IV. *LA PROTECCIÓN DE DATOS EN EL ÁMBITO ESPAÑOL Y EL PANORAMA JURÍDICO BRASILEÑO*

Sabrina Morais[1]

1. Introducción. 2. Normativa aplicable 3. Creación y Gestión de ficheros de titularidad privada 4. El panorama jurídico brasileño y el movimiento internacional de datos 5. Conclusiones.

1. Introducción

El objetivo del artículo que ahora se presenta es bosquejar una visión de conjunto de la normativa española actual acerca de la protección de datos, haciendo hincapié en las cuestiones relacionadas con la creación y gestión de ficheros de titularidad privada, la protección de datos privados por los responsables del fichero o encargados de su tratamiento, estableciendo algunas relaciones con la realidad brasileña acerca del tema en lo concerniente al movimiento internacional de datos.

El estudio se fundamenta en la creciente relevancia del tema en la sociedad contemporánea, a consecuencia del aumento significativo de las actividades informáticas y de la mayor preocupación de la conservación y tratamiento de datos personales y sus reflejos en el derecho a la privacidad.

2. Normativa Aplicable

El derecho fundamental a la protección de datos personales en España deriva de la Carta Constitucional Española que, en el marco de una sociedad abierta y democrática resguarda a la totalidad de la sociedad española la facultad de controlar sus datos y ejercer un poder de disposición y decisión sobre los mismos. Así, al reconocer el derecho a la dignidad de la persona y el derecho a la limitación del uso de la informática como modo de garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, la Constitución Española en sus artículos 10 y 18.1 y 4, respectivamente, resguarda el derecho fundamental a la protección de los datos personales.

Artículo 10.

1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social.

[1] Sabrina Morais. Doctora en Derecho por la Pontifica Universidad Católica de São Paulo y Universidad Complutense de Madrid. Especialista en Derecho Español por la Universidad de Alcalá de Henares. Estudiante del Master en Asesoría Jurídica Empresarial por el Centro de Estudios Financieros de Madrid. Abogada vinculada al despacho SCA Legal Abogados y Consultores, en Madrid. Contacto: sabrina.morais@sca-legal.com

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

……..

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[2]

A través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en lo sucesivo LOPD, se resguarda el derecho fundamental a la protección de datos en España, siendo la Agencia Española de Protección de Datos el órgano público encargado de tal tarea.

La Agencia española de protección de datos, con su Estatuto aprobado por el Real Decreto 428/1993, tiene por objetivos generales velar por el respeto a la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de los mismos.[3]

El derecho fundamental a la protección de datos también esta resguardado por un conjunto de Leyes, Resoluciones y Decisiones judiciales que en su esencia crean mecanismos de protección, reglamentan actuaciones y establecen procedimientos en caso de ofensa a tal derecho. Deben pues, ser interpretados según los preceptos del derecho internacional de la protección de datos, la Constitución española y la Ley 15/1999.[4] Entretanto, después de casi

---

[2] Constitución Española de 1978. Acceso en 31.10.2007. Disponible en: http://noticias.juridicas.com/base_datos/Admin/constitucion.t1.html Importante resaltar que los derechos constantes en la Sección Primera del Capitulo II de la Constitución, en especial el art. 18, poseen un complejo sistema de garantías que comprende la protección mediante un procedimiento preferente y sumario ante los tribunales ordinarios y mediante el recurso de amparo ante al Tribunal Constitucional (art. 53.2 CE), comparable al "*Mandado de Segurança*" brasileño.

[3] Asimismo, la Agencia Española de protección de datos promueve campañas de difusión de la legislación, informando a los afectados de sus derechos y recibiendo sus peticiones de reclamación. Tiene competencias para emitir autorizaciones para transferencias de datos, requerir medidas de corrección, ejercer la potestad sancionadora y recabar ayuda e información que precise para la buena tutela del derecho de protección de datos personales, dictando Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD. En materia de telecomunicaciones, la Agencia española de protección de datos tutela los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente. Del mismo modo, vela por la publicidad de los tratamientos y desarrolla cooperación internacional en materia de la protección de datos personales. Disponible en: https://www.agpd.es Acceso en 31.10.2007.

[4] Son diversas las referencias acerca de la legislación y decisiones judiciales acerca del tema: Constitución Española de 1978, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Sentencia 290/2000, de 30 de noviembre de 2000, del Tribunal Constitucional. Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5-1992, Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los artículos 21-1 y 24-1 y 2 de la Ley Orgánica 15-1999, Real Decreto 428/1993, de 26 de marzo,

ocho años de publicación de la LOPD, sus disposiciones todavía siguen pendientes de reglamentación, de modo que la Agencia Española de Protección de datos orienta a la aplicación e interpretación de la LOPD según el amplio resguardo de los derechos en ella reconocidos y bajo los preceptos de la Constitución Española, que en el marco de la protección del derecho fundamental a la intimidad resguarda su efectividad.

Del mismo modo, en el Tratado por el cual se establece la Constitución Europea se reconoce el derecho fundamental a la protección de datos, donde todos los países miembros de la Unión Europea deben desarrollar mecanismos para resguardar y proteger tal derecho, contando con una autoridad independiente que lo tutele. Tal derecho se recoge de la parte I, título VI, referente a la vida democrática de la Unión, en el artículo I-51, referente a la protección de datos de carácter personal, donde "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" y en la parte II, concerniente a la Carta de los Derechos Fundamentales de la Unión, en su título II, que hace referencia a las libertades y en el artículo II-68 que añade que los datos de carácter personal "se tratarán de un modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de

---

por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica, Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados., Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, Resolución de 22 de junio de 2001, de la Subsecretaría de Justicia, que concreta el plazo para la implantación de medidas de seguridad de nivel alto, Resolución de 30 de mayo de 2000, de la APD, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático, para la inscripción de los ficheros, Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos, Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático, Resolución de 8 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se corrigen errores en las Resoluciones de 12 de julio de 2006, por las que se crea el Registro Telemático y se aprueban los formularios electrónicos para inscribir los ficheros en el Registro General de Protección de Datos, Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos, Instrucción 1/1995 de 1 de marzo de la APD relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

Instrucción 2/1995, de 4 de mayo, de la APD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal, Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, Instrucción 2/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo, Instrucción 1/1998, de 19 de enero, de la APD, relativa al ejercicio de los derechos de acceso rectificación y cancelación de datos, Instrucción 1/2000, de 1 de diciembre, de la APD, relativa a las normas por las que se rigen los movimientos internacionales de datos, Sentencia de la Audiencia Nacional , de 15 de marzo de 2002, en relación con la Instrucción Número 1/2000, de 1 de diciembre, Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones, Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. De la legislación autonómica aplicable al tema se puede hacer referencia a la Ley 8/2001 (CAM), de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, Ley 5/2002 (Comunidad Autónoma de Cataluña), de 19 de abril, de la Agencia Catalana de Protección de Datos, Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

otro fundamento legítimo previsto por la ley, y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

Así, los países miembros de la Unión Europea a través de las Directivas, Reglamentos, Convenios y Decisiones de las Comisiones están obligados a fomentar a través de su legislación interna la protección del derecho fundamental a la protección de los datos personales, creando una autoridad independiente que controle y garantice tal derecho. [5]

En este sentido, la manutención de los datos y su tratamiento debe orientarse según el principio de la lealtad y licitud, de modo que se respete el consentimiento del interesado o que exista normativa reglamentando los límites de esta utilización cuando es realizada sin su consentimiento.

Asimismo, el interesado del que se recaben los datos debe ser informado al tiempo de su recogida de la identidad del responsable del tratamiento, los fines para que los datos vayan a ser tratados y sus derechos, resguardándose la transparencia del procedimiento.

El tratamiento de los datos debe estar orientado según medidas de seguridad y confidencialidad, estableciendo limitaciones a las transferencias internacionales de datos a países que no ofrezcan garantías adecuadas, salvo que cuenten con autorización de las autoridades competentes. Estas autoridades, léase la Agencia Española de Protección de Datos, deben realizar el control del tratamiento de los datos personales, de modo a garantizar la efectividad de la normativa vigente, actuando con plena independencia e imparcialidad y estableciendo un régimen sancionador en casos de incumplimiento de la legislación.

3. Creación y Gestión de ficheros de titularidad privada

La Ley 15/1999 establece las directrices y principios básicos de protección de datos que, orientados en los acuerdos y directrices internacionales adoptados en este ámbito, deben orientar la actuación del sector público y privado en el Estado Español.

---

[5] Entre las Directivas Comunitarias relacionadas con el tema se puede hacer referencia: Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE; Directiva 2004/82/CE, del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas; Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas); Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal); Directiva 2002/21/CE, del parlamento Europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas; Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización); Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso); Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) y, por último, Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

El objeto de la Ley está regulado en sus artículos 1 y 2.1, que expresamente establecen:

> "*Artículo 1. Objeto:*
> *La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.*
> *Artículo 2. Ámbito de aplicación:*
> *La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado."*

Por ello, según informe emitido por la Agencia Española de Protección de Datos, no le es de aplicación a la Ley Orgánica 15/1999 los datos de personas jurídicas[6] y los datos de las personas fallecidas, aplicándole los datos de las personas físicas y de los empresarios individuales; la grabación de datos de voz e imágenes, siempre que se pueda identificar a las personas que aparecen en las mismas y se hallen incorporadas a ficheros informáticos y los ficheros de empresas que tengan una relación de personas físicas de contacto, como Administradores, Gerentes, Directores Generales, Comerciales, etc.

Así pues, en los términos del artículo 25 de la LOPD sólo podrán crearse ficheros de titularidad privada mediante previa notificación a la Agencia Española de Protección de Datos, cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de los referidos datos personales.

No obstante, la Agencia Española de Protección de Datos evaluará la posibilidad de inscripción o no del fichero previa información acerca de la titularidad del mismo, su finalidad, ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

El responsable del fichero debe comunicar a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación, así como la cesión de datos, indicando quien son los afectados, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario, salvo en los supuestos previstos en los apartados 2, letras c, d, e y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Las letras c, d, e y el apartado 6 del artículo 11 de la LOPD hacen referencia al tratamiento de datos que responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho

---

[6] Disponible en: https://www.agpd.es/upload/Canal_Documentacion/Informes%20Juridicos/Ambito%20de%20Aplicacion/A%20%282001-0000%29%20%28%E1mbito%20subjetivo%20de%20la%20aplicaci%F3n%20de%20la%20LOPD%29.pdf

tratamiento con ficheros de terceros; cuando la comunicación que deba efectuarse tenga por destinatario a instituciones autonómicas análogas al Defensor del Pueblo o al Tribunal de Cuentas o cuando sea destinatario el Defensor del pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Del mismo modo, cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

La LOPD entre los artículos 28 y 32 hace referencia a la gestión de los distintos ficheros de datos, determinando modos distintos según la naturaleza del fichero y los objetivos del mismo, como por ejemplo los ficheros creados por empresa dedicada a la prestación de servicios de información sobre solvencia patrimonial y crédito, fines de publicidad y de prospección comercial o a la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas.

Así, autoriza, bajo previa evaluación de la Agencia Española de Protección de Datos a la creación de códigos deontológicos que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo, a través de acuerdos sectoriales, convenios administrativos o decisiones de empresa orientadas según los principios de la LOPD.

En los artículos 4 al 12 de la LOPD se regulan los principios de la protección de los datos, estableciendo que el responsable del fichero y en su caso el encargado del tratamiento deberán, considerando la naturaleza de los datos y la tecnología disponible adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, ya provengan de la acción humana o del medio físico o natural.

La LOPD en su disposición transitoria tercera mantiene la vigencia de las normas reglamentarias preexistentes, entre las que se cita el Reglamento de Medidas de Seguridad, en cuanto no se oponga a la Ley. Así pues, como el Reglamento de la LOPD todavía no ha sido publicado, las medidas de índole técnica y organizativas necesarias a la garantía de la seguridad de los datos de carácter personal se encuentran desarrolladas en el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio, todavía vigente.

Desde la entrada en vigor de la LOPD, tal Reglamento resulta aplicable a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la Ley Orgánica, el 14 de enero de 2000. “Los ficheros en soportes no automatizados que existieran antes de dicha fecha dispondrán, a estos efectos, del período de adaptación establecido en la Disposición Adicional Primera (finalizado en octubre de 2007)”, según aclara la Agencia Española de Protección de Datos.[7]

De este modo, aunque no exista concretamente una normativa relacionada con los ficheros en papel, la Agencia Española determina que su seguridad sea realizada de acuerdo con el sentido común, debiendo los mismos ser almacenados en sitios cerrados y con llaves,

[7] Información disponible en: https://www.agpd.es/index.php?idSeccion=162. Acceso en: 21/10/2007.

reuniendo todos los cuidados típicos para preservación de documentos relevantes. Asimismo, los datos personales de carácter electrónico requieren requisitos y condiciones distintas de tratamiento, diferenciando los niveles de seguridad en básico, medio y alto.[8]

Así pues, la empresa será responsable por la integridad y seguridad de los datos así como a las de los centros de tratamiento, locales, equipos, sistemas y programas utilizados en el almacenaje y tratamiento de los datos.

Se reconoce el deber de secreto de los datos, de modo que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

La comunicación de datos a terceros es admisible sólo y cuando la comunicación sea fundamental para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario y previo consentimiento del interesado, con las excepciones dispuestas en el apartado 1 del artículo 11 de la LOPD, ya referenciadas anteriormente.

Cabe resaltar que no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento, es decir, cuando se le entregue los datos para que complemente el desarrollo de las actividades del responsable del fichero.

Esta actividad debe ser precedida de un contrato escrito que delimite la forma de gestión de los datos, siendo expresamente prohibida la divulgación a otras personas, ni siquiera para su conservación, aunque ya exista por parte del Poder Judicial Español decisiones que limitan tal precepto.[9] Asimismo, cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. Cualquier divulgación o utilización distinta de lo dispuesto contractualmente originará la responsabilidad por el tratamiento de los datos, tanto del encargado como del responsable del fichero.

4. El panorama jurídico brasileño y el movimiento internacional de datos.

La progresiva inserción de las actividades informáticas ya se hace realidad en la mayoría de las sociedades contemporáneas y, en Brasil, crece cada día el número de ficheros

[8] La Agencia Española de Protección de Datos ha elaborado un cuadro resumen acerca de las medidas de seguridad aplicables a todos los ficheros de datos. Disponible en: https://www.agpd.es/upload/Informa%20AEPD/cuadro_reglamento1.pdf Acceso en: 21/10/2007.

[9] Sentencia de la Audiencia Nacional, de 15 de marzo de 2002, en relación con la Instrucción Número 1/2000, de 1 de diciembre. Disponible en :https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.18%29%20Sentencia%20de%20la%20Audiencia%20Nacional.pdf. Acceso en; 21/05/2005.

de datos de personas físicas de las más distintas actividades sociales. Este progresivo cambio fomenta la pregunta de cómo estas informaciones son almacenadas y protegidas contra personas mal intencionadas, ya que el derecho brasileño no posee ninguna regla específica acerca de la protección de las informaciones provenientes de datos.

Mucho se habla del derecho a la privacidad de la persona en Brasil, comprendido en su sentido amplio al englobar la prerrogativa de preservación de un espacio inquebrantable e inaccesible a favor de la persona en el ejercicio de su vida privada. Tal derecho está garantizado a través de un gran conjunto de normas que hacen referencia al mismo, empezando por la Constitución Federal, que en su artículo referente a los derechos fundamentales reconoce como inviolables la vida privada, el honor y el imagen de las personas, asegurando el derecho a la indemnización por daño material o moral en caso de violación.

Del mismo modo, la Constitución hace referencia al sigilo de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas, en esta última hipótesis relativizado en los casos de investigación criminal o instrucción procesal penal en los términos del art. 5º, XII y Ley nº 9.296/96. Como instrumento de tutela del derecho a la información personal, la Constitución resguarda el habeas data para asegurar el conocimiento de informaciones relacionadas con la persona del impetrador, constantes en los registros o bancos de datos de entidades gubernamentales o de carácter público. Por último, se resguarda la libertad de rectificación de estos datos, cuando no se prefiera realizado dentro de un proceso sigiloso, judicial o administrativo.

La otra referencia relevante consta en el Código de Defensa del Consumidor [10] al reconocer que el consumidor tendrá libre acceso a sus informaciones cuando constantes en ficheros públicos o privados de consumo, los cuales deben ser claros, objetivos y verdaderos, no pudiendo constar informaciones por más de cinco años.

También el Código Penal, a través del establecimiento de algunas conductas típicas hace referencia a la existencia de datos y su incorrecta inserción para obtención de ventajas indebidas. Asimismo, la Ley General de Telecomunicaciones y la Ley de Política Nacional de Informática hacen referencias a los datos informáticos y a los principios orientadores de las conductas relacionadas con estos ficheros.[11]

---

[10] Código de Defensa del Consumidor (Ley nº 8.078/90)

§ 3° El consumidor, siempre que encontrar inexactitud en sus datos y ficheros, podrá exigir su inmediata corrección, debiendo el responsable por el fichero, en el plazo de cinco días hábiles, comunicar el cambio a los eventuales destinatarios de las informaciones incorrectas."

[11] Artículo. 2º de la Ley 7.232/84 acerca de la Política Nacional de Informática:

"VIII - establecimiento de mecanismos e instrumentos legales y técnicos para la protección del sigilo de los datos almacenados, procesados y difundidos del interés y de la privacidad y de seguridad de las personas físicas y jurídicas privadas y públicas."

"IX - establecimiento de mecanismos e instrumentos para asegurar a todo ciudadano el derecho al acceso a la rectificación de informaciones sobre ele exigentes en base de datos publicas o privadas"

"Art. 72. Sólo en la ejecución de su actividad, la prestadora podrá valerse de informaciones relacionadas con la utilización individual de los servicios por el usuario.

Entretanto, la ausencia de una norma específica dificulta sobremanera las relaciones comerciales de Brasil con los países europeos. De acuerdo con lo que ya fue dicho en su momento, es fundamental que se establezca una normativa adaptada a las necesidades urgentes del comercio e integración internacional, es decir, que haga referencia a los datos informáticos de usuarios de redes electrónicas, su forma de colecta y tratamiento así como las sanciones en caso de no respeto y los órganos responsables por la tutela y aplicación práctica de tal derecho.

Esto se evidencia en los casos de las transmisiones de informaciones, como por ejemplo, según la legislación española, que cuando sea para el exterior del territorio español, se constituye una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable de fichero, constituyen transferencia internacional de datos, según la Norma Primera de la instrucción 1/2000 de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los Movimientos Internacionales de Datos, en consonancia con la LOPD en sus artículos 33 y 34 al determinar que:

Artículo 33. Norma general

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

---

§ 1° La divulgación de las informalidades individuales dependerá de la anuencia expresa y específica del usuario.

§ 2° La prestadora podrá divulgar a terceros las informaciones agregadas sobre el uso de sus servicios desde que ellas no permitan la identificación directa o indirecta del usuario o la violación de su intimidad"

c. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e. Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j. Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k. Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

La Instrucción 1/2000 ha fijado los criterios seguidos por la Agencia Española de Protección de Datos en la materia, aclarando el procedimiento a seguir para dar cumplimiento a las previsiones contenidas en la normativa reguladora del tema. Así, en el supuesto del movimiento internacional de datos, hay que identificar:

a) la naturaleza de los datos, finalidad y duración del tratamiento o de los tratamientos previstos;

b) país de origen y destino de los datos, asimismo si la legislación del país de destino final presenta un nivel de protección adecuado de los mismos.

c) Identificación de la actuación jurídica de las entidades relacionadas en la trasferencia, si son responsables del fichero o encargadas del tratamiento, según lo dispuesto en la LOPD.

d) existencia de autorización del Director de la Agencia de Protección de Datos.

El apartado 1 del artículo 2 de la LOPD española dispone:

"Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito

Asimismo, el artículo 4 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece que:

"1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento."

En el supuesto de que sean remitidos datos por las entidades españolas a entidades con sede en otros países comunitarios, es importante, para que se defina la ley aplicable, que se identifique cuál es la situación jurídica de la entidad española que procedió a la recogida de los datos, remitiéndolos posteriormente a otro país, dado que sería preciso conocer si la mencionada entidad tiene la naturaleza de responsable del tratamiento, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "*persona física o jurídica, de naturaleza pública o*

privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento", o si, por el contrario, ha de ser considerada mera encargada del tratamiento, es decir, en los términos previstos en el artículo 3 g) de la Ley Orgánica 15/1999, "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*".

Así, si las entidades españolas tuvieran la condición de responsables del tratamiento, la recogida y tratamiento de los datos efectuado por las entidades estaría sometido a lo dispuesto en la Ley Orgánica 15/1999, cumpliéndose con todas sus exigencias (consentimiento informado, información acerca del fichero y destinatarios de la información, resguardo del derecho de acceso, rectificación, cancelación y oposición e identificación del responsable del tratamiento)

Del mismo modo, el envío de los datos a la empresa con sede en el exterior se adapta a lo dispuesto en el artículo 11 de la Ley 15/1999, configurando la transmisión de datos. El apartado 1 de este artículo dispone que:

> *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".*

Si el país destinatario es miembro de la Unión Europea se presume que tiene un nivel adecuado de protección, admitiéndose la transferencia de los datos personales. De lo contrario, no siendo el país miembro de la Unión Europea y no presentando un nivel de protección de datos equiparable al de la LOPD, no se admite el envío internacional de los datos, en los términos del artículo 33 de la referida Ley, salvo las excepciones dispuestas en el artículo 34.

Del mismo modo, tal y como se establece en el artículo 26 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en los artículos 6 y 8 del Real Decreto 1332/1994 que sigue en vigor, se deberá comunicar a la Agencia Española de Protección de Datos las transferencias internacionales que se vayan a realizar, pues en su gran mayoría, necesitan de autorización expresa del Director de la Agencia, con excepción de lo dispuesto en el artículo 34 de la Ley Orgánica 15/1999, según informado anteriormente.

Siendo el responsable por el tratamiento de los datos la empresa con sede en Alemania, por ejemplo, la legislación aplicable es la alemana, tanto en lo referente al cumplimiento de los principios de la misma como en lo atinente a los deberes formales que establezca dicha legislación, sin perjuicio de la obligación de las empresas españolas de aplicar las medidas de seguridad previstas en la legislación española. Del mismo modo, la responsabilidad por la violación de los ficheros de datos estará vinculada a la aplicabilidad de la norma alemana según así la admita o no.

En los términos de la LOPD la nacionalidad de los interesados es indiferente para el supuesto de reconocimiento de la responsabilidad por violación o transferencia irregular de datos personales, pues siendo la empresa española la responsable por el secreto de los datos a consecuencia será la legislación española de aplicación obligatoria, de modo que el afectado que resida o no en España podrá, según su interés, ejercer los derechos reconocidos en la LOPD, con independencia de la nacionalidad que posea.

Por lo tanto, el envío de datos a país no comunitario como Brasil conlleva al análisis por la Agencia Española de Protección de Datos de la naturaleza de los datos, finalidad y duración del tratamiento, las normas de derecho vigentes en Brasil, los contenidos de los informes de la Comisión de la Unión Europea y medidas de seguridad impuestas en dichos países.

Así pues, actualmente Brasil a no atender a las exigencias de protección impuestas para el envío internacional de informaciones, restringe sobremanera el intercambio de informaciones y comercio con los países europeos.

5 - Conclusiones

1 –El ordenamiento jurídico español resguarda el derecho fundamental a la protección de datos y reconoce la responsabilidad de los responsables por ficheros de datos personales o encargados de su tratamiento, por violación de los preceptos de la Ley y en especial por divulgación voluntaria o culpable de ficheros de datos bajo su cuidado.

2 - Se faculta a la Agencia Española de Protección de Datos a velar por el respeto a la legislación de protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición, cancelación de datos y sanción por violación a la LOPD.

2 – La LOPD enumera las infracciones y sanciones aplicables a la divulgación voluntaria o culpable de ficheros de datos, identificando niveles distintos de culpabilidad según la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, y al grado de intencionalidad, entre otros.

3 – El Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio enumera los niveles de protección exigibles a los ficheros que contengan datos de carácter personal.

4 – La ausencia de una normativa específica acerca de la protección de datos en Brasil dificulta sobremanera el libre transito de información y datos en el ámbito internacional, en especial con los países de la Comunidad Europea. Asimismo, es fundamental que Brasil capacite a los órganos públicos brasileños para el ejercicio de las actividades de manutención y tutela de ficheros con las informaciones

5 – Parece fundamental que Brasil establezca una legislación que prime por la identificación concreta de algunos conceptos básicos tales como lo que se comprende por dados personales y sensibles, identificación de los ficheros y el grado de seguridad que deben tener, la identificación de medidas a ser tomadas por los responsables por los datos, los criterios de cuidados, la previsión de un organismo de controle que concentre las informaciones y tenga competencia para imponer las sanciones en caso de violación de los derechos.