewall intended to filter the TCP and UDP ports (135, 137,138, 139 and 445) of your computer, though this measure could cause the network to cease functioning.

### **-Phishing**

This is not exactly a category of Spam, but rather a technique of social engineering for gathering data fraudulently.

Phishing is the duplication of a website in order to make the visitor believe that he is in the original site rather than the illicit one. It is usually used for criminal purposes by duplicating the websites of banks and indiscriminately sending Spam mail telling the recipient to access that page in order to update access data to the bank such as passwords, expiry dates, etc.



### **-Hoax**

The *hoax* is an email message with a false or deceitful content and normally distributed in chain form.

Some hoaxes inform on viruses, others make pleas to solidarity, or they contain formulas for winning millions or creating chain letters.

The objectives sought by whoever starts a *hoax* are normally to capture email addresses or saturate the network or the mail servers.

### **-Scam**

Scam has no marketing communicational nature. This type of undesired message implies a fraud by telematic means, whether by mobile phone or by email.

### **-Spam in the mobile**

As well as communications from the telephone operator by means of text messages (SMS – *Short Message Services*) or multimedia messages (MMS – *Multimedia Message Services*), there also exist other types of advertising communications in which there is no prior consent nor any contractual relation, and are therefore considered to be unsolicited marketing communications.

This type of communication generates a waste of time and money. Moreover, MMSs can introduce viruses and maliciously exploit any vulnerability in the telephone's internal systems.

### **- Unsolicited advertisements by fax or automated phone call**

While this type of message is not considered Spam per se, they are nevertheless subject to sanction by the Spanish Data Protection Agency, which will apply the same fines established by law for Spam.

### **III.- Help prevent SPAM**

The email address is the means most used for registering the identity of a person in the Internet and it usually serves as the basis for gathering information on him. It very often contains information on the person such as surname, the company where he works or country of residence. This address can be used in a great many places in the network and can be easily obtained without our knowledge. This makes it necessary to follow a series of rules for safeguarding our privacy.

#### **- Be careful who you give your email address to**

Only give your email address to individuals and organisations that you want to communicate with and that you trust to keep it private.

#### **- Consider using two or more email addresses**

It is advisable to create an email address which will be the one that has to be provided in those cases where you don't trust the recipient or know them well enough. By doing this, your personal address will be known only by your friends or professional contacts, with the saving in time implied by not having to separate important mail from the undesired ones.

The same thing is recommended when it comes to using instant messaging services.

#### **- Choose a less vulnerable email address**

*Spammers* obtain email addresses in many different ways. For example, by searching the web, chat rooms and IRC, and even in contact directories or using social engineering. They sometimes buy lists of email addresses from sites that are willing to sell their customers' details. And when all else fails, they simply 'guess'.

Email addresses which refer to a person as such usually contain some element identifying them and which are easy to remember. This way of creating



the mail allows *spammers* to guess email addresses. For example, if your name is John Smith, the spammer will try the following options: john.smith@..., j.smith@..., jsmith@..., smith.j@..., etc.

*Spammers* have access to software packages that do the 'guessing' for them automatically. They can create hundreds of addresses in a minute since they work by using dictionaries, in other words, a list of words that are usually used in email addresses. These dictionaries normally contain fields such as the following:

- Forenames
- Surnames
- Initials
- Nicknames
- Pet names
- Brand names
- Star signs
- Months of the Year
- Days of the Weeks
- Place Names
- Car Makes and Models
- Sporting Terms
- Etc.

These programs simply introduce data into each of these fields and try various combinations with them all. They also add letters and numbers in the combinations, since dates or birthdays, ages, etc., are usually added.

In order to create an email address and reduce the level of Spam, it would be good idea to not to introduce fields that are potentially guessable by the *spammer*.

**-Don't advertise your email address.**

Don't advertise your email address on search engines, contact directories, forums or websites. If you use chat systems, never expose your email on the listing or directory and never disclose it to anyone other than friends.



When sending mail in which a lot of addresses appear, send them using BCC (Blind Carbon Copy) so as not to make all the addresses visible.

If you need to use your email address in a website, sent it in image format or with 'at' instead of @. In that way, it won't be picked up by the Spam creator programs.

Also, if you forward a mail, delete the address of the previous recipients: this data is easy for spammers to obtain.

**-Check Privacy Policies and Marketing Opt-Outs Carefully.**

If you are going to subscribe to a service on-line, or purchase a product, check the privacy policy before giving your email address or other private information. It could be that the company is going to pass on the data to other companies or to its subsidiaries and make sure that it does not subscribe to any marketing bulletins. So it is advisable to know the policy on rental, sale or exchange of data which has been adopted, both by your Internet provider and by the administrators of directories and distribution lists where you are included. Download the screen and pages where you bought them and safeguard the identifying data.

Also, read suspicious messages as text and not as html and disable the previsualisation of mail.

**Do not hesitate to use your rights of access and cancellation of your data with these companies.**

**-Make children aware about the use of mail and instant messaging**

Children are the ideal targets for promoting information on the composition and consumption practices of a household. This makes it important to remind them of some practical advice which will help to prevent children from providing personal data.

Also, from their email address it's not possible to know who the recipient of mail is, and that mail could contain contents unsuitable for children.



## **IV.- Help reduce Spam**

### **What to do if you receive Spam?**

Once you have started to receive Spam, it is almost impossible to stop it completely other than by changing your email address. In any case, a series of recommendations are included here which can be applied for reducing the proliferation of “junk mail”.

### **-It is not advisable to reply to the Spam**

Article 21.2 of Act 34/2002 provides that those who produce electronic advertising messages have to have simple and free procedures so that recipients can request not to receive any more messages. Nevertheless, it must be borne in mind that the majority of junk mail received comes from outside our borders, and is therefore not subject to our legislation. Replying to this mail tells the sender that the address is live, which could encourage both him and other *spammers* to send more messages. You should not reply to emails sent from outside Spain unless you are familiar with, and trust, the sender.

It is advisable to turn off the option for sending an acknowledgement of receipt to the sender for email messages that have been read. If a *spammer* receives it, he will know that the address is live and will most likely send more Spam.

### **-Don't click on adverts in spam mail.**

By clicking on spammers' web pages, you are identifying your email as a live address and may make yourself a target for even more email. Graphics and images (and also what are known as web bugs -) in spam mail can provide the spammer not only with information that the message has been received but also other private information such as your IP address.

### **-Use mail filters**

### **- Email filtering programs**



Email management programs, along with many mail websites, offer the possibility of enabling filters which separate desired mail from Spam. The main disadvantages are that they can confuse legitimate mail with junk messages. More and more advanced programs are being produced in this field, and they can often be downloaded free on the Internet. These filters receive instructions for defining the type of mail it is wished to receive and which mail is considered to be Spam.

#### **- ISP based filters**

Many Internet providers offer solutions that can be very effective when it comes to blocking Spam. They use combinations of blacklists and scanning of contents in order to restrict the amount of Spam reaching the addresses. The main downside is that they sometimes block good email and there is also usually a cost involved. For further information, please check with your provider.

#### **-Keep your system up to date**

Personal computers require maintenance. Most software companies issue product updates and patches that fix known problems with their software. These updates are usually available on the manufacturers' websites and are usually free to download and install. Users should also have **antivirus** programs to protect against rogue virus programs that can destroy all the files of a computer and are increasingly being exploited by *spammers*.

It is also highly recommendable to install a **firewall** in order to monitor what is going on in the computer.

#### **-Consult our Recommendations Guide for Internet Users**

These [recommendations](#) describe the main Internet services, the identification of possible risks for privacy which its use might occasion, and they provide advice for users.

## **V.- Legislation and texts of interest**

The laws regulating the sending of unsolicited electronic marketing communications are, on the one hand, the Information Society Services Act 34/2002 and, on the other, the Telecommunications General Act 32/2003.

The Telecommunications General Act 32/2003, of 3 November (LGT), and the Information Society Services Act 34/2002, of 11 July (LSSI), grant powers to the Spanish Data Protection Authority.

The Telecommunications General Act assigns to the Authority the task of safeguarding the rights and guarantees of subscribers and users in the field of electronic communications, delegating to it the imposition of sanctions for violation in the provision of electronic communication services.

On the other hand, the Information Society Services Act sets down that it corresponds to the Authority to impose sanctions in the event of infringement due to the sending of unsolicited marketing communications by electronic mail or equivalent electronic communication means, in breach of the provisions stated in its articles.

### **-Articles in the LSSI relating to the sending of electronic communications**

The relevant articles on the sending of unsolicited communications via the Internet are the following: 19, 20, 21, 22, 38 and 43.

### **-Articles of the Data Protection Organic Act (LOPD).**

The relevant articles of the LOPD are the following: 3.a), 4, 5, 6, 37.1.n) and 44 and 45.

### **-Articles of the Telecommunications General Act.**

Articles 38, 53.z, 54.r, 58.b and Additional Provision Nine of Act 32/2003.

### **-Other legal texts of interest.**



- Directive 1995/46/EC, concerning the protection of individuals with regard to treatment of personal data and the free flow of that data (Directive on data protection).

- Directive 2000/31/CE, on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce).

- Directive 2002/58/CE, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

#### **- Article 29 Group Documents**

- 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 2 November 2000 (WP 36).

- Opinion 5/2004 on unsolicited communications for marketing purposes under article 13 of Directive 2002/58/EC. Adopted on 27 February 2004 (WP 90).

#### **- Other Texts**

- Communication from the Commission to the European Parliament, to the Council, to the European Economic and Social Committee and to the Committee of the Regions on unsolicited marketing messages or Spam. Brussels, 22.01.2004

- Commission of the European Communities. Unsolicited marketing messages and data protection. Summary of the conclusions of the study. January 2001.



## VI.- Powers of the Spanish Data Protection Authority

The Telecommunications General Act 32/2003, of 3 November (LGT), and the Information Society Services and Electronic Mail Act 34/2002, of 11 July, (LSSI), modified by the LGT and by the Electronic Signature Act 59/2003, of 19 December, expanded the powers of the Spanish Data Protection Authority.

The Telecommunications General Act attributes the Authority with the power to safeguard the rights and guarantees of subscribers (*natural or legal person with a contract with the operator*) and users (*those who use the services without having contracted them*) in the field of electronic communications, entrusting it with the imposition of sanctions due to violation of the following rights in the rendering of electronic communications services:

- To make their traffic data anonymous or to cancel it when it is no longer necessary for the purposes of the transmission of a communication. The necessary traffic data for the purposes of invoicing subscribers and payments of interconnections shall be able to be processed only up to expiry of the period for challenging the invoice for the service or for which the operator can demand payment.
- To use their traffic data for marketing ends or for the rendering of value added services, only when their informed consent has been given for this.
- To receive non-itemised invoices when so requested (\*).
- That the processing of location data other than traffic data may only be done when it has been made anonymous or with their prior informed consent and only to the degree and for the length of time necessary for the rendering of value added services as the case might be, with the unequivocal knowledge of the data that is going to be subjected to processing, the purpose and duration of it and the value added service for which it is going to be provided.
- To halt the automatic rerouting of calls made from his terminal by a third party (\*).

- To prevent, by means of a simple and free procedure, the display of the identification of his line in calls made.
- To prevent, by means of a simple and free procedure, the display of the identification of his line to the user making a call (\*).
- To prevent, by means of a simple and free procedure, the display of the identification of the calling line in incoming calls and to reject incoming calls in which that line does not appear identified (\*).
- To not receive automated telephone calls or fax messages of a commercial nature without having given prior informed consent to the communication.
- Furthermore, to guarantee to subscribers the right not to appear in subscriber directories or directory services. In this case, express consent is required for the initial inclusion in such directories and services, and tacit consent is required for subsequent publications. However, with regards to information already existing in subscriber directories, as defined by article 30 of RD 424/2005, consent will be considered sufficient if, after receiving a request for expression of their preference whether or not to maintain their information in the directory, the subscriber does not respond within one month with expressed refusal of consent. However, in order to include information in addition to that which is described in article 30\* of RD 424/2005, express consent is required, both for initial and subsequent use.

*\* This includes, at a minimum, the following information a) Name and surname, or title b) subscriber number or numbers c) postal address of the residence, excluding floor, number and hall d) specific handset that the user wishes to identify, should that be the case e) name of network service provider*

*(\*) These rights are only acknowledged by the LGT for subscribers to electronic communications services.*

The **Information Society Services Act** sets down that it corresponds to the Authority to impose sanctions in the event of infringement due to the sending of unsolicited marketing communications by means of electronic mail or equivalent electronic communication means, in breach of the following provisions:

- The sending of **advertising or promotional messages by electronic mail** or other equivalent electronic communication means is prohibited if it has not been **solicited or expressly authorised** by the recipients thereof, **unless** there exists a **prior contractual relation**, always provided the sender has obtained the contact data of the recipient in a lawful manner and that he uses it for the sending of marketing communications referring to products or services of his own company which are similar to those that were initially the subject of contracting with the customer.

*(\*) In all cases, the sender must offer the recipient the possibility of opposing the processing of his data for promotional ends by means of a simple and free procedure, both at the moment of gathering the data and in each of the marketing communications sent to him.*

**The recipient shall at any moment be able to revoke his consent** provided for the reception of marketing messages with a simple notification of his wishes to the sender. For such purposes, the providers of services must have **simple and free procedures** so that the recipients of services can **revoke** their consent which they have given and they must **provide information on those procedures**, accessible by electronic means.

- When the providers of services employ **data storage and retrieval devices in terminal equipment (cookies)**, they shall **inform** recipients clearly and simply concerning their utilisation and purpose, offering them the **possibility of rejecting the processing** of data by means of a **simple and free procedure**.

The above shall not prevent **the possible storage of or access to data** for the purposes of technically effecting or facilitating the **transmission of a communication** by an electronic communications network or, to the degree that is strictly necessary, for the rendering of an information society service **expressly requested** by the recipient.

*(\*) This provision has been introduced by the LGT, and has been in force since 5 November 2003. Also, this Act has toughened up the system of infringements and sanctions provided for in the LSSI in those cases in which the mass sending of spam is*



*made, or the sending to the same recipient of more than three undesired marketing messages within a period of a year by electronic means.*

The sanctions provided for in the Information Society Services Act 34/2002 are also applicable when there is a violation of the right of subscribers not to receive automated telephone calls or fax messages of a commercial nature without having given prior informed consent to the communication.

Investigating cases of Spam is becoming an ever more complicated task, due to the fact that *spammers* contract computing pirates in order to hide their true identity (*spoofing*). Internet service suppliers (ISP) are usually diligent when it comes to cutting off the service to *spammers* when they realise that junk mail is being generated from their networks.

If you have knowledge of the country where the Spam is coming from, you can inform the concerned authorities of this. In the case of Spam coming from a State of the European Union, the data on all the European authorities for data protection is available on the website of the AEPD. If the Spam is being sent from the United States of America, unsolicited messages can be forwarded to the Federal Trade Commission, which provides an alert procedure on its web page [www.ftc.gov](http://www.ftc.gov), and with whom the Spanish Data Protection Authority (AEPD) has signed a Memorandum of Understanding.

In the section on [Complaints and Claims](#) on our website, you will find information on how to file a complaint with the Authority. Before informing the AEPD of a case of Spam, make sure that it is not a solicited marketing message.

Below you will find the web addresses of counterpart bodies to the Spanish Data Protection Authority, many of them with powers in the fight against spam.

Austria: [Austrian Data Protection Authority](#)

Belgium: [Privacy Protection Commission](#)

Cyprus: [Office of the Commissioner for Personal Data Protection.](#)

Denmark: [Danish Consumer Ombudsman](#)

Slovakia: [Slovak Personal Data Protection](#)

Estonia: [Estonian Data Protection Inspectorate](#)



Finland: [Data Protection Ombudsman](#)

France: [Commission Nationale de l'informatique et des Libertés \(CNIL\)](#)

Greece: [Hellenic Data Protection Authority](#)

Hungary: [Data Protection and Freedom of Information Commissioner of Hungary](#)

Ireland: [Data Protection Commissioner](#)

Italy: [Garante per la protezione dei dati personali](#)

Latvia: [Datu valsts inspekcijas](#)

Lithuania: [Valstybinė duomenų apsaugos inspekcija](#)

Luxembourg: [Commission nationale pour la protection des données](#)

Malta: [Data Protection Commissioner](#)

Netherlands: [College bescherming persoonsgegevens](#)

Poland: [Inspector General for the Protection of Personal Data](#)

Portugal: [Comissão Nacional de Protecção de Dados](#)

Czech Republic: [Office for Personal Data Protection](#)

Sweden: [Swedish Data Inspection Board](#)



## **VII.- International solutions to an international problem**

Ever since the Spanish Data Protection Authority took charge of watching over compliance with the Information Society Services Act and the Telecommunications General Act in 2003, granting it powers of enforcement in the matter of unsolicited marketing messages (Spam), its international activity has been expanded and promoted since, by virtue of article 37.1 of the Data Protection Organic Act, this body has to carry out the necessary international cooperation for complying with the duties entrusted to it.

Indeed, the actual nature of the Internet and the technological evolution of the media via which it takes places mean that the problem with Spam is an eminently international problem against which one has to act with measures requiring synchronised international participation adopted jointly by everyone involved, in accordance with all legislations, which sometimes do not regulate this field in the same way.

To achieve this international cooperation, various documents have been signed on reciprocal collaboration and assistance with institutions in charge of that enforcement role in different countries, at both the Community and extra-Community levels.

### **- Relations with Europe**

In the intra-European field, the Spanish Data Protection Authority forms part of the *Contact Network of Spam Authorities* (CNSA). This group consists of the national authorities responsible for the regulation and control of unsolicited communications of the European Union and of the European Economic Area. In the last meeting held in Brussels, it was agreed to draw up a document with the aim of establishing an intra-European framework for the exchange of information on complaints made about Spam among the competent authorities, with clear instructions on what has to be done when a complaint is received. The common point of these countries is article 13 of Directive 2002/58/EC.

This document was signed in December 2004 and it contained a cooperation procedure in the transmission of information referring to the



application of article 13 of Directive 2002/58/EC or any other applicable national legislation referring to unsolicited marketing communications.

By virtue of this agreement, the following forms of collaboration have been approved:

- When an international complaint is received, before sending it to the Competent National Authority, the national authority has to confirm that the complaint is viable and that it concerns a natural person. The complainant must also be informed that his personal data will be passed on to another Authority. The different authorities having information on the violation of the regulations on Spam in another national jurisdiction will share that information with the competent Authority.
- To establish the cooperation framework among authorities and the division of complaints.
- To maintain secrecy concerning information and complaints, eliminating any sensitive information that has been communicated by one Authority to another, in accordance with the applicable national legislation.
- This text is not binding on national or international legislations.
- **Relations with the United States.**

With this idea of global cooperation, a [Memorando Of Understanding](#) (MOU) has been signed with the Federal Trade Commission (FTC) for fighting against Spam, the FTC being the federal body with enforcement and control powers in the United States. By virtue of this Memorandum, both parties agree on the following forms of collaboration:

- To instruct users and companies in relation to Spam.
- To promote codes of conduct on good practices.



- To exchange information on the most advanced technical solutions and keep informed on new developments;
- To collaborate with the universities of the respective countries in order to promote research, conferences and training courses on the subject;
- To render mutual assistance in their investigations.

The fight against Spam in the United States starts from a normative reality that is very different from the European one. Basically, in the USA, the system of *opt-out* is established in the Act regulating this type of communications, the “CAN-SPAM Act”.

- **Multilateral relations.**

The Spanish Data Protection Authority has participated in multilateral working parties against Spam and for that purpose a meeting was held in London in October 2004 together with other bodies at the world level in charge of the fight against Spam (independent authorities and concerned ministries) and involved industrial sectors.

This working party brought together the heads of the US Federal Trade Commission, the Information Commissioner’s Office of the United Kingdom, the Office of Fair Trading of the United Kingdom, the French National Commission of Liberties and Information, the Telecommunications Regulator of the Netherlands, the Director of the Australian Competition and Consumer Commission, the Director of the Spanish Data Protection Authority and the international head of the FTC.

The outcome of this meeting was a final declaration for initiating a joint plan of action known as the “**London Action Plan**” (LAP), which was signed by 19 organisations and institutions from 15 different countries.

The aim of the LAP is to develop international contacts for investigating cases of Spam and all problems connected with it. We signatories of the LAP were mostly National Authorities and Commissions, and we have taken on sufficient commitments for:



- Encouraging and promoting communication among us in order to enforce compliance with the law more efficiently.
- Organising periodical conferences for debating: cases, normative developments, investigations, new techniques and ways of eliminating obstacles in the investigation of cases of Spam. Informing and educating users and consumers.
- Promoting dialogue with public authorities and the private sector in order to act jointly and encourage cooperation initiatives.
- **Relations with Ibero-America.**

The Authority has also wished to strengthen ties and define common positions concerning the protection of personal data in Ibero-American countries, for which it participated very actively in the III Ibero-American Encounter, held in Cartagena de Indias (Colombia) in 2004. This gathering, which had the collaboration of the Spanish Agency for International Cooperation (AECI) and the International and Ibero-American Foundation of Administration and Public Policies (FIIAPP), brought together more than 40 authorities and outstanding representatives from the public and private sphere of 15 Ibero-American countries (Argentina, Brazil, Chile, Costa Rica, Colombia, El Salvador, Ecuador, Spain, Mexico, Nicaragua, Peru, Panama, Portugal, Uruguay and Venezuela). Among other topics, the meeting dealt with attacks on privacy in the telecommunications and Internet sector and the fight against Spam, with the following actions being agreed upon:

-To define technical and legislative measures against Spam in the fight in this regard.

-To promote international collaboration, establishing a homogenous framework.

-To encourage initiatives on sector self-regulation that would complement and facilitate the expansion of the regulating framework in this field.



The outcome of this Encounter was the approval of some conclusions which were included in the approved final Declaration ([Cartagena Declaration](#)), which analyse and propose common approaches concerning the major topics that were examined.

There also exist other international forums in which Spain actively participates and collaborates, such as the following:

- **ITU- International Telecommunications Union.** To find out more about this forum, you can access it via the following hyperlink. <http://www.itu.int/osg/spu/spam/>. The ITU was the United Nations body in charge of organising the World Summit on the Information Society. The Authority participated in International Cooperation Actions with the aim of generating confidence and security in the use of the ICTs. The Authority also works on various initiatives in the fight against Spam.
- **OECD Task Force.** In this forum, the objectives are directed towards providing an international response in the different policies and towards coordinating the fight against Spam, encouraging and promoting measures for combating Spam and codes of good practice in the sector of industry and in business, in addition to facilitating cross-border law enforcement. A workshop was held in Brussels last year in order to combat Spam, in which both Enforcement Authorities and private sector representatives took part, in order to analyse the technical and socio-economic aspects of Spam. For further information, follow this hyperlink: [OECD Work on Spam](#).



## VIII.- Glossary of Spam related terms

**Acknowledgement of receipt:** A kind of message sent to show that a mail has arrived at its destination without errors. An acknowledgement of receipt can also be negative, in other words, it can show that a block of data has failed to arrive at its destination.

**Antivirus:** Computer program permitting computing viruses to be detected and eliminated.

**Can-Spam Act:** Federal Act on the practice of spamming in the United States, of 16 December 2003, which came into force on 1 January 2004. The text provides an opt-out mechanism and explicitly bans deceitful messages (use of false sending addresses or camouflaging the nature of the message) and false advertising of the content of the message. Can-Spam Act is an acronym for "*Controlling the Assault of Non-Solicited Pornography and Marketing Act*".

**Cookies:** Set of data sent by a Web server to any navigator visiting it, with information on the use made by the navigator of the server's sites, with regard to the navigator's IP address, address of sites visited, address of the site from which it is accessed, date, time, etc. This information is stored in a file in the user's computer for being used the next time the server is visited. Also, there exist servers which restrict the use of certain functionalities of its services or even deny their use if the user decides not to accept the recording or location of the cookie in his computer.

**Firewall:** Security system permitting control over communications among computing nets. Installed between the Internet and a local network, it permits non-authorised access in the latter to be prevented, thus protecting its internal information.

**Electronic mail or email address:** Series of numerical or alphanumeric characters, uniquely identifying a certain source and permitting access to it. The email address is considered to be personal data since it allows its user to be identified.



**Filters:** Based on the ISP under instructions and configuration of the user and in programs.

**Hoax:** Deceit, fake.

**Https:** Secure version of the http protocol. The HTTPS system uses ciphering based on Secure Socket Layers (SSL) for creating a more suitable channel for the traffic of personal information than the HTTP protocol. It is normally used by banks, on-line stores and any kind of service requiring the sending of personal data or passwords.

**IRC:** Initials for Internet Relay Chat, communications protocol permitting one to participate in virtual conversations in real time (see Chat Room).

**ISP:** Internet Service Provider.

**Blacklist:** Identification control mechanism permitting differentiation between people who can access a particular service and others who, contained on that list, cannot.

**Opt-in:** Mechanism in which marketing communications will only be able to be sent by means of express request from the individual. Any kind of unsolicited marketing communication is prohibited. This is the mechanism adopted by the latest European Directives. Directive 2002/58/CE of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, transposed to our internal law by the Telecommunications General Act 32/2003.

**Opt-out:** Mechanism which permits the free sending of this type of message provided it allows the recipient of it to ask to be taken off the sending list. It used to be the old European tendency concerning the granting of consent, as provided for in 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. In the United States, it is still the legislative system in force.



**Phishing:** Contraction of "password harvesting fishing".

**Network:** Set of machine connected for exchanging information among each other.

**Chat Room:** Virtual site of the network, also called channel, where users meet to chat with others in the same room.

**Spam:** See "What is Spam"

**Spammer:** The person or company who sends Spam.

**Spamming lists:** Marketing lists. Lists of mail addresses for the mass sending of advertising.

**Spoofing:** Supplanting the identity of a third party. Though it can occur in different environments, one of the most common where it frequently appears is in the mass sending of Spam.

**URL:** The URL is the chain of characters with which a unique address is assigned to each of the information sources available on the Internet.

**Computing virus:** Computer program that can infect other programs or modify them in order to include a copy of itself. Viruses are propagated with different objectives, normally with fraudulent ends and causing damage to the computing equipment.

**Web bug:** "micro spies" are transparent images in a web page or in an electronic mail with the size of 1x1 pixels. As occurs with "cookies", they are used to obtain information on readers of those pages or mail users, such as the IP address of their computer, the internaut's navigator type and version, the operating system, language, how many people have read the mail, etc.

