Balancing the interests in the context of data retention (INVODAS)

Spain

Julio Pérez Gil & Juan José González López

A. State of play of the transposition of the Directive 2006/24/EC

General questions

The Directive 2006/24/EC has been already transposed into Spanish law through Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (hereinafter LCD) [Law 25/2007, of 18th October, on the retention of electronic communications data and public communications networks][1].

In accordance with the contents of its 5th Final Provision, the LCD entered into force 20 days after its publication in the Official Bulletin of State, which took place on 19th October 2007. As a consequence, it has been in force since 8th November, 2007. The Only Derogatory Clause in the Law annulled article 12 of Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (hereinafter LSSICE), [Law 34/2002 of 11 July on Information Society Services and Electronic Commerce], which regulates mandatory data retention of electronic communications traffic; a provision that never entered into force due to insufficient regulatory developments.

The LCD, in accordance with the Second Final Provision, was drawn up under the protection of the provisions in articles 149.1.21ª and 29ª of the Spanish Constitution (hereinafter SC), which attributes exclusive competencies to the State in matters of public security and telecommunications respectively. As a consequence, the Autonomous Communities lack competencies in relation to data retention and disclosure of data on electronic communications, notwithstanding what was explained in respect of police corps of the autonomous regions.

The LCD is an ordinary law, approved by the Cortes Generales [Spanish Parliament] (art. 66.2 of the SC). Ordinary laws are those approved by Parliament, unlike organic laws. In accordance with article 81.1 SC, "Son Leyes orgánicas las

[1] As soon as we know, there is no official version of the LCD in English as yet. There is on the Ley de Protección de Datos de Carácter Personal 15/1999 del 13 de Diciembre [Organic Law on Personal Data Protection 15/1999 of 13 December].

relativas al desarrollo de los derechos fundamentales…". [Organic laws are those that relate to the development of fundamental rights]. Given that widespread data storage (data retention) affects fundamental rights, an infringement of article 81.1 SC has been raised, which would determine its unconstitutionality; for having been incorporated into the Spanish legal order through an ordinary law, in other words, as opposed to the development of fundamental rights which is the reserve of Organic Laws. The Supreme Court, Criminal Chamber, gave an opinion on this point, in judgment 249/2008, of 20 May, but it is an opinion obiter dicta, from a jurisdictional organ which has no authority over the constitutionality of the law (matters reserved for the Constitutional Tribunal).

On 9th January 2008, the Association of Internet Users requested that the Ombudsman lodge a complaint of unconstitutionality against Articles 1, 6, 7 and the first Final Provision of the LCD (http://www.internautas.org/html/4707.html). The complaint was based fundamentally on defects of the regulatory procedure (it is not an Organic Law and it affects a basic right), on a supposed infringement of Articles 18.3 and 4 of the CE (secrecy of communications and protection of data) and the absence of an effective judicial control over the information. The Ombudsman rejected the arguments set out and did not make use of his right to lodge the appeal. His view was that the LCD was neither a rule developing the basic right to secrecy in communications nor did it contain any restrictions of that right. He also felt that the need for judicial authorization implied a high degree of guarantee, completely in accordance with the on-going line of the jurisprudence of the Constitutional Court on the requirements regarding intervention in communications (pages 1399 and the following pages of the report published in http://www.defensordelpueblo.es/ documentacion/informesanuales/informe2008.pdf).

With regard to the interception of communications, but linked to the above, is the Ruling of the Third Chamber of the Supreme Court of 5th February, 2008. This resolved a complaint lodged by the same Association of Internet Users against certain precepts of Royal Decree 424/2005, of 15th April (RLGT). It was claimed that there were defects in the legislative technique as the interception of communications was governed by Royal Decree. The ruling rejected these claims maintaining that the domain of Organic Law did not have to extend to each and every one of the accessory or instrumental questions relating to those interceptions (for example the protocols for the conduct of the operators). The rule does not restrict the right to secrecy in communications, but it dictates which technical mechanisms are available to the judicial authority and the entitled bodies. The doubt concerning the range covered by the ordinary law (level of competence) has been settled because by virtue of the 1st Final Provision of the LCD the essence of its contents is included in Art. 33 of the Law 32/2003, of 3 November, on General Telecommunications (hereinafter LGT).

There are not lawsuits – nor pending nor concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which Spain is involved (as far as we have been able to ascertain). The Ruling of the Court of Justice (Grand Chamber) of 10th February 2009 (case C

301/06) on the legal basis of Directive 2006/24/CE went practically unnoticed in Spain and was only reflected, in a limited manner, in academic circles.

Main issues to consider about the transposition

Among the most important issues concerning the transposition of the Directive into Spanish law, can be highlighted those which we include in this section of our piece of work.

Article 3 of the Spanish Data Conservation Law (LCD) stipulates the data to be retained transcribing literally Article 5 of the Directive, as far as it reproduces its structure and content. Only a few details have been added and we believe that these are insignificant as they consist of specifications or refinements. For example among the data necessary to determine the date, time and duration of a communication (item (c) (1) the term "communication" has been replaced by "the call or, if appropriate, the messaging service or the multimedia service". In item (d) (1) (data necessary to identify the type of communication), possible telephone services used are specified: "(voice transmission, voicemail, conference calls, data), supplementary services (including call forwarding or call transfers) or messaging or multimedia services used (including short message services, advanced multimedia services and multimedia services)."

Data on unsuccessful call attempts are required to be retained. In this case, we refer to Article 4.2 of the LCD which defines this type of call as "a communication in the course of which a telephone call has been made successfully but without a reply, or in which the operator or operators involved in the call have intervened."

The same Law, in its Single Additional Provision, introduced an obligation concerning the identification of the users of mobile telephony with prepaid cards. The service operators are now required to hold a record book recording the identity of the customers who acquire a smart card with this form of payment (Nº 1). This provision came into force with the law but it also provided for the obligation to deactivate the prepaid cards whose cardholders had not been identified within two years, counting from that moment (Nº 8). With regard to the obligation of disclosure of these data the law describes the obligated parties more openly than in relation to the rest of the data (Nº 2). Furthermore, it does not require it to be in relation to the investigation of serious crimes, stating that disclosure is obligatory "…. when it is required by these (the entitled bodies) for the purposes of investigation, detection and prosecution of a crime that is provided for in the Penal Code or in the special criminal laws" (Nº 4).

There are no specific provisions which are different from those of the Directive as regards the purposes for which data retention is mandated in each case. Article 1 of the LCD mentions generally "the purposes of detection, investigation and prosecution of serious offences that are provided for in the Penal Code or in the special criminal laws". The mention of "serious offences" disappears in relation to the disclosure of data on the identification or prepaid telephone holders. Security investigations of people or entities within the context of intelligence activities may

also be considered as a purpose of the retention of data. This is deduced from the description of the staff of the National Intelligence Centre as being entitled to require the disclosure of data.

There are not specific rules in Spanish national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower).

The only reference may be derived from the rules governing the protection of data of a personal nature where the data are specially protected: those that reveal ideology, trade union affiliation, religion, beliefs, racial origin, health or sex life. But it is difficult for us to know when we are dealing with data of this nature as the contents of the communications or the information consulted upon is expressly excluded from the retention (Art. 1.3 of the LCD).

There are no specific laws on the point of exemptions from the obligation to retain or to transmit certain data that are worth being protected. The limits will be derived from weighing up the essential contents of the various fundamental rights at stake, with the principles of need and proportionality coming into play. In any event, it will have to be assessed by the judge at the time of granting the authorization to disclose the data, but not before.

In accordance with the national rules transposing the Directive the data are to be retained for twelve months, counting from the date on which the communication has taken place (Article 5 of the LCD). According to the rules and having previously consulted the operators, it is possible to lengthen or shorten the retention period for certain data or a data category to a maximum of twenty-four months or a minimum of six months. For this to happen it would be necessary to take into account the cost of the storage and conservation of the data, as well as their relevance to the general aims of the Law (investigation, detection and prosecution of a serious offence).

The authorities or other bodies entitled to access the data retained are described in Article 6.2 of the LCD. There are three cases: a) members of the Security Forces and Security Corps when they perform judicial police duties; b) officials of the Deputy Directorate of Customs Surveillance in carrying out their duties as Judicial Police; and c) the staff of the National Intelligence Centre when they carry out security investigations of people or entities. Disclosure of data to any other subject, either public or private, is not provided for.

The retained data may only be disclosed for the purposes that are determined in the law (Art. 6.1 of the LCD): detection, investigation and prosecution of serious offences that are defined in the Penal Code or in the special criminal laws. Their use for the exercise of the sanctioning power of the Administration (Administrative Law sanctioning), beyond the sanctions for not fulfilling the obligation to retain the data is not provided for.

For the exercise of civil actions nobody - neither individuals nor the Administration - is recognized as entitled to access the filed data. The question has been raised before civil courts on the subject of royalties for the purpose of determining the ownership of an IP address. It was resolved by the well-known ruling of the European Court of Justice (Grand Chamber) of 29/01/2008 (Subject C-275/06, Spanish Music Producers (PROMUSICAE) v. Telefónica de España, S.A.U.), in response to the prejudicial question raised by Commercial Court Nº 5 of Madrid.

Specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned before. The LCD refers to "serious offences" (Art. 1.1), a concept which is defined in Art. 13.1 of the Penal Code: those which carry a severe penalty. By virtue of Art. 33.2 of the Penal Code severe penalties are prison sentences of more than five years, absolute disqualification, special disqualifications for longer than five years, suspension of employment or from public posts for longer than five years, withdrawal of the right to drive motorized vehicles for more than eight years, etc.

This demand appears to be a literal translation of the text of article 1 of the Directive, but it has made use of the same term that is used by the Penal Code to classify offences. For this reason it is seen by some (for instance the Public Prosecutor and the Police) as an error of the legislator which leads to disproportionate outcomes, weakening and hampering the investigation. This criticism is not completely wrong as, for example, most of the offences that are committed through the use of electronic communications do not reach this degree of seriousness. Offences such as phishing scams, system intrusion, computer sabotage and even certain offences relating to child pornography are punishable with penalties of less than 5 years of deprival of freedom if there are no additional unfavourable factors.

We know however that the data are also requested and obtained on occasions for the investigation of offences which, strictly speaking, should not be regarded as "serious offences" (as they do not carry such severe penalties). It is probable that this occurs in practice because the interception of communications is not legally delimited with precision by the seriousness of the offence. There have therefore been demands for a proportionality judgment which takes into account not only the seriousness of the punishment, but also the protected legal asset, the commission of crimes by criminal organizations and that the incidence of the use of information technologies should be considered. This is observed, for example, in a ruling of the Constitutional Court concerning crimes against intellectual property (ruling 104/2006, dated 3rd of April).

Those data held may only be disclosed to the entitled bodies with prior judicial authorization (Art. 6.1 of the LCD). This court order is governed by Art. 7 of the LCD, which requires that it:

- be in compliance with the Law of Criminal Procedure (hereinafter referred to as LECrim). Examining magistrates are therefore assigned and it must be explained

and it will therefore be in the form of a court document (Art. 245 and 248 of the LOPJ -Organic Law on the Judiciary- and 141 of the LECrim)

- be issued in accordance with the principles of necessity and proportionality.

- establish a timeframe for implementation which takes account of the urgency of the disclosure, the purposes of the investigation involved, and the nature and technical complexity of the operation.

This requirement has been criticized by significant elements within the Police and the Public Prosecutor's Office who advocate its suppression stating that it is an added difficulty in criminal investigations.

The aggrieved party has no right to learn about the access to the data before it occurs: Art. 9.1 of the LCD provides that the person responsible for the processing of the data will not communicate the disclosure of data that has been carried out. This provision is provided for in the law connected with the data protection rules, as an exception to the rights of access and deletion.

A court order is necessary in all cases where retained data is requested, including data requests made by the CNI (National Intelligence Centre) whose personnel are "authorised agents", whereby they are subject to article 7.1. This authorisation is coherent with the previous judicial authorisation system provided in the single article of Organic Law 2/2002 of 6 May, which regulates the preliminary judicial control of the National Intelligence Centre.

Spanish law does not content a provision giving the aggrieved party the right to be notified of the data access before it takes place. After the access (or disclosure of the data) the obligation to notify will only exist if criminal proceedings are opened and these play an important role in the investigation. Although it is not directly provided for, this requirement stems logically from the generic right to a defence and other procedural guarantees. Art. 302 of the LECrim provides for the right of the parties "to learn of the legal proceedings and to intervene in all the steps of the proceedings", from which as a logical presupposition of the defence, it is deduced that the defendant has to be aware of the source of the evidence. Nor do we have any difficulties with deducing as much in a similar manner from the requisites regarding the intervention of communications that are being demanded by jurisprudence.

The investigation could be carried out and kept secret for a period of one month (which can be extended) and it will be necessary to appeal at least 10 days before the conclusion of the preparation stage (Art. 302.II of LECrim). This way it is possible to exclude the accused and the private prosecuting parties from having knowledge of all the investigative measures (but not the prosecutor who will always be able to have knowledge of them).

There is not a specific regulation of a right of the aggrieved party to be informed about the data accessed as far as they are related to him/her.

There are several means of defence against unlawful access to the data, and these can be made use of under various sets of rules:

a) If what is invoked is a failure to comply with the data protection rules, the method of defence will be to make an official complaint to the Spanish Data Protection Agency (Art. 8.4 of the LCD; 48 of the Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (hereinafter LOPDCP) [Organic Law 15/1999, of 13th December, Protection of Data Personal], and 122 of the Reglamento de desarrollo de la Ley de Protección de Datos de Carácter Personal (hereinafter RPDCP) [Regulation on the development of the Law on the Protection of Personal Data]).

b) If the disclosure of data does not translate into the initiation of legal proceedings, it would be possible to consider the liability of the Administration stemming from harm done to the private individual (Article 139 of Act 30/1992, dated 26th of November, on the Legal Regime of the Public Administrations and the Common Administrative Procedure). But it will only be possible to indemnify for harm when the private individual has no legal duty to bear it under the Law and, in this case, there is a legal provision (the LCD). We believe that the prospects of success in this case will be minimal.

c) Once the criminal proceedings are opened, the aggrieved party may request that the use of the data be declared unlawful if fundamental rights or freedoms have been violated either directly or indirectly (Art. 11.1 of the LOPJ). This is what would happen, for example, if there were no judicial authorization.

d) Finally, it would be possible to consider the lodging of a formal complaint for an offence of discovery and disclosure of secrets when the conduct was serious enough for it to be subsumed in the relevant offence: Arts 197 and following articles of the Penal Code.

The protection and guarantees of security of the data retained against unauthorized access are governed by Art. 8 of the LCD. This requires from the obligated parties firstly the identification of the personnel who are specially authorized to access the data. Furthermore, the adoption of technical or organizational measures preventing the following is required:

- their handling or use for purposes other than those included in it (in the authorization)

- their accidental or unlawful destruction

- their accidental loss

- their unauthorised storage, processing, circulation or access

These provisions, together with the obligations to guarantee the quality and confidentiality of the data and the protection level are connected with the rules on

personal data protection. The organ in charge of overseeing compliance with these provisions is the Spanish Data Protection Agency.

There are not specific provisions according the destruction by the accessing bodies of the transmitted data to them. Only by virtue of Articles 4.5 of the LOPDCP and 6 of the RPDCP data of a personal nature should be deleted and therefore blocked "when they are no longer necessary or relevant to the purpose for which they have been gathered or recorded." This provision is excluded in some cases: when the data have to be processed with a view to the data being made available to the Public Administrations, Judges and Courts, to attend to the possible responsibilities arising from processing and only during the life time of those responsibilities. Once this period has elapsed the data should be eliminated. (Art. 5.1.b) RPDCP).

1. The obligation to retain data

Duty to cooperate

The duty of individuals to cooperate with the Judicial Authorities has its constitutional basis in Art. 118 of the SC. This is likewise provided for in Art. 17 of the LOPJ and Art. 4.1 of the Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad-hereinafter LOFCS) [Organic Law 2/1986, of 13th March, on the Security Forces and Security Corps], but not too specifically.

Apart from the legal provisions, this duty could be specified in each case by means of suitable requirements for the completion of an activity by the authorities in charge of dealing with the offence. In these cases, it will be necessary to include a warning on the consequences of failure to comply, which could include the commission of offences such as disobedience and even complicity.

In areas such as electronic communications, the general duty is specific. Accordingly, article 33.2 of the LGT provides that "Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de Ley Orgánica. [Operators are obliged to perform the interceptions that are authorised in accordance with article 579 of the Rules of Criminal Procedure, Organic Law 2/2002 of 6 May, which regulates the preliminary judicial control of the National Intelligence Centre, and other organic laws]".

Owing to its similarity with data retention, we must make special mention of the conservation of documents provided in article 25 of Law 10/2010 of 28 April on the prevention of money-laundering and the financing of terrorism.

Article 24.2 of the SC provides the right to not declare against oneself and to not admit guilt. These rights are provided specifically for the detainee or prisoner in article 520.2.b) of the LECrim. With regard to the application of these rights to the provision of information by the accused, three levels of protection have been

defined for the right to refuse whatsoever procedure that leads to self-incrimination: maximum (associated with the verbal declarations made by the accused, not susceptible to being obtained by force or to the refusal thereof to be considered as any form of evidence), medium (body examinations and interventions affecting the accused, not susceptible to force but susceptible to the refusal thereof being considered as a form of evidence) and minimum (related to evidence obtained from sources other than the accused, which may be obtained with the use of force, such as documents, STC 76/1990 of 26 April; breathalyser tests, STC 103/1985 of 7 October; and radiological examinations, STS 590/2000, Criminal Chamber, 8 April).

The possibility of conflict referred to does not appear to exist. In its Judgement 205/2005 of 14 April, the Constitutional Court accepted that medical analyses carried out for diagnostic or therapeutic purposes could be provided for the prosecution of a crime against traffic safety.

In accordance with article 10 LCD, incompliance with the envisaged obligations will be sanctioned according to the provisions of the LGT, notwithstanding any eventual criminal responsibility that might arise from incompliance with the obligation to disclose data to entitled bodies.

Article 53 LGT typifies as very serious infringements, in section o), "el incumplimiento deliberado de las obligaciones de conservación de los datos…[deliberate incompliance with data retention obligations]", and in section z), "el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados…[serious or repeated incompliance with obligations pertaining to the protection and security of stored data...] ". Article 54 of the same Law typifies as serious infringements, in section ñ), "el incumplimiento de las obligaciones de conservación de los datos …, salvo que deban considerarse como infracción muy grave [incompliance with data storage obligations..., except where they should be considered as a very serious infringements]", and in section r), "el incumplimiento de las obligaciones de protección y seguridad de los datos…, salvo que deban considerarse como infracción muy grave [incompliance with obligations pertaining to the protection and security of the data..., except where they should be considered a very serious infringement]".

The reference to possible criminal liability in the case of incompliance with the obligation on access, refers to the criminal offence in article 556 of the Criminal Code (resistencia o desobediencia grave a la autoridad, con pena de prisión de seis meses a un año [resistance or serious disobedience towards authority, with a prison sentence of six months to one year].

Private companies obligated

In accordance with article 2 LCD, the following are obligated "…the operators that make electronic communications services available to the public or manage public communications networks, under the terms established in the LGT" […los operadores que presten servicios de comunicaciones electrónicas disponibles al

público o que exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones]". The LGT provides the following definition of an "operator" (Annex II, 21): "natural or legal personality that operates public electronic communications networks or makes electronic communications services available to the public and that has notified the Telecommunications Market Commission of the start of their activity [persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad]". The definition of "electronic communications service" is found in Annex II 28 and the "electronic communications network" in Annex II, 25, both from the LGT.

The LCD applies to operators, in other words, solely to those that provide continuous services, either completely or mainly, in the transport of signals through networks of electronic communications. It includes Internet access providers, but not providers that do not include access. With regard to the former, the LCD extends the duty of retaining not only the data corresponding to the Internet connection, but also to the other aforementioned services (email, Internet telephony), whenever they are also provided.

The duty of storing data is not limited to obligated parties in the private sector, but includes the Public Administrations whenever they act as operators of networks and/or providers of electronic communications services. It is contemplated in this way in the Circular 1/2010, de la Comisión del Mercado de las Telecomunicaciones, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por las Administraciones Públicas [Circular 1/2010 of the Telecommunications Market Commission, in regulation of the conditions for the management of networks and the provision of electronic communications services by Public Authorities] (approved under Resolution 18.06.2010, Official Bulletin of State 09.08.2010). On the contrary, those physical or legal persons that do not provide services that are available to the public are not obligated, which is the case of company intranet, universities, etc., as they do not come under the definition of "operator" that is used in the LGT.

Responsibility and cost for operators

Responsibility for data storage rests with the operators, the parties that are under an obligation to store the data (articles 2 and 4.1 LCD). Article 65.4 RLGT states that traffic data may only be processed by persons acting with the authority of the service provider or network operator that is responsible for logging and management of data traffic, for information requests from clients, fraud detection, commercial promotion of the electronic communications services, provision of a service with added value or supplying information required by courts and tribunals, by the Ministry of Justice or any other organs or entities that might require it.

Article 96 RPDPCP provides that "A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán,

al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título [As from the medium level, the information systems and data processing and storage installations will undergo, at least every two years, an internal or external auditory that will verify compliance with the present title]". Section 7 of Annex II of Order ITC/110/2009, of 28 January, regulates the auditing registries. In relation to this question, it is interesting to point out that in May 2009, the Spanish Data Protection Agency began an inspection to analyze whether the guarantees were being fulfilled on safeguards for stored data, security measures, data disclosures and the retention deadlines in the telecommunications sector in relation to the LCD.

There is no official study on cost. The estimates undertaken by various firms in the electronic communications sector put the costs at around €50 and €100 million per year.

The LCD only establishes in its Disposición Final Cuarta, apartado 2º [Fourth Final Provision, section 2] that "Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos [The obligated parties to which article 2 of this law refers will have a deadline of six months from its entry into force, to configure, at their cost, their equipment and to carry out the technical preparations to comply with the obligations on data storage and disclosure]". However, Annex II of Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados (BOE 15 de febrero de 2013) [Order PRE/199/2013, of 29th January, by defining the delivery format of data recorded by operators of electronic communications services or of public communications networks to authorized agents (Official Bulletin of State 15th February, 2013)] provides that the authorized agent will pay the installation and maintenance of the data stored transportation system.

Protection and guarantees of security of the data retained

This matter is considered in art. 8 LCD, which states, under sections 1 to 3, that:

"1. The obligated parties will have to identify especially qualified personnel to access the data that is the subject of this Law, adopt technical and organizational measures that will prevent their manipulation or use for purposes other than those contained in the law, their accidental or illegal destruction and their accidental loss, as well as their unauthorized storage, processing, divulgation or access, according to the provisions of... (the data protection regulation) [Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento,

tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la… (normativa de protección de datos)].

2. The obligations relating to measures to guarantee data quality and confidentiality and safety in their treatment will be those established in the... (the regulation on data protection) [Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la… (normativa de protección de datos)].

3. The level of protection of the stored data will be determined in accordance with the provisions of... (regulation on data protection). [El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la… (normativa de protección de datos)]".

This obliges us to make use of the security measures provided in the RPDCP. Its Article 81.4 demands that: a) the level of basic security (staff functions and duties, register of incidences, access control, management of data storage devices and documents, identification and authentication and back-up and recovery copies, the means to add the access register; b) the work environment (person in charge of security, accounting, management of devices and documents, identification and authentication, control of physical access and registry of incidences) and c) the access register.

We must also address measures of Annex II (security measures), with regard to Orden ITC/110/2009 del 28 de enero (BOE 3 de febrero de 2009) [Order ITC/110/2009 of 28th January (Official Bulletin of State 3rd February, 2009)], which, in accordance with the report from the Agencia Española de Protección de Datos [Spanish Data Protection Agency], meet the high level security requirements. Annex II of Order PRE/199/2013, of 29th January refers to this level of security.

The requirements arising from application of the aforementioned security levels, in accordance with article 81.7 RPDCP "tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero [are considered minimum requirements, without prejudice to legal provisions or specific regulations in force that could be applicable in each case or those that on their own initiative are adopted by the file manager]". With respect to disclosure, Order ITC/110/2009, of 28 January, envisages in section 8 of Annex II that "Las medidas de seguridad establecidas en esta orden se aplicarán sin perjuicio de cualesquiera otras medidas de seguridad adicionales… [The security measures in place in this order will be applied notwithstanding any other additional security measures" and likewise "Las medidas de seguridad se actualizarán por parte de los sujetos obligados según la evolución de la tecnología [the security measures will be updated by the obligated parties along with advances in technology]".

More specifically, article 97.1 RPDCP states that "Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de

envío y la persona responsable de la recepción que deberá estar debidamente autorizada [A system shall be set up to register incoming media that, either directly or indirectly, provide information on the type of document or storage media, the date and time, the sender, the number of documents or data included in the message, the type of information that it contains, the sending method, and the addressee who should be properly authorized]". These measures are controlled by the security manager or managers who should be designated, in accordance with article 95 RPDCP and relate to the responsibility of the operator (article 51.a) LGT).

We know of no specific regulations on data storage locations, beyond the guarantees on safety that are contemplated in various ministerial orders, particularly Order ITC/110/2009, which is applicable as its article 13 permits the assimilation of the data storage system the legal interception systems.

The requirement for storage in Spain arises from obligations in matters concerning the protection of personal data. Article 6 LGT does not require Spanish nationality for network operation or the supply of electronic communications services to third parties, although it does require the designation of a responsible person for the purposes of notifications registered in Spain. Article 8 LGT establishes as a condition for service provision and operation, the protection of the rights of the final users, including the protection of personal data, regulated under Chapter V of the of RLGT. Article 3 RPDCP identifies, as territorial scope of operation, data processing that is carried out within the framework of the activities of an establishment of the body responsible for processing or with equipment situated within Spanish territory, which is the case of operators that develop their activities in Spain. Acceptable compliance and supervision of the security measures, which include provisions relating to data retention, require their storage in Spain.

Supervision is dependent on the measures that must be adopted by the obligated parties to record access (article 103 of the Regulation). Article 8 of Order ITC/110/2009 includes authorization for accreditation purposes. The interfaces are regulated in that same order, in ITC/313/2010 (Official Bulletin of State 18.02.2010) and in ITC/682/2010 (Official Bulletin of State 19.03.2010). They are based on the provisions of articles 33.9 LGT and 95 RLGT, according to which "Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones [The obligated parties shall at all times have one or more interfaces prepared through which both the electronic communications that are intercepted and the information relating to interception shall be transmitted to the centres that receive the interception]". The reception of interceptions by the entitled body requires prior approval in the form of a court order, as only in that case may an interception order be technically activated. It is of interest to point out that the interception system which responds to the order in question (SITEL), was analyzed by the Spanish Data Protection Agency in its report of 19 January 2010, in which it concluded that access "se efectúa exclusivamente en los términos previstos por la autoridad judicial y para la investigación concreta a la que se refiera dicha autorización de interceptación, pudiendo acceder al sistema los agentes facultado

por ella designados [is carried out exclusively under the terms envisaged in the court order and for the specific investigation to which the authorization to intercept refers; the entitled bodies designated for that purpose being able to access the system]".

In this manner, Article 92.2 RPDCP sets down that "La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad [Outgoing media and documents that contain personal data, including the contents of e-mails and their attachments, sent out of the premises under the supervision of the person responsible for the file or its processing should be authorized by the person responsible for the file or have been duly authorized in the security document]". Section 5.3 of Annex II (security measures) of Order ITC/110/2009 establishes that "El acceso al sistema sólo será posible tras comprobar la identidad y la autorización de todo aquel que intente acceder, tras superar previamente con éxito los procesos de identificación, autenticación y autorización. Esta comprobación se hará preferiblemente mediante un dispositivo de autenticación fuerte conforme a la definición recogida en el apartado k) del apéndice [Access to the system shall only be possible after confirming the identity and the authorization of all those that attempt to access it, after successfully completing the identification, authentication and authorization processes. This testing will preferably be done through a strong authentication device in accordance with the definition in section k) of the appendix]".

Article 4.5 of the LOPDCP states that "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados [Personal data will be cancelled when it is no longer necessary or pertinent for the purposes for which it had been gathered or registered]". This has to be placed in relation to the maximum retention period in article 5.1 LCD, and article 16.3 LOPDCP (to which article 5.2 LCD makes reference). Cancellation will block the data, which will only be retained for public administrations, courts and tribunals, in order to look into any responsibilities arising from processing, during the period of their prescription. Once the aforementioned period is finished, the data should then be deleted. Nevertheless, we should highlight that there are no specific regulatory provisions that guarantee the destruction of the data once the storage period as required in the LCD is over.

2. Disclosure of data

Recipients

This matter is regulated in articles 6 (general rules on data disclosures) and 7 (data disclosure procedures) LCD, particularly in the second that establishes the following:

"1. Operators will be obliged to disclose stored data to the entitled body pertaining to communications that identify people, to which article 3 of this Law refers,

notwithstanding the court order envisaged in the following paragraph. [Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente]

2. The court order will determine, in conformity with the provisions of the Law of Criminal Procedure and according to the principles of necessity and proportionality, the stored data that have to be disclosed to the entitled bodies. [La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados]

3. The timeframe for compliance with the disclosure order will be fixed in the court order, considering the urgency of the disclosure and the purposes of the investigation to which it purports, as well as the nature and technical complexity of the operation. If no other time frame is set, disclosure must be made within seventy two hours calculated from 8:00 am of the working day subsequent to that on which the order is received by the obligated party [El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación. Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden]".

The retained data may only be disclosed to the entitled bodies described in Article 6.2 of the LCD. There are three cases:

a) the members of the Security Forces and Security Corps when they perform judicial police duties (Article 547 of the LOPJ. The term "Security Forces and Security Corps" includes not only the police corps who come under the State, but also those of the Autonomous Communities (regional authorities) and those of the Local Corporations. (Article 2 of LOFCS).

The role of the Judicial Police is described in Article 126 SC: "La policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la Ley establezca [The judicial police is answerable to the Judges, the Courts and the Public Prosecution in its roles of ascertainment of the offence and discovery and verification of the delinquent, in the terms that are provided for by the Law]". Their regulation for the purposes which concern us here is given in Art. 29 of the LOFCS which mentions certain specific units. Nevertheless it allows staff of the police forces of the Autonomous Communities and local corporations to carry out their Judicial Police duties, albeit in liaison with the State Security Forces and Security Corps.

In view of the interrelation between all these rules, the following police corps should be understood to be included in this item: the Civil Guard, the National

Police Corps and the Autonomous Police forces of Catalonia (known as Mossos d'Esquadra) and the Basque Country (known as Ertzaintza).

b) The officials of the Deputy Directorate of Customs Surveillance in carrying out their duties as Judicial Police. This is about a specific area of investigation, particularly relating to crimes of trafficking of drugs and other banned substances (Art. 283.1 of the Law of Criminal Procedure).

c) The staff of the National Intelligence Centre when they carry out security investigations of people or entities. The legal basis for this role is to be found in Act of Law 11/2002, dated 6th May, which governs the National Intelligence Centre, and Organic Law 2/2002, dated 6th May, which governs the prior judicial control of the National Intelligence Centre. The judicial authorisation in this case is coherent with the previous judicial authorisation system provided in the single article of Organic Law 2/2002 of 6 May, which regulates the preliminary judicial control of the National Intelligence Centre.

Although it is not provided for expressly, we believe that the Public Prosecutor could insistently request the relevant judicial authorization to gain access to the data in certain cases. We are referring specifically to the cases in which they are legally entitled to conduct investigations of a pre-trial nature (Art. 5 of Act of Law 50/1981, Art. 773.2 of the LECrim, etc.). In the exercise of such duties the Public Prosecutor could give instructions to the Judicial Police so that, if this right were not recognized, it would suffice to channel the request through the entitled bodies. It should also be said that this possibility becomes important in the context of judicial cooperation within the EU, where the Public Prosecutor has a key role.

Disclosure of data to any other subject, either public or private, is not provided for.

Form of disclosure

The disclosure of data should be in line with the contents of article 7 LCD. Fourth Final Provision, section 1 LCD establishes that "La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley [Disclosure to an entitled body of data whose retention is mandatory will be in an electronic format, in the form that is defined by the joint Order of the Ministries of the Interior, Defense and the Economy and the Treasury, that will be approved within a space of three months from the entry into force of this Law]". Order PRE/199/2013, of 29th January (article 2), whose rubric is "Formato de entrega de los datos a los agentes facultados" ["Delivery format of the data to the authorized agents"], states that:

Number of individual requests for transfer of data among all authorized agents more than 2,000.- In the framework of Law 25/2007, of October 18, the transfer to the authorized agents of the data whose conservation is mandatory by operators shall be made, when the number of individual requests for the transfer of data between all

authorized agents exceed 2,000 applications during the calendar year prior to the entry into force of this ministerial order, according to the format set out in the technical specification of European Institute Telecommunications Standardization Institute (ETSI) TS 102 657, Lawful Interception (LI) Retained data handling; Handover interface for the request and delivery of Retained data, with the modifications and clarifications set out in Annex I to this order ministerial.

Number of individual requests for transfer of data among all authorized agents no more than 2.000.-When an obligor has received a number of individual requests for transfer of data among all authorized agents no exceeding 2,000 applications during the year before the entry into force of the this ministerial order, or during subsequent years saw reduced the number of the same below and above 2,000 applications, instead of using the delivery format based on the ETSI TS 102 657 may choose to use another technology solution agreed previously authorized agents from the different formats for this case specified in Annex III, in electronic format and whose name will be adapted as defined in paragraph 7.1 of Annex I of the Ministerial Order.

To be eligible for this solution, the obligated party must notify each authorized agent have not been exceeded in the previous year 2,000 individual applications and petitions for alternative technological solution to the previously agreed. In any case the agreed technological solution must ensure compliance with required safety measures as set out in the regulations for the protection of personal data.

If in the first case no agreement was reached between the obligated mandatory and authorized agents or if the exemption established in the second case is exceeded then the number of 2,000 applications, apply the provisions of paragraph 1 of this Article.

Adoption period format-When an obligor has received a number over 2,000 individual requests data transfer during the year preceding the entry into force of this ministerial order (day following its publication in the Official Bulletin of State) or agreed the exception of paragraph 2 of this Article is exceeded then the number of 2,000 applications within a calendar year, shall have the period laid down by the Law 25/2007, of October 18, in his fourth final provision, to implement the assignment procedure based on the ETSI TS 102 657 adopted in this order. This period is counted from the entry into force of this ministerial order in the first case and from the moment you exceed the number of 2,000 applications within a year in the second.

With regard to the control of the disclosure, it should be distinguish between various circumstances:

a) Prior to the decision over the disclosure of data, the court responsible for authorizing access examines the situation. In accordance with article 7.2 LCD, “determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados [It will determine, in accordance with the contents of the Law on Criminal Procedure and in accordance with the

principles of necessity and proportionality, the stored data that have to be disclosed to the entitled agents]". The reference to the Law on Criminal Procedure may be justified as a way of integrating this measure into an ongoing criminal investigation. Perhaps the legal grounding may be found there for linking the disclosure of data to the existence of evidence of a criminal act having been committed by a particular party.

b) There are no provisions at all in relation to supervision following disclosure and verification of compliance with what is established in the court order (affected parties, disclosed data, timeframe). Supervision will take place in the framework of criminal procedure to which the disclosed data will be added as evidence and will be done by the instructing judge (judicial organ to which the address of the investigation belongs) or, in the case of an oral hearing, by the court that sits in judgment. Articles 11.1 (inefficacy of the evidence obtained, directly or indirectly, violating fundamental rights of freedoms) and 238 (nullity of the procedural acts) of the LOPJ.

c) Under the circumstances in which the data that is disclosed is not incorporated into a process (disclosure for the purposes of prevention or investigation that does not lead to proceedings), it may be understood that supervision, with regard to the protection of personal data, corresponds to the Spanish Data Protection Agency (article 8.4 LCD). The LOPDCP envisages as a serious infringement (article 44.4.b)), "The communication or disclosure of personal data, outside the cases in which it is permitted [La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas]". Supervision of the legality of disclosure for any motives other than these should be done through a challenge by the Administration itself (administrative recourse) or by challenging the rights of the Administration (contentious-administrative) (disclosure is categorized as a preventive police measure and, as a result, is of an administrative nature). Article 58.b) LGT empowers the Agencia Española de Protección de Datos to issue fines in that regard. It is an independent body (art. 35.1 LOPDCP), although it does not have a status that is comparable to a jurisdictional organ. For example, its Director is named by Royal Decree (article 36.1).

Security measures

In reference to the security measures applicable to the data given to the police force, we refer to Order ITC/110/2009.

After the media containing the information that has been obtained have been provided to the judicial authority, they are kept under the custody of the Clerk of the Court, since they constitute an object related to the court case (article 459 of the LOPJ).

We have no express regulation specifying the conditions of the custody, since Order 2590/2004 of the Ministry of Justice, dated 26 July, which regulates the general protocol for the computer security of the records of the Justice Administration, is not applicable to the conservation of computer media for use in criminal

proceedings. A recent law related to this subject (Law 18/2011 of 5 July, which regulates the use of information and communications technologies in the Justice Administration) also fails to provide for this matter.

There is no specific regulation in the LCD on access to the already retained data. In general, the functions of the judicial police grant them access as entitled bodies, on which basis criminal procedural rules will be applied relating to the disclosure of data to authorities in charge of a criminal investigation. The same is true in respect of information to which the CNI (National Intelligence Centre) has access which reveal acts likely to be of a criminal nature.

International transfer of data

No specific limits are established nor in the Constitution nor in Law in respect to the transmission of retained data to other countries.

The only limitations are found on occasion in the regulations on international movement of personal data (article 33 and 34 LOPDCP and Title VI of the RPDCP, Arts. 65-70). A level of protection that is comparable to that which is provided in Spain is required, particularly taking into consideration the nature of the data, the purpose and duration of the processing or of the envisaged processing, the country of origin and the final destination country, the general or specific Legal rules in force in the third country concerned, the content of the reports of the EU Commission, as well as the professional rules and the security measures in force in those countries. This will be verified by the Spanish Data Protection Agency. As a specific example we can point out that the disclosure of data from the List of Inhabitants to a foreign consulate is not admissible, even when it is of a Member State of the EU if this disclosure is not justified under the LOPDCP (Report 0425/2009 of the AEPD, i.e. the Spanish Data Protection Agency).

Some cases are excluded from this: when the international transfer of data arises from the application of treaties or conventions which Spain has signed or when the transfer is made for the purposes of providing or requesting international judicial assistance. This forces us to pay attention to the existence of treaties of this nature, which we will distinguish according to the territorial areas:

a) The European Union:

Data exchange is regulated by the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, done in Brussels on 29th May, 2000. Its Art. 6 gives the requests for assistance the form of direct communications between the authorities that have the competence to formulate requests for judicial assistance, avoiding the intervention of the Central Authorities. With regard to the cross-border exchange of personal data, its Art. 23 is determinative, defining the limits and conditions.

We also presume that the future regulations that transpose the following directives will be equally determinative:

- Council Framework Decision 2008/978/JHA of 18th December 2008, on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (DOUE L350 of 30.12.2008). Deadline for transposition is 19th January 2011 (Art. 23)

- Council Framework Decision 2008/977/JHA of 27th November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This will have to be incorporated before 27th November 2010 (Art. 29)

Nevertheless, neither of them has been incorporated into Spanish legislation as yet and there are no immediate provisions for reform on the matter.

In this way, the international requests for data will have to be in line with the actual premises of police and judicial cooperation.

With regard to common working language we presume that the use of European standards facilitates the exchange of data. We refer, for example, to the use of the technical specifications of the European Telecommunications Standards Institute on matters of interception of communications, which, undoubtedly, will be applicable to certain operational aspects of the disclosure of traffic data:

- ETSI TS 101 671 "Lawful Interception (LI), Handover Interface for the Lawful Interception of Telecommunications Traffic". This has been adopted in Spain by Order ITC/313/2010, of 12th February (Official State Gazette of 18.02.2010)

- ETSI TS 133 108 (3GPP TS 33.108) "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; handover interface for Lawful Interception (LI)". This has been adopted by Order ITC/682/2010, of 9th March (Official State Gazette 19.03.2010).

There is still no regulation however on specification ETSI 102 232, for the interception of IP based communications.

b) The Council of Europe:

In this area the text to refer to will be the European Convention of Mutual Assistance in criminal matters, of 20th April 1959 (ETS nº 30), particularly after it was supplemented by the Additional Protocol of 2001 (CETS nº 182). On the subject of the protection of personal data reference should be made to its Art. 26.

The general rule on the method of transmitting and returning the requests through the Justice Ministries (Art. 15 of the 1959 Convention) was superseded definitively in the second protocol to the Convention of 59, whereby requests for assistance could be made directly between the authorities in charge of criminal prosecution.

The Convention on Cybercrime was ratified by Spain very recently, the consent being expressed on 03.06.2010. This legal instrument will be applicable to Spain from 01.10.2010 onwards, although it has been used up to now in practice as a

reference document. The principle of favor cooperationis which rules it will be the main incentive for the international exchange of the data.

Other important Conventions which cover the cross-border exchange of information should also be mentioned. In these we may include telecommunications traffic data: the one on the prevention of terrorism (CETS 196), and the one on money laundering, and the search, seizure and confiscation of the proceeds from crime and on the financing of terrorism (CETS 198), both of 16th May 2005.

c) Cooperation with the United States

The bilateral treaty on mutual legal assistance in criminal matters between the United States of America and the Kingdom of Spain had been signed on 20th November 1990 but it was altered recently as a result of the Agreement on Mutual Assistance with the European Union that was signed on 25th June 2003. The text currently referred to is the the "Joint text of the provisions of the Treaty on Mutual (legal) Assistance of 1990 and of the Legal Assistance Agreement between the EU and the USA (Official State Gazette of 26.01.2010, which has been in force since 01.02.2010).

In accordance with its Article 2, the requests for cooperation should be channelled through the central authorities, who will communicate with each other. These Authorities will be: in the USA, the attorney-general or those designated by him, and in Spain, the Justice Ministry or those designated by it.

3. Socio-legal background from a Spanish perspective

Some remarks on the fundamental rights concerned

Ideological and religious freedom have two facets: positive (holding or no longer holding ideas and beliefs that are considered acceptable, without experiencing reprisals) and negative (not to be obliged to declare one's own beliefs or ideas). With regard to freedom of expression and freedom of information: the former consists of the manifestation and diffusion of thoughts, ideas and opinions, through the spoken or written word, or any other means of reproduction, while the latter comprises the freedom to communicate or to receive accurate information through any means of diffusion. The difference between the first and the second resides essentially in the requirement that the information be accurate (understood not in absolute terms, because the diligent confirmation of the credibility of the information is also understood to be acceptable, even though subsequently it is confirmed as false); a requirement that is required in news, and not in opinions.

We are unaware as to whether the consequences of data retention have been the subject of analysis for the rights of freedom of expression and information (article 20 SC) (except for some points on the restriction involved in the normal involvement of users of electronic communications). With regard to ideological and religious freedom (article 16 SC), it is not thought that these rights will be affected from the standpoint of data retention, as these data are not particularly sensitive or

protected. We could only point to its dissuasory effect, in relation to the above-mentioned rights.

Under article 18 SC. These are the right to honour, to personal and family privacy and own image (18.1), to the inviolability of the home (18.2), secrecy of communications (18.3) and to the protection of personal data. This last right has been construed by the jurisprudence of the Constitutional Tribunal, on the basis of 18.4 ("The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.").

The expression of the right to privacy is neither passive in jurisprudence nor in the literature. It follows that it is seen as a generic right, from which the other rights contemplated under article 18 SC flow. Although there are authors and judgments that attribute a positive dimension to this right (in line with the right to the protection of personal data), there is general agreement over its negative aspect: the exclusion of extraneous knowledge. With regard to its scope, jurisprudence follows a material criterion for its definition, according to which, what is considered private is that which has to be hidden to enjoy a dignified life with a minimum of quality. From this idea, the scope of the right is submitted to abundant casuistry. For example, bodily privacy and sexual orientation would be included, but not the personal wealth of the person, at least with regard to public authorities. Likewise, it should be pointed out that intimacy which is defended in article 18.1 is not only personal, but also a family right (although with less transcendence). The right to own image includes the image as a physical aspect of the person and also the voice, even though they are not presented as private.

The scope of the right to secrecy is usually identified with communications over a distance, which take place through secure channels (between particular people) in a communications infrastructure, regardless of the subjective sphere of those communicating (as secrecy of communications is not guaranteed in that regard). Thus, the Judgment of the Supreme Court, Criminal Chambers, 18th March, 2010. Article 18.3 SC solely refers to "secreto de las comunicaciones [secrecy of communications]", without specifically distinguishing between the "content". Constitutional Jurisprudence has affirmed the formal scope of the right, which protects the communication regardless of its intimacy. It provides no notion of "content", despite referring to this concept to affirm that the right to secrecy of communications does not stop there, but also extends to other aspects, such as the secrecy of the existence of the communication and the "circunstancias o datos externos [external circumstances or data]" (time, duration, destination).

We differentiate between a double formal content (data traffic) and material content (information whose voluntary transmission by the issuer to the receiver motivates the communication). Although certain authors and jurisprudence exclude the requirement for an enabling court order in order to intercept communications in areas such as labour or family relations, the requirement for a court order is generally upheld, and is unanimously upheld with regard to those issued for the purposes of a criminal investigation. The intervention, in any case, should be

justified as it is an action that curtails a fundamental right which, in the case of acts grounded in criminal proceedings, require the reasons to be stated for an enabling court order. The decision should be founded on the existence of evidence that a criminal act may have taken place, investigation of which justifies the measure, and on the relation with the person or persons affected by such an act, and should be in accordance with the principle of proportionality and its three requirements: effectiveness or suitability, necessity and subsidiarity, and proportionality stricto sensu.

Although it is not passive, the doctrine and jurisprudence has identified the right to the protection of personal data as right with a positive dimension that is intended to guarantee individual power and control over the use and destination of personal data, with the aim of preventing illegal traffic that harms the dignity and the right of the affected party. It translates into a range of powers that in the main consist of the judicial power to impose the completion or omission of certain behaviours on third parties the specific regulation of which the Law should establish (Judgment of the Constitutional Tribunal 292/2000, of 30 November).

The SC does not specifically set out the limits on the rights to honour, intimacy and own image, because of which they arise from their interaction with other legal or constitutionally protected rights, among which figure the repression of crime, particularly in relation to the right to privacy.

Article 18.3 SC, with respect to the right to secrecy of communications, requires a court order as necessary for its contravention. In the case of the right to protection of personal data, article 18.4 SC places limitations on the use of information processing to protect the honour, and personal and family privacy of citizens and the full exercise of their rights.

There is no specific provision referred to by part of the doctrine as "a right to the anonymity of the user or browser". The constitutional provisions related to the confidentiality of communications include article 18.1 (right to privacy), 18.3 (secrecy of communications) and 18.4 (in which the Constitutional Court has included the fundamental right to the protection of personal data). The protection afforded by each of these laws depends on the type of communications and the content thereof.

Case law (together with an important sector of similar doctrine) seems to be finding a place for an opinion in favour of a more limited right to the secrecy of communications than in the past, provided to define the cases in which a court decision is necessary for its implementation. According to this view, the secret would be subject to revelation only in communications characterised by the communicator's express will to exclude third parties from the exchange of communication (the case of telephone communications or electronic mail), but not those used for the broadcasting of information to an undetermined group of individuals (such as news forums and blogs, etc.)

For its part, the right to (material) privacy does not cover the entire content of communications, but rather only that which affects the most reserved individual sphere.

The right to the protection of personal data applies to communications in general. However, no right to anonymity has been deduced from said protection beyond the technical limitations to third-party access to the interlocutors' identities.

Constitutionality has not been questioned, except for some reference to the type of law by which the transposition has been regulated and precision over the requirement for an enabling court order. These nuances proceed from the Supreme Court, the highest judicial organ, which is not, however, empowered to supervise the constitutionality of the regulations that have the full force of a law. In this respect, "legally relevant" aspects of the lack of character of the Organic Law of the LCD have been noted (Judgment of the Supreme Court, Criminal Chamber, 18 November 2008). Firmly, but as an obiter dicta opinion, the Judgment of the Supreme Court, Criminal Chamber, of 20 May 2008, affirms that "no deja de llamar la atención la clamorosa insuficiencia, desde el punto de vista de su jerarquía normativa, de una ley que, regulando aspectos intrínsecamente ligados al derecho al secreto de las comunicaciones, y a la protección de datos personales, no acata lo previsto en el art. 81.1 de la CE [the clamorous failings do not cease to attract attention, from the perspective of its normative hierarchy, of a law that, regulating points that are intrinsically linked to the right to secrecy of communications, and the protection of personal data, fails to respect the contents of art. 81.1 of the SC]".

With regard to the requirement for judicial authorization, the non-jurisdictional General Chamber of the Supreme Court, on 23rd February, 2010, approved the agreement that "Es necesaria la autorización judicial para que los operadores que presten servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el artículo 3 de la Ley 25/2007, de 18 de octubre [A court order is necessary so that operators that provide services for electronic communications or public communication networks disclose the data that are generated or processed for such purposes. As a result, the Justice Ministry will require such an authorization to obtain the retained data from the operators which are specified in article 3 of Law 25/2007, of 18 October". This agreement reflects the Sentence of the Supreme Court, Criminal Chambers, of 18th March, 2010.

The obligations imposed by the LCD involve limitations on the freedom of the firm (article 38 SC) and private property (article 33) (with nuances, as the provision of communications services and the operation of networks is dependent on an asset in the public domain –the radioelectric spectra-). None of these two rights are found among the fundamental rights for which reason we ask ourselves whether the burden imposed on the activity amounts to a) a legitimate restraint on the freedom of enterprise and b) whether the social function that defines the content of the right to private property justifies that burden.

a) Company freedom is basically a right of access to an area and is not the regulation of that area in a particular way: the law can restrict company freedom in cases of conflict with other constitutionally protected rights.

b) With regard to private property, the presence of a general interest that should take precedence over the private allows burdens to be imposed that, in other cases, would not exist. Thus, it is necessary to look at the principle of proportionality, in such a way that, if the end that is pursued is legitimate and the sacrifice on the part of the operators is not excessive, it should be understood as in accordance with the SC.

It is of interest to highlight that firms, despite their inclination during the enactment of the law towards alternative measures other than data retention, have not questioned the constitutionality of the LCD from that point of view. We consider that its possible unconstitutionality does not arise directly from the burden that is imposed, which may be understood as justified when it serves the purpose of crime prevention and investigation, but precisely from the illegitimacy that we attribute to its delinking from the existence of evidence of a crime.

It is not a circumstance that has been recognised in jurisprudence as susceptible to creating the right to reimbursement. The LCD does not imply expropriation, as it does not singularly cause deprivation of private property or legitimate rights or patrimonial interests (article 33.3 SC). Neither does it constitute a legislative act as described in article 106.2 SC that refers to losses that may arise as a result of public services. Neither is it applicable to article 139.3 of Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y de Procedimiento Administrativo Común [Law 30/1992, of 26th November, on the Judicial Regime of the Public Administrations and Common Administrative Procedure] ("The Public Administrations will reimburse individuals due to the application of legislative acts the nature of which are not to expropriate rights, which these individuals have no legal duty to sustain, when it is so established in the legislative acts and in the terms that are specified in the aforesaid acts. [Las Administraciones Públicas indemnizarán a los particulares por la aplicación de actos legislativos de naturaleza no expropiatoria de derechos y que éstos no tengan el deber jurídico de soportar, cuando así se establezcan en los propios actos legislativos y en los términos que especifiquen dichos actos]").

All in all, it would be worth appealing to the expectations of the operators not to see alterations in the legal regime for the provision of services. But it is questionable whether that is enough to generate a right to be reimbursed, notwithstanding that it may appear appropriate to set up some sort of compensation (the Supreme Court has noted as much). In relation to this, article 100 RLGT contemplates sharing costs in the case of legal interception and which we understand might be partially in application.

Social context

The existence of widespread surveillance measures is known in Spain but their proliferation is being accepted without excessive criticism and without public debate

on the matter. Neither is this one of the problems that worries Spanish society, nor does it provoke any controversy in the non-specialist media.

The transposition of the Directive through the LCD did not provoke any major controversy in Parliament and all the parties represented supported the Bill, although with some minor points being raised. (There were 294 votes in favour, 12 abstentions and 0 against). The new rule was presented by all the media as a tool that is necessary for tackling serious crimes (terrorism, drug trafficking, etc) and those which make use of the communication networks (spreading of child pornography, computer fraud, etc).

Opposition to the LCD is only found in sectors that are very aware. This is the case, for example, of the Association of Internet Users (www.internautas.org), which entered a legal challenge against it. There are also some popular blogs which provide arguments against the LCD, such as the one by Enrique Dans (http://www.enriquedans.com), whose view is that it not only limits rights, but that it is also basically useless. It is very significant that among the signatories of the letter sent to the Commissioner Malmström on 22nd June 2010 regarding the reform of directive 2006/24 there was only one from Spain and, furthermore, it was very unrepresentative.

The item which gave the LCD the greatest public notoriety was the requirement for the users of mobile phones with prepay cards to be identified. But in general it was perceived as an annoying procedure which some people had to go through, rather than as meddling in basic rights.

Opinions are generally favourable among lawyers. The criticisms which the LCD receives do not concern any harm to rights, but rather the opposite. It is criticised for the following reasons: a) the obstacle of having to obtain a court order in order to go after crimes even when the secrecy of communications is not affected; b) the restrictions it imposes on the work of dealing with serious crimes.

It may be interpreted as a sign of a growing interest in this subject in legal circles the fact that the 2010 edition of the "La Ley" Prize, one of the most prestigious awards in legal circles in Spain, was won by a work relating to this subject. The title of the winner paper was "The disclosure of personal data for criminal investigation. A proposal for its immediate inclusion in the Law of Criminal Procedure". The authors of that paper are also the signatories of this present document.

This contrasts with the complete lack of debate on the holding of traffic data, and the intense confrontation with regard to the computer system for the interception of telecommunications (SITEL). Its legal and constitutional basis is called into question as is the very limited effectiveness of judicial supervisory functions over its operation. This debate is not limited to legal circles as it has fully reached the political arena, particularly through the efforts of the main opposition party, the Popular Party. The question cannot be separated from the involvement of some leading figures in that party in crimes relating to corruption and being investigated using the interception of communications.

Nevertheless, several rulings of the Penal Chamber of the Supreme Court have supported its operation (for example rulings 250/2009 and 1078/2009), although bringing to light some significant shortcomings. Also, a report from the Spanish Data Protection Agency (of 10.01.2010) has indicated that it believes that the system guarantees the satisfactory performance of the high level security measures provided for in the RLOPD, especially those relating to access to the system by its various users and the security of the transport of the software containing the information up to its handover to the judicial authority.

In Spain there are many obligations to collect data of a personal nature without a specific reason, some of which are fully taken for granted, particularly in the public sphere. The following are worth pointing out:

a) The National Identity Card - known in Spain by its initials DNI-, is a document that is used on a daily basis and is indispensable in day to day life, both in the public sphere and in private relationships. Currently the relevant rule to be referred to is Royal Decree 1553/2005, dated 23rd December, which governs the issue of the national identity card and its electronic signature certificates (Official State Gazette Nº 307, of 24th December). The Foreigners` Identification Number – known in Spain by its initials NIE – serves the same purpose for foreigners.

b) The Municipal List of Inhabitants is the administrative record of the inhabitants of each town. This disclosure of its data to other Administrations is permitted and this may include disclosure to the various police corps (Article 16.3 of the Law governing the Basis of the Local System (Law 7/1985, of 2nd April), drafted in accordance with the provisions of Organic Law 14/2003, of 20th November).

c) The Vehicles Record, governed by Art. 2.1 of the General Vehicle Regulation, which was approved by Royal Decree 2822/1998, of 23rd December. All police forces may have access to its data in the performance of their duties: the "maintenance of public safety and security".

d) Another essential basis for the requirement to retain data is to be found in Article 12 of Organic Law 1/1992, of 21st February, on the Protection of Law and Order, which provides in general terms for requirements for documented records and information when activities relating to law and order are involved. In each case it will be the specific rule which governs these requirements in detail, but the above mentioned law expressly includes various activities. Among these it is particularly worth pointing out the recording of lodging data (Article 45.1 of the Schengen Convention and Order INT/1922/2003 of 3rd July, on record books and check-in records of travellers in hotels and similar establishments). But reference is also made to the activities of trade or repair of used objects, renting or scrapping of motorized vehicles, buying and selling of jewels and precious metals, sailing in high speed boats, the manufacture, storage and trading of chemicals that could be used in the production or transformation of toxic drugs, narcotics, psychotropic substances and other substances that are seriously harmful to health.

With this legal background, the categories and retention times of telecommunications traffic data have not caused too many problems. As far as the

purposes of the Law are concerned, this is some discussion, particularly regarding the need for it to concern "serious offences". In general there are requests for an interpretation of the law which would allow the use of traffic data for the investigation of other offences too when these are the only possible sources of evidence.

The paper from the Public Prosecutor's Office presented in September 2010 (available at www.fiscal.es) expressly requests the modification of the LCD (pages 1258 and following) in two ways: a) the elimination of the judicial authorization when the traffic data do not enter into the secrecy of communications; b) the removal of the limitation to serious offences because this means not being able to deal with the great majority of crimes committed through the Internet.

4. Personal opinion and conclusion

In our opinion, the retention of data on a general scale should be considered unconstitutional, basically because it does not meet the requirements of intervention only in the case of evidence that should characterise all measures designed to limit fundamental rights for the prevention or prosecution of crime. Besides its questionable effectiveness, it is an indiscriminate measure since it affects all users of electronic communications to which the data that is conserved refers, where there are no suspicions that allow for the individualisation of the addressee of the interference and no appearance of crime that justifies the need for its prevention or investigation.

In the search for support for this type of action, the main reason found is the appreciation of the general risk of the commission of crime for the clarification of which the data that is conserved may be useful. It may be the case that, in the absence of such a measure, said data would not be available. However, that risk is completely generic and, owing to its lack of precision, we consider it insufficient to justify the existence of a need that legitimates a measure adopted regardless of the presence of evidence. In principle, the users of electronic communications networks are not responsible for sources of danger or not located in places that are dangerous on a spatial level. In our opinion, adopting measures with this capacity for interference without evidence of crime goes beyond what is acceptable in accordance with the principle of proportionality.

However, our opinion is not the most common among those (very few) who have considered the matter in Spain.

An improvement, clarification and updating of the whole criminal procedural rules is absolutely necessary in Spain. But in the short term there is insufficient political consensus to achieve it. Proposals for its improvement must therefore, regrettably, be very limited. From our perspective, the fundamental problem lies in the detached nature of evidence which implies the generalized retention of communications data. For this reason we are in favour of preservation measures such as those described in the Convention on Cybercrime.

We believe that we urgently need to coordinate the criminal procedural rules with the rules making it possible to disclose personal data in criminal investigations, so that this information can be regarded as a source of evidence that is fully respectful of fundamental rights. On this matter, our legislation suffers from insufficient "quality of rules" in the sense demanded by the jurisprudence of the European Court of Human Rights. We therefore propose a reform of the Law of Criminal Procedure to incorporate a preliminary step in the investigation, consisting in the empowerment of a court to require anybody to disclose personal data. Together with this, it would be necessary to provide for the order for the conservation of these same data for their subsequent disclosure, something which in urgent cases would also have to be issued by the police. Electronic communication traffic data would be one of the cases in which such a measure could be used.

We also believe that it is necessary to introduce explicitly the principle of proportionality in the acquisition and conservation of data, but especially in its subsequent disclosure. From the point of view of proportionality in the strict sense it would make it necessary to consider three elements:

a) The fundamental rights concerned, a factor which is closely linked to the type of data to be requested: each type of data affects different rights. The general underlying factor, present in all cases, will be the right to the protection of personal data.

b) The seriousness of the offence. Given the enormous casuistry in which it is possible to think it is not advisable to lay down by law a catalogue of offences or a penological threshold beyond which the measure may be used. The judicial organ should be left to attend to the seriousness of the offence and the penalty as items for them to weigh up, but only as factors for consideration.

c) The link between the type of data and a certain group of offences, which would help us understand their special relevance to the investigation. In the case of communication data (both of traffic and of subscriber) they would be relevant when going after crimes which leave traces on the communication networks. But this circumstance exists in relation to any type of data: bank data are particularly useful in the investigation of financial crimes, health data for those in which biological samples play an important role, those which reveal the ideological or religious content could be relevant in the investigation of crimes of terrorism.

Thus, for example, the requirement for data which are particularly relevant to the investigation of a certain offence could be acceptable, even when the offence was not particularly serious (for example: the disclosure of communications traffic data to investigate threats made through electronic mail). Likewise the requirement for specially protected data would be justified when they were highly relevant to the investigation of a crime of extreme seriousness (for example: the disclosure of the data on a religious organization to investigate a terrorist attack). Or, the disclosure of data that are not specially protected could be justified to investigate a crime to which they are not particularly relevant, but the crime is very serious (for example

data on stays at hotels or other such establishments in order to follow the trail of murderers).

5. Literature

- CABEZUDO RODRÍGUEZ, N., "La Administración de Justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando por el olvido", *Revista Jurídica de Castilla y León*, n.º7, octubre 2005.
- CORRIPIO GIL-DELGADO, Mª.R. y MARROIG POL, L., *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones*, Agencia de Protección de Datos, Madrid 2001.
- ETXEBERRIA GURIDI, J.F., *La protección de los datos de carácter personal en el ámbito de la investigación penal*, Agencia de Protección de Datos, Madrid 1998.
- FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones en Internet*, Thomson-Civitas, Madrid 2004.
- GONZÁLEZ-CUÉLLAR SERRANO, N., "Garantías constitucionales de la persecución penal en el entorno digital", VVAA, *Derecho y Justicia penal en el siglo XXI*, Colex, Madrid 2006.
- GONZÁLEZ LÓPEZ, J.J., *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal*, La Ley, Madrid 2007.
- GONZÁLEZ LÓPEZ, J.J., "La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica", *Diario La Ley*, n.º6456, 5 de abril de 2006.
- GONZÁLEZ LÓPEZ, J.J., "Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones", *Revista General de Derecho Procesal*, n.º 16, octubre 2008.
- GONZÁLEZ LÓPEZ, J.J., "Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva", PEDRAZ PENALVA, E. (coordinador), *Protección de datos y proceso penal*, La Ley, Madrid 2010.
- GONZÁLEZ LÓPEZ, J.J., "Consideraciones acerca de las dificultades conceptual e iusfundamental planteadas por los datos de las comunicaciones electrónicas en la investigación penal", CABEZUDO RODRÍGUEZ, N. (editor), *Inclusión digital: perspectivas y experiencias*, Prensas Universitarias de Zaragoza, Zaragoza 2011.
- GUERRERO PICÓ, M.C., "Protección de datos personales e Internet: la conservación indiscriminada de los datos de tráfico", *Revista de la Facultad de Derecho de la Universidad de Granada*, n.º8, 2005.
- HERNÁNDEZ GUERRERO, F.J., "La intervención de las comunicaciones electrónicas", Estudios Jurídicos del Ministerio Fiscal, III-2001.
- LLAMAS FERNÁNDEZ, M. Y GORDILLO LUQUE, J.M., "Medios técnicos de vigilancia", VELASCO NÚÑEZ, E. (director), *Los nuevos medios de investigación*

en el proceso penal. Especial referencia a la tecnovigilancia, Consejo General del Poder Judicial, Madrid 2007.

- LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, La Ley, Madrid 2011.
- LÓPEZ YAGÜES, V., *La inviolabilidad de las comunicaciones con el abogado defensor*, Tirant lo blanch, Valencia 2003.
- LUCAS MURILLO DE LA CUEVA, P., "Los derechos fundamentales al secreto de las comunicaciones y a la autodeterminación informativa", VVAA, *Derechos procesales fundamentales*, Consejo General del Poder Judicial, Madrid 2005.
- MARCHENA GÓMEZ, M., "Dimensión jurídico-penal del correo electrónico", *Diario La Ley*, n.º 6475, 4 de mayo de 2006.
- MARCHENA GÓMEZ, M., "La intervención del mensaje corto de telefonía móvil (sms)", *E-newsletter*, n.º 50, junio 2009.
- MUÑOZ DE MORALES ROMERO, M., "La intervención judicial de las comunicaciones telefónicas y electrónicas", GONZÁLEZ-CUÉLLAR SERRANO, N. (director), *Investigación y prueba en el proceso penal*, Colex, Madrid 2006.
- ORTIZ PRADILLO, J.C., "Tecnología versus Proporcionalidad en la Investigación Penal: la nulidad de ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas", *La Ley Penal*, n.º 75, octubre 2010.
- PEDRAZ PENALVA, E., "Principio de proporcionalidad y principio de oportunidad", PEDRAZ PENALVA, E., *Constitución, jurisdicción y proceso*. Madrid: Akal, 1990.
- PEDRAZ PENALVA, E., "La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva", PEDRAZ PENALVA, E. (coordinador), *Protección de datos y proceso penal*, La Ley, Madrid 2010
- PÉREZ GIL, J. Y GONZÁLEZ LÓPEZ, J.J., "Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal", *Diario La Ley*, nº 7401, 13 de mayo de 2010.
- PÉREZ GIL, J., "Medidas de investigación y de aseguramiento de la prueba en el «Convenio sobre el cibercrimen»", *Actualidad Penal* nº36, Semana del 29 de septiembre al 5 de octubre de 2003.
- PÉREZ GIL, J., "Investigación penal y nuevas tecnologías: algunos de los retos pendientes", *Revista Jurídica de Castilla y León*, n.º7, octubre 2005.
- PÉREZ GIL, J., "Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal", *Revista jurídica de Castilla y León*, n.º14, enero 2008.
- PÉREZ GIL, J., "Los datos de localización geográfica en la investigación penal", PEDRAZ PENALVA, E. (coordinador), *Protección de datos y proceso penal*, La Ley, Madrid 2010.
- RODRÍGUEZ LAINZ, J.L., *Intervención judicial en los datos de tráfico de las comunicaciones*, Bosch, Barcelona 2003.

- RODRÍGUEZ LAINZ, J.L., "El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones" (I y II). *Diario La Ley*, n.º6859 y 6860, 11 y 12 de enero 2008.
- RODRÍGUEZ LAINZ, J.L., "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas", *Diario La Ley*, n.º 7689, 7 de septiembre de 2011.
- VIDAL FUEYO, Mª.C., "Libertades públicas y nuevas tecnologías", en GALINDO, F. (coordinador), *Gobierno, Derecho y tecnología: las actividades de los poderes públicos*, Thomson/Civitas, Cizur Menor (Navarra) 2006.