UOC
www.uoc.edu

September 2004

Article

The right to privacy and to personal data protection in Spanish legislation

http://www.uoc.edu/dt/eng/vilasau0904.pdf

Mònica Vilasau

UOC
www.uoc.edu

Article

The right to privacy and to personal data protection in Spanish legislation*

http://www.uoc.edu/dt/eng/vilasau0904.pdf

Mònica Vilasau

Abstract

This article is designed to be an introduction to the regulatory framework for data protection in force in terms of Spanish law. The analysis centres mainly on Organic Law 15/1999, which replaced the previous law from 1992, adhering to Directive 95/46/EC on protection of individuals with regard to the processing of personal data and on the free movement of such data.

The current Organic Law develops article 18.4 CE and looks to guarantee people's right to privacy and informational self-determination in terms of the many forms of intrusion that information and communication technologies represent.

In line with the Directive, principles are established for data protection and the processing involved in the use of personal data. The starting point is the consent of the individual in question, consent, which in the case of sensitive data, has to be reinforced. However, despite this wide-ranging protection that the regulations seem to offer, a range of exceptions to this general principle of consent have been found.

In terms of the creation of files, Spanish regulations set a distinction between whether the files are publicly or privately owned, providing virtual impunity for the former, given that the sanctions are practically inexistent.

Finally, reference is made to the rights of the interested or affected party, concluding with an introduction to the international movement of data.

Keywords

data protection, privacy, consent, public accessible sources, files

Introduction

New technologies, new threats to the right to privacy

Every time we surf the net, buy a book, visit a web page or consult our accounts through on-line banks, we leave a trail,[1] we leave data such as our name, address, account number, or our preferences. Much of this data is not exactly secret. So where is the danger of giving it? The danger comes from the sophistication of the information and communication technology, and the possibilities of storing, controlling, cross-referencing and exchanging this data which on its own may seem irrelevant. It is also in the possibility of using powerful search engines. Often, also, the subject does not know what data is in a third party's possession, or the use and transmission carried out.

This ease in obtaining and cross-referencing data is of great benefit, for both businesses and government. Companies are very interested in knowing the preferences of potential consumers when it comes to sending them specific marketing or a bank will wish to know if a person offers enough guarantees in order to approve a loan. On the other hand public authorities are also interested in having the maximum amount of information on the citizens, to fight against crime and terrorism or to prevent fraud.

*Updated version of the article previously published in [2003] CTLR, volume 9: issue nº 7.

Translated from original Catalan by Katy Reay. The author would like to thank Dr. Mark Jeffery for his valuable feedback.

1. Regarding the dangers that surfing the net involves see: RIBAS ALEJANDRO, p. 143-161.

The new technologies really do represent a risk and a threat to the privacy, secrecy and defence of a sphere of personal autonomy. It is necessary to create new protection mechanisms for people's private lives. But the right to privacy is not an absolute right, rather, when it comes to defining this right it will be necessary to bear in mind other rights and interests. The right to privacy must be weighed up against the freedom of information. To this limit it is necessary to add the principal of freedom of the company within the framework of the market economy, which is kept very much in mind in common law countries.[2]

In respect of the control of personal data, the sentence of the German Constitutional Tribunal, of 15 December 1983 on the Law of censorship,[3] formed a new right, the right to information self-determination, as a corollary to the right to self-determination of the individual. The right to information self-determination means that the individual can basically decide for himself when, and within what limits, to disclose information relating to his life.[4]

Concern of the legislator, regulatory evolution of data protection

International framework

Facing these dangers, the Law has reacted in order to try to provide a solution, safeguard the fundamental rights of the individual and weigh up the interests concerned. The 1970s are testimony to a wide legislative movement moving towards creating a framework for the defence of the right to privacy.

This legislative impulse focused on establishing specific regulations to regulate the compilation and handling of personal data and to adopt measures regarding the secrecy of the communications. It also established independent authorities that control the compliance with these regulations (Data Protection Authorities).

A first legislative movement is found on a national level. After the first Law on data protection approved by the Parliament of the German Land of Hesse in 1970, countries such as Sweden, the United States, New Zealand, Canada, and the majority of European countries created legislative instruments on this matter.

Another legislative impulse is found on an international level. To start with it is necessary to highlight Convention 108 of the European Council, of 28 January 1981, on the protection of individuals with regard to automatic processing of personal data.[5]

Later, on a Community level, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data[6] was passed and Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector, has been approved.[7] The latter Directive has repealed Directive 97/66/EC of the European Parliament and of the Council, of 15 December 1997, on the processing of personal data and the protection of privacy in the telecommunications sector.[8]

The European Union had been rethinking its policy on data protection and in order to finish defining it, it held a European conference in Brussels in autumn 2002.[9]

What regulation is there in the Spanish State?

Article 18.4 of the Spanish Constitution (CE) is the starting point. This provision has been developed by the specific legislation on data protection and also it is necessary to bear in mind the legislation on e-commerce, the penal code, the civil code and Organic Law 1/1982.

Organic Law 15/1999, of 13 th December, on the protection of personal data (forthwith LOPD) is the main law that is applicable[10] and the Sentence of the Constitutional Court 292/2000, of 30 November, has declared some of its articles unconstitutional. Law 34/2002, of 11 July, on information society and e-commerce services (forthwith LSSI)[11] has been added to this framework.

In the context of the Internet, and often on the subject of data protection, it is necessary to refer to the elements of self-regulation that arise. An example is the codes of the type that a group of companies or public authorities can agree to and that establish a series of rules, organisational conditions, operational schemes, applicable procedures, or policies on the processing of personal data.[12]

2. About the different interests in conflict and different positions adopted by the legislator, see: «US tech protests EU privacy laws». http://zdnet.com.com/2100-1106-960134.html
3. This sentence can be found translated into Spanish in the Constitutional Jurisprudence Bulletin, nº 33, 1984, p. 126 and following.
4. See German Constitutional Tribunal Sentence, Constitutional Jurisprudence Bulletin, nº 33, p. 152-153.
5. One must bear in mind the additional Protocol to the aforementioned Treaty, dated 8-XI-01. http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm
6. You can find it in: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=ES&numdoc=31995L0046&model=guichett
7. OJEC L 201/37, dated 12th July 2002. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=32002L0058&model=guichett
8. You can find it in: http://europa.eu.int/eur-lex/pri/es/oj/dat/1998/l_024/l_02419980130es00010008.pdf
9. Regarding this conference see: http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm
10. Published in the Spanish Official State Bulletin (BOE) nº 298, on 14th December 1999, it repealed Organic Law 5/1992, although it has temporarily left some regulatory provisions in force which developed Organic Law 5/1992. Organic Law 15/1999 has had minor amendments by law 62/2003, of 30 th December, (BOE nº 313, on 31st December). See Spanish regulations on data protection at: https://www.agpd.es/index.php?idSeccion=72
11. BOE nº 166, on 12th July.
12. See Art. 18 LSSI and Art. 32 LOPD.

Regarding the contents of the LOPD, this is organised around some principals, found in Title II and which are the following:

- Quality of the data (Art. 4), in order to guarantee its reliability and accuracy.
- Consent (Art. 6): In order to process personal data the unequivocal consent of the data subject is necessary. In relation to this principal, complete information must be given to the data subject (Art. 5). Also there are certain data that, depending on their purpose, enjoy even greater protection (Art. 7).
- Security and secrecy in the processing of the data (Art. 9 and 10) and consistency and proportionality in its use (Art. 11 and 12).

To ensure the application of these principals, the LOPD acknowledges a series of rights for the data subject (Title III): the right to object to assessments (Art. 13), the right to consult and access the data (Art. 14 and 15), the right to rectification and cancellation (Art. 16), the right to protection (Art. 18) and the right to compensation (Art. 19).

One key characteristic of the LOPD is that it regulates publicly owned databases separately from privately owned ones, and grants the public sector databases privileged treatment.[13]

Organic law 15/1999, on protection of personal data[14]

Scope of application

The LOPD defines personal data as «any data concerning identified or identifiable natural persons» (Art. 3a). The LOPD is applicable to any data, including that which is not automated, though it is subject to a specific regime.[15]

The scope of protection of the LOPD is considerably wider than that of Law 5/1992 because unlike the latter, it extends to any data, including data on members of political parties, trade unions or religious organizations.

Not all databases that contain personal data are subject to the LOPD. Databases kept by natural persons in the exercise of their personal activities are excluded, as are those relating to classified matters and those established for the investigation of terrorism and organised delinquency.

Evidently natural persons are the owners of the rights acknowledged in the LOPD and this is clear from Arts. 1 and 3.e) LOPD.[16] By contrast, legal persons are excluded from the scope of application of the LOPD although they have protection under the civil and criminal law.

And what about the individual businessman? The Data Protection Authority considers that the LOPD is applicable when the data refers to the private life of the data subject, assuming from the start the private nature.

Data collection

At first we might think that data can only be collected because the data subject has provided it. However, there are other forms (allowed by Law) of data collection which do not pass by the data subject, such as through publicly accessible sources or by means of data transfer.

Data collected via the data subject

To begin with it is necessary to bear in mind that data must be provided for a specific purpose (Art. 4.2) and that the data subject must be given the information as required by Art. 5 LOPD.[17]

The general rule

Personal data processing requires unequivocal consent of the data subject, unless the Law provides otherwise (Art. 6.1).

Regarding consent, Art. 3.h) determines that consent by the data subject is understood to be: «any manifestation of intention, free, unequivocal, specific and informed, through which the data subject consents to the processing of the personal data that concerns him».

Would tacit consent be admissible? A tacit declaration of intention is understood to be that in which a specific act or behaviour is carried out from which it can be deduced that intention exists.[18] It is admitted that Art. 6.1 LOPD extends to a tacit declaration of intention whenever the data subject, understanding this to be an average person, has a clear idea of what is involved.[19]

How should silence be assessed? Silence can be considered as a declaration in all cases in which good faith imposes a positive obligation to show a refusal.[20] Some authors argue that in data processing silence has a positive value[21] and indeed it seems that the Data Protection Authority allows it in its Recommendation to the e-commerce sector, of 24 July 2001.

No need for consent

Nevertheless the above mentioned, no consent is needed when the personal data being collected is for the exercise of functions

13. See SUÑÉ, p. 157.
14. A general view on the LOPD can be found in ÁLVAREZ-CIENFUEGOS.
15. Art. 32.2 Directive 95/46/EC and Additional Provision (DA) 1. 2 LOPD.
16. In the same way: Art. 18.4 EC and Consideration 24 of Directive 95/46/EC.
17. As provided for in Art. 6.1.b) Directive 95/46/EC.
18. For all, DÍEZ-PICAZO, p. 148-149.
19. APARICIO, p. 58-63 and TÉLLEZ, p. 150.
20. DÍEZ-PICAZO, p. 150-151.
21. In this sense, APARICIO, p. 63-69; DE MIGUEL, p. 551-552 and TÉLLEZ, p. 150.

of public Administration; when it refers to the parties of a business, labour or administrative relationship and is necessary for its maintenance or fulfilment[22] (art 6.2); when the purpose of the processing is to protect a vital interest of the data subject (Art. 7.6 LOPD) and when the data figures in publicly accessible sources [Art. 3 j), 28 and 30 LOPD].

It should also be noted that although consent may have been given, this is revocable when a justified cause exists and retroactive effects are not attributed (Art. 6.3). In the cases where consent of the data subject is not necessary for the processing of personal data, the data subject can oppose that processing when fundamental and legitimate motives exist relating to a concrete personal situation.

Specially protected data

For so-called sensitive data, stricter requirements are established for obtaining the data subject's consent. Thus, the express consent, in writing, of the data subject will be necessary to process data that reveals ideology, union affiliation, religion or beliefs (Art. 7.2) and express consent for processing data relating to racial origin, health or sexual life (Art. 7.3).[23] However, even with regard to this data, consent can be dispensed with in exceptional circumstances (Art. 7.6 LOPD).

Data not collected from the data subject

Art. 5.4 LOPD refers to those cases in which the data are not collected from the data subject and also those cases in which data are collected from publicly accessible sources as from data transfer. In these cases, however, a special obligation exists to inform the data subject of the content of the processing, the origin of the data, and of the information required in Art. 5.1.a), d) and e). However, unlike Art. 11 of the Directive, the LOPD allows this communication to be deferred for up to 3 months from the registration of the data.

Publicly accessible sources

Art. 3.j LOPD considers as publicly accessible sources promotional listings, telephone listings,[24] lists of people belonging to a professional group, newspapers and official journals and means of communication.

The essential part of the concept of publicly accessible sources is that their data can be used without the data subject's consent. However Art. 6 establishes some important distinctions. Starting from the assumption that it is data originating from a publicly accessible source, is required that the data processing is necessary for the satisfaction of a legitimate interest of the database administrator or of the third party to whom the data is communicated and it is on the condition that it does not harm the fundamental rights and freedoms of the data subject.

When the data is in publicly accessible sources the regime to which the consent is subjected changes. Amongst other provisions that apply in this area we find articles 5.5.2, 6.2 and 11.2.b) and it also necessary to bear in mind articles 28, 29 and 30 LOPD.

It must be stressed that in the case of publicly accessible sources, the only thing that is excluded is the need for the data subject's consent. But that is the only exception, and the data subject's right to be informed about the processing of his data is not excluded.

Transfer to a subject other than the data subject

The general rule for the transfer of data is that the data must be of use for the fulfilment of purposes directly related to legitimate functions of the transferor and the transferee, and also the prior consent of the data subject (Art. 11.1).

There is, however, a whole series of exceptions to the rule of consent, which are set out in Art. 11.2.

The communication of data between public administrations is regulated in Art. 21 LOPD and part of this provision was found to be unconstitutional by Sentence of Constitutional Court 292/2000, of 30 November. The transfer of data in the case of privately owned databases is regulated in Art. 27 LOPD. There is specific regulation regarding the transfer of data relating to information about solvency and credit (Art. 29.4).

Access to data by third parties (Art. 12)

According to Art. 12.1, access to data by a third party is not considered to be a data transfer when this access is necessary to provide a service to the processing administrator. However, when a third party has to intervene in some way in the processing of this data, according to the prevision in Art. 12.2, it is necessary to create a contract between the processing administrator and the third party.

Creation of databases

Title IV of the LOPD regulates the creation of databases. Unlike Directive 95/46/EC, the LOPD makes a distinction between publicly owned databases (chapter I) and those that are privately owned (chapter II) granting the former a somewhat privileged treatment.

22. In the framework of a contractual relationship one piece of data that can be given is the e-mail address. Now, when the LSSI is applicable, if the service provider wants to use the e-mail address that has been given to him in the contractual relationship for subsequent commercial communications, he needs –with some exceptions– the data subject's consent (Art. 22.1 LSSI), consent that can be revoked at any time (Art. 22.1 LSSI).
23. Some authors do not consider the difference in requisites established for obtaining consent between the data contemplated in Art. 7.2 and that of 7.3 as justified, as it seems to indicate a certain hierarchy between the different data contemplated. For this reason it is defended that the data contemplated in the two provisions have the same value. Therefore, the requisites have to be the same and in the assumptions contemplated in Art. 7.3 express written consent would also be necessary when obtaining data (TÉLLEZ, p. 130). This thinking seems reasonable, above all bearing in mind that some data, such as for example that referring to sexual life, goes together with ideology.
24. Regarding the application of the LOPD to the telecommunications sector and its specificity consult DE ASÍS ROIG, p. 201-228.

Publicly owned databases (Arts. 20-24 LOPD)

Publicly owned databases are understood to be those of the public Administrations or other public law bodies, organs or corporations.

The creation, modification or removal of data can only be carried out by means of a general provision published in the Official Bulletin of the State or corresponding Official Journal (Art. 20.1).

The creation/modification dispositions have to indicate what is provided for in Art. 20.2.

Once the database is created, the Administration or organ that is responsible for it has to notify the Data Protection Authority for its inscription in the General Data Protection Register (Art. 5 RD 1332/1994). The removal of databases is contemplated in Art. 20.3.

Data transfer between public administrations is regulated in Art. 21 LOPD, and part of this provision was declared to be unconstitutional by the Sentence of Constitutional Court 292/2000. It must be noted that the databases of the security forces have special treatment, set out in Articles 22, 23 and 24 LOPD.

Privately owned databases (arts. 25-32 LOPD)

According to Art. 25, privately owned databases containing personal data can be created when the all of the following requirements are fulfilled:

- It is necessary for the legitimate purposes of the person, company or entity that owns it.
- The guarantees established by this Law or the protection of persons are respected.

The creation of databases with personal data needs to be previously notified to the Data Protection Authority (Art. 26.1) indicating all the circumstances demanded by Art. 26.2.

The General Data Protection Register will proceed with the inscription of the database if the notification complies with the imposed requisites, that is to say, that the inscription is regulated if the legal requisites are complied with.

In the case of data transfer, the database administrator, has to inform the data subjects (Art. 27.1).

There are some privately owned databases that have a special regime, for example those that contain data relating to solvency. Regarding this, the Data Protection Authority has issued Directive 1/1995, of 1 March.

The processing of databases for the purpose of marketing and commercial research is regulated in Art. 30 LOPD. This is an attempt to reconcile the respect for privacy with what is known as «relationship marketing». It is necessary to relate Art. 30 LOPD with Articles 19-22 LSSI which regulate electronic commercial communications.[25] These provisions have opted for a restrictive solution when it comes to allowing communications to potential consumers. It has followed the «opt-in» system (Art. 21.1) in such a way that it prohibits sending marketing or promotional communications by e-mail that have not been previously requested or expressly authorised by the recipients. Nevertheless, these kind of communications can be sent when there is a previous commercial relationship between the sender and the recipient and the communication refers to the same kind of product that has been previously contracted.

In short, regarding marketing or promotional communications by e-mail, it is not enough to be in possession of a series of data to be able to carry out a marketing campaign, the consent of the data subject to whom this type of communication is to be sent is also necessary.[26]

There is also special regulation on common databases of insurance companies that contain personal data for the liquidation of insurance claims (Additional Section 6 LOPD). Data transfer to these databases does not require the prior consent of the data subject, but it does need the communication of the possible transfer of data. The treatment of these databases is extremely criticised as it introduced an exception that was not provided for in the Directive 95/46/EC.[27]

Data procesing and rights of the data subject

Data processing

The LOPD establishes an obligation for the database administrator and the person responsible for the processing to guarantee the security of the data. This brings with it the need to adopt measures to make the security of the data effective and avoid its alteration, loss, unauthorised processing or access (Art. 9).

This security obligation is established in relation to some concrete parameters: the state of the technology, the nature of the stored data and the risks to which it is exposed. Just as technology determines what is possible, the nature of the data to be protected provides the criteria for what is reasonable.

The security requirements provide that personal data should not be registered in databases that do not fulfil the conditions established (Art. 9.2). At the moment, the Royal Decree 994/1999 of 11 June continues in force, which approves the Regulations of security measures of automated databases that contain personal data. This is the basic legal instrument in the matter of database security and carries, amongst other obligations, the need to create a security policy in a single document.

The Regulations establish three levels of security: basic, medium and high, depending on the nature of the data processed, in relation to the greater or lesser need to guarantee the confidentiality and the integrity of the data.[28]

25. This articles have been modified by Law 32/2003 of Telecommunications of 3rd November (Final disposition nº 1). BOE nº 264 on 4th november 2003.
26. Regarding the different systems that may be followed in relation to commercial communications, see: RODRÍGUEZ and LOZA p. 3-18.
27. See the criticisms made by the doctrine regarding this DA 6, SUÑÉ, p. 171-172.
28. The Regulations of Security Mesures (RMS) establishes 3 levels of security, a basic level (for databases contemplated in Art. 4.1 RMS and the security measures are regulated in arts. 8-14 RMS) medium (data contemplated in Art. 4.2 and 4.4 and measures regulated in arts. 15-22) and high (data contemplated in Art. 4.3, and measures regulated in arts 23-26).

In addition, the database administrator and whoever intervenes at any stage of the data processing is obliged to maintain a professional secrecy (Art. 10), an obligation that endures even after the termination of the contractual relationship.

Rights of the data subjects

The right to consult and the right to access the database

The right to consult carries with it the right to know, on request to information from the General Data Protection Register, of the existence of determined personal data processing, its purposes and the identity of the person responsible for the processing. The General Register is free, for public consultation (Art. 14).

The right to access fulfils what is provided for in Art. 4.6 LOPD, according to which personal data should be stored in such a way that allows the exercise of the right to access, unless it is legally cancelled.

On the basis of this right, the data subject can request and obtain for free information about his data that are subject to processing, the origin of the data and the transfers carried out or which are foreseen (Art. 15.1). This right to access can only be exercised at intervals of no less than 12 months and its exercise is free.[29]

Rectification and cancellation

Art. 4 LOPD establishes the principal of the quality of the data: this includes, amongst other aspects, cancellation and substitution *ex oficio* of personal data which is inexact (Art. 4.4). Art. 16 LOPD regulates that right to rectification and cancellation. These two provisions are the two sides of the coin. It is Art. 4 LOPD where the determining facts can be found on the need to rectify and cancel the data.

Personal data will be rectified or cancelled if the processing does not comply with the Law, in particular, if data are inexact or incomplete (Art. 16.2). The person responsible for the processing is obliged to carry out the right to rectification or cancellation within a period of 10 days (Art. 16.1).

Cancellation includes blocking the data, and keeping it solely for the use of administration and tribunals in determining responsibilities (Art. 16.3). Therefore cancelling it is not synonymous with eliminating it as there exists the possibility of blocking the data.[30]

Procedure for objection, access, rectification or cancellation (Art. 17)

Art. 17 LOPD establishes the means to set the procedure to exercise the rights of the data subject. At the moment, this regulatory procedure is understood to be effected by the Royal Decree 1332/1994, of 20 June, which develops determined aspects of Organic Law 5/1992. For the interpretation of these regulations one must also see Directive 1/1998, of the Data Protection Authority of 19 January.

The rights of the data subject are personal and independent. To exercise them it is necessary to send an application to the database administrator. The right to access is regulated in Art. 12-14 Royal Decree 1332/94 although it is necessary to bear in mind the restrictions to its exercise that are established in Arts. 23 and 24 LOPD. Sentence of Constitutional Court 292/2000 has declared this latter provision partially void. Regarding personal data registered in privately owned databases, access is only denied when a person other than the data subject makes the application.

The exercise of these rights of rectification and cancellation is found in Art. 15 RD 1332/94, with the modifications which are to be understood from a literal interpretation of Art. 16 LOPD.

In those cases in which the exercise of the above-mentioned rights has been unsuccessful due to the opposition or reticence of the database administrator or the person in charge of processing, the data subject may file a claim before the Data Protection Authority arguing that his rights have been infringed. The final resolution of the Data Protection Authority is appealable without a further right of appeal before the relevant division of the High Court.

As well as claims made in order to exercise the rights acknowledged in LOPD, the data subject who as a consequence of the non-compliance of what is provided for in this Law suffers harm or injury to his goods or rights, has the right to be compensated. Regarding publicly owned databases, the responsibility will be determined in accordance with the regulatory legislation of the regime for public administration responsibility. In the case of privately owned databases the claim is made before the ordinary jurisdiction (Art. 19).

International data movement

The international movement of data is regulated in Arts. 33-34 LOPD, which implements Arts. 25 and 26 of Directive 96/46/EC.

The European Directive establishes a data protection system on the basis of the principal according to which personal data forms goods that are integrated within commerce. As a result, the freedom of movement of goods, people and services that are established as basic freedoms for the success of the EU are applied in exactly the same way to any other goods that are the object of commerce found within the scope of the EU.

Therefore, there is only an international data transfer when the destination country is a third State, that is to say, a State that is not a member of the EU.[31] Currently, the movement of data between countries of the European Community is free, due to application of Art. 1.2 Directive 95/46/EC.

29. See the form provided by the Data Protection Authority for the exercise of the right to access: https://agpd.es/upload/mod_a_derecho_acceso.pdf
30. See the forms provided by the Data Protection Authority for the exercise of the rights to rectification and cancellation respectively.
https://agpd.es/upload/mod_b_derecho_rectificacion.pdf
https://agpd.es/upload/mod_c_derecho_cancelacion.pdf
31. APARICIO, p. 185.

Directive 95/46/EC established detailed minimum regulations, which can be improved by national legislation, as long as it does not serve to justify any obstacle to the free transmission of data between member countries. The standard of the Directive is considered to be sufficient and no State can invoke a superior protection, subject the transfer to organisations established in the territory of one of the member states to authorisation.

In contrast, the transfer of data to countries with less protection than that of this Directive, supposes a violation of the community law, and therefore of the national legislations, and as a result is susceptible to sanction.

It must also be borne in mind that international data transfers cannot constitute an abstract act, but must always have a particular objective, as set out in the law.

Art 33 LOPD provides that international data transfers cannot be made to countries that do not provide a level of protection comparable with that of the LOPD, unless that, as well as observing what is provided for by this law, prior authorisation is obtained from the Data Protection Authority. The latter, on the basis of the provisions of Art 33.2 LOPD, evaluates the adequate nature of the protection.

The problem posed by the adaptation of the provisions of the Directive that has been made relating to the international transfer of data is that it seems to be left, as a last resort, to the criteria of the processing administrators whether the third country to which the data is being exported offers enough guarantees or not.

On the contrary, from Community law it seems to be deduced that it should be the States who should determine, case by case, a list of States that offer adequate protection. If this protection is missing transfers could only be authorised once the circumstances are evaluated, a sufficient level of privacy is guaranteed.

For this reason, some authors consider that the system offered by the LOPD has to be interpreted in a way that most conforms to the Directive. In concrete it is considered that it must be understood that no exportation of data can be made to third countries unless they had been declared as safe destinations by the Ministry of Justice, or that they had obtained prior authorisation from the Data Protection Authority.[32]

The interest of the Data Protection Authority in the transfer of data is specified in Directive 1/2000, of 1 December, published in the Official Bulletin of the State on 16th December.

The Data Protection Authority, following the position adopted by the Data Protection Group created by the Directive, has admitted the contractual solution as an instrument that allows the processing administrator to offer adequate guarantees on transferring data outside countries of the EC, and therefore, outside the scope of application of the Directive and general framework of Community Law.

The contractual regulation has to have all the basic principals for data protection, giving details of the purpose, the means and the conditions of processing of the data transferred as well as the form in which the basic data protection principals were applied. The prohibition of transfer to third parties not bound by contract has to be expressly contemplated.[33]

On the other hand Art. 25.6 of Directive 95/46/EC, which must be kept in mind, determines that «The Commission may find [...] that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article [...]». At the moment the Decisions 2000/518/EC, 2000/519/EC and 2000/520/EC of 26 July exist, according to which the level of personal data protection granted by the legislation of Switzerland and Hungary is considered adequate; and the level of protection conferred by the «Safe Harbour» principal is considered adequate for the protection of privacy in the USA.

With regard to the USA it must be stressed that there is no specific law that regulates personal data processing. Although numerous sectors have requested it, the US has opted for the solution of combining legislation, regulations and above all industry self-regulation. It argues that companies themselves should voluntarily undertake to respect the rights of the consumers. This, therefore, will reward those companies that provide greater protection. Given the different level of protection between the USA and Europe, finally they have agreed to Safe Harbour. According to this agreement, the 15 consent to the flow of data by companies that voluntarily accept a set of principals and practices defined by the Department of Commerce. The latter will be the authority that ensures the compliance with these undertakings by the organisations that agree to this Safe Harbour for the data supplied by the consumers.

Bibliography

ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M. (2000). Notas a la nueva regulación de la protección de datos de carácter personal. In *La Ley*, n. 5036, 17 April.

APARICIO SALOM, J. (2000). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. Navarra: Aranzadi.

DE ASÍS ROIG, A. (2002). Protección de datos y derecho de las telecomunicaciones. In CREMADES, J.; FERNÁNDEZ-ORDÓÑEZ, M.A.; ILLESCAS, R. (coord.). *Régimen jurídico de internet*, *La Ley*. Madrid, p. 201-228.

DE MIGUEL ASENSIO, P.A. (2002). *Derecho privado de internet* (3rd ed.). Madrid: Civitas.

DÍEZ-PICAZO; PONCE DE LEÓN, L. (1993). *Fundamentos del Derecho civil patrimonial. I Introducción. Teoría del contrato* (4th ed.). Madrid: Civitas.

GRIMALT SERVERA, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Comares.

MIRALLES MIRAVET, S.; BACHES OPI, S. (2001). La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos. In *La Ley*, vol. XXII, n. 5.306, 11 May.

OLIVER LALANA, D. (2002). El derecho fundamental «virtual» a la proteccion de datos. tecnologia transparente y normas privadas. In *La Ley*, n. 5592, 22 July.

32. Compare APARICIO, p. 189.
33. See rule five of the abovementioned directive 1/2000.

RIBAS ALEJANDRO, J. (2000). Riesgos legales en Internet. Especial referencia a la protección de datos personales. In MATEU DE ROS, R.; CENDOYA MÉNDEZ DE VIGO, J.M. (coord.). *Derecho de Internet. Contratación electrónica y firma digital*. Navarra: Aranzadi, p. 143-161.
RODRÍGUEZ CASAL, C.; LOZA CORERA, M. (2002). Protección de la privacidad. Aproximación al opt-in/opt-out. In *Revista de la contratación electrónica*, n. 23, January, p. 318. Cádiz.
SUÑÉ LLINÁS, E. (2000). *Tratado de Derecho informático*. Vol. I. «Introducción y protección de datos personales». Madrid: Servicio de publicaciones, Facultad de Derecho, Universidad Complutense, 2000.
TÉLLEZ AGUILERA, A. (2001). *Nuevas tecnologías y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*. Madrid: Edisofer.
ULL PONT, E. (2000). *Derecho público de la informática (Protección de datos de carácter personal)*. Madrid: UNED.

Related links

Spanish Data Protection Agency:
https://www.agpd.es/index.php
European Commission. Internal Market Directorate General. Data protection:
http://europa.eu.int/comm/internal_market/privacy/index_en.htm

To cite this document, you could use the following reference:

VILASAU, Mònica (2004). «The right to privacy and to personal data protection in Spanish legislation» [online paper]. UOC. [Date of citation:dd/mm/yy]
<http://www.uoc.edu/dt/eng/vilasau0904.pdf>

Mònica Vilasau
Professor of Law and Political Science Studies
mvilasau@uoc.edu

The author is a professor of Civil Law and, initially, focused her attention on areas relating to damages and liability in construction, in particular.
Subsequently, she became interested in areas relating to privacy and new technologies, and more specifically the so-called right to informational self-determination. Currently she is working on the principle of consent in data processing and exceptions thereto.