Jesús Rubí
Adjunto al director de la Agencia de Protección de Datos

Ana Marzo
Gerente del Equipo Marzo

TODO SOBRE EL NUEVO REGLAMENTO DE LA PROTECCIÓN DE DATOS

SODENA
Sociedad de Desarrollo de Navarra

colegio oficial
ingenieros de telecomunicación

asociación navarra
ingenieros de telecomunicación
anit - navarra

5 de Marzo de 2008, Pamplona

IDEAS para debate

Jornada Divulgación
Nueva Ley Orgánica de Protección de Datos

Intervenciones realizadas en el Salón de Actos de la Confederación de Empresarios de Navarra (CEN)

Gobierno de Navarra

SODENA
Sociedad de Desarrollo de Navarra

colegio oficial
ingenieros de telecomunicación

asociación navarra
ingenieros de telecomunicación
anit - navarra

INTRODUCCIÓN

Les damos la bienvenida en un nuevo encuentro, a través de esta publicación, que nace gracias al empeño de entidades y asociaciones como el Colegio Oficial de Ingenieros de Telecomunicación en Navarra, la Asociación Navarra de Ingenieros de Telecomunicación y SODENA (Sociedad de Desarrollo de Navarra), con el objetivo de poner encima de la mesa las principales directrices que marca el nuevo Reglamento de la Ley de Protección de Datos (LOPD). Una cuestión que está "de moda" en cualquier rincón de cualquier departamento de cualquiera de las organizaciones que trabajan en el tejido industrial y empresarial de la Comunidad Foral.

Es un hecho, según señalaba el secretario general de la Confederación de Empresarios de Navarra (CEN), Javier Martinena, que "prácticamente a diario los ciudadanos estamos proporcionando nuestros datos personales de cualquier naturaleza de una forma expresa o tácita a empresas, a entidades públicas y privadas a través de Internet o de otros medios. Ello conlleva el riesgo del mal uso de los datos por los receptores a través de su manejo o su manipulación de forma no perceptible al usuario y desde luego, sin su consentimiento". Hemos podido comprobar en los últimos años , comentaba el secretario general de la CEN, "cómo el tráfico de datos personales con fines mercantiles o publicitarios se ha convertido en una práctica habitual".

La Ley, según los expertos, nace con un objetivo claro: velar por la utilización de las tecnologías de la información con el fin de salvaguardar el honor e intimidad de las personas. En este sentido, la normativa establece una serie de parámetros que pretenden crear procedimientos y procesos de trabajo para que el nuevo Reglamento se cumpla a rajatabla.

La sesión divulgativa sobre el nuevo Reglamento comenzaba con la presentación, por parte del decano delegado del Colegio Oficial de Ingenieros de Telecomunicación en Navarra, Carlos Fernández Valdivielso, de dos "pesos pesados" en la materia: por un lado, Jesús Rubí, abogado; ha recorrido diferentes puestos de responsabilidad dentro de la Administración estatal como, por ejemplo, fue director del gabinete del ministro de Justicia durante cuatro años, secretario general técnico del Ministerio de Relaciones con las Cortes, director general de Relaciones con las Cortes, vocal del Tribunal de Defensa de la Competencia, adjunto al director de la Agencia de Protección de Datos, subdirector general de Inspección de Datos de la Agencia de Protección de Datos y actualmente adjunto al director de la Agencia Española de Protección de Datos.

Javier Martinena, secretario general de la CEN; Jesús Rubí; Carlos Fernández Valdivielso, decano delegado del Colegio Oficial de Ingenieros de Telecomunicación en Navarra y Ana Marzo.

Ana Marzo, licenciada en Derecho por la Universidad de Valencia en la especialidad de Empresa, abogada y en la actualidad socio del bufete Equipo Marzo Abogados. Está especializada en la asesoría y consultoría en materia de propiedad intelectual, protección de datos y comercio electrónico. Además es coautora de diversos manuales sobre derecho y nuevas tecnologías y protección de datos con las editoriales jurídicas Aranzadi, Lex Nova, Ediciones Experiencia, Civitas y Dijusa. También ha sido profesora en distintos cursos y seminarios y master sobre derecho y nuevas tecnologías y ex miembro de la Asociación para el Fomento del Comercio Electrónico Empresarial.

Con el objetivo de completar la exposición de estas dos personalidades, la organización quiso incorporar a la mesa a dos personas, cumpliendo el binomio de representantes jurídicos y expertos en sistemas de información. Dos personas de empresas de Navarra para que, además de la información y prospectiva que puedan dar Jesús Rubí y Ana Marzo, podamos tener la visión global de lo que se hace en Navarra.

Por un lado, participó Óscar Rived, de Larraby, empresa especializada en seguridad informática; y por otro, Álvaro Abáigar, de ARPA Abogados, responsable de nuevas tecnologías.

JESÚS RUBÍ:“ ASPECTOS RELEVANTES DEL REGLAMENTO DE LA LOPD. CONSECUENCIAS PRÁCTICAS Y ACLARACIONES”

Voy a hacer una presentación del Reglamento de la Ley Orgánica de Protección de Datos y lógicamente, como el tiempo es limitado, voy a tratar de destacar los aspectos que me parecen más relevantes por sus consecuencias prácticas y por las aclaraciones que introducen en la medida en que, aunque sea un decreto que ha aprobado el Gobierno, hemos colaborado con el Ministerio de Justicia en la elaboración de esta norma y sobre todo, para trasladarle cuáles eran problemas importantes que se nos estaban planteando.

El Reglamento de la Ley de Protección de Datos tiene un objetivo y este es tratar de conseguir mayor seguridad jurídica. En muy buena medida el Reglamento lo que hace es consolidar los precedentes de resoluciones de la Agencia Española de Protección de Datos, de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional (que es el órgano que revisa esas resoluciones) objetivándolos para que se puedan conocer con mayor facilidad. Ese es el primer objetivo del Reglamento.

El Reglamento también trata de dar respuesta a una serie de dudas que se le plantearon a la Comisión Europea en el momento en que se aprobó la Ley Orgánica de Protección de Datos sobre cómo se había incorporado a nuestro sistema legal la Directiva Comunitaria de Protección de Datos.

En tercer lugar el Reglamento recoge una serie de aspectos de política legislativa que son decisiones del Gobierno, por ejemplo, el haber hecho una regulación específica del consentimiento de los menores, el haber reforzado las garantías para las personas antes de su posible inclusión en ficheros de información sobre solvencia patrimonial y crédito o el haber impulsado las llamadas listas “Robinson” para que quien no quiera recibir publicidad se pueda inscribir en una lista de esta naturaleza y no la reciba .

Y en cuarto lugar, hay algunos aspectos en los cuales la ley estaba pendiente de un desarrollo reglamentario porque la normativa introdujo novedades que las normas anteriores no habían contemplado. Esto afecta fundamentalmente al hecho de que la ley del año 1999 se aplica también a tratamientos de datos en soportes no automatizados, fundamentalmente en soporte papel, y estaba pendiente el aclarar una serie de extremos sobre estos ficheros no automatizados, insisto, fundamentalmente en papel, y en particular sobre las medidas de seguridad que debían implantarse para estos ficheros.

Yo voy a tratar una selección de los temas que me han parecido más relevantes. Probablemente, omitiré cuestiones que a algunos de ustedes les interese, pero como luego vamos a tener la posibilidad de hacer un coloquio o de atender sus preguntas sobre lo que no trate, estoy a su disposición.

El primer aspecto que destaca en este Reglamento, y es el que se refiere al ámbito de aplicación de la Ley. Ni el Reglamento, ni la Ley por tanto, se aplicará a los datos de personas físicas que sean personas de contacto de otro tipo de organizaciones (personas jurídicas). No será aplicable a los ficheros que se limiten a incorporar datos de personas físicas que presten sus servicios en personas jurídicas siempre que estos datos sean únicamente el nombre y los apellidos, las funciones o puestos desempeñados o la dirección postal o telefónica, el teléfono y el número de fax. De esta manera el Reglamento viene a dar mayor seguridad porque ha habido una zona siempre imprecisa a la hora de considerar si estos datos de estas personas, que son simplemente un elemento de contacto con otra organización eran personas protegidas o sujetas a este régimen de garantías o no lo eran. El Reglamento aclara que no, que cuando se utilicen exclusivamente estos datos de esas personas y se utilicen lógicamente para una comunicación dentro del entorno de activida-

des o para alguna finalidad que sea la propia de la actividad de esa organización, de esa empresa o de esa persona jurídica, el tratamiento de esos datos personales está al margen de la normativa de protección de datos.

Esto ha llevado en algunos de los foros en los que yo he participado a una reacción o una pregunta inmediata que es: "a partir de ahora, en los ficheros de proveedores, por ejemplo, que responden básicamente a estas características ya hay que solicitar la baja en el Registro General de Protección de Datos o ya no hay que notificarlos". Efectivamente, si esos ficheros son los que recogen exclusivamente esta información y se utilizan exclusivamente para esta finalidad, esto es así. El problema es que la experiencia acredita que normalmente las cosas no suelen ser tan nítidas sino que normalmente en estos ficheros hay algunos datos más que no son los que están excluidos específicamente o se acaba utilizando esta información no sólo para una comunicación relacionada con la actividad de las empresas, sino para otras finalidades adicionales o complementarias o que afectan directamente a esos individuos que son personas de contacto. Y en la medida en que eso sea así, es prudente seguir notificando y seguir manteniendo este tipo de ficheros. Pero si alguien desarrolla una actividad de una manera tan rigurosa que efectivamente está perfilado el fichero de forma y manera que sólo se utilizan estos datos para estas finalidades, serían ficheros excluidos.

El nuevo Reglamento tiene como primer objetivo conseguir una mayor seguridad jurídica, consolidando los precedentes de la Agencia Española de Protección de Datos y de la Sala de lo Contencioso Administrativo de la Audiencia Nacional.

Y también en este mismo artículo, se aclara otro de los debates tradicionales que es en qué medida la normativa de protección de datos es de aplicación a personas físicas, que están realizando una actividad empresarial, fundamentalmente los autónomos. Recogiendo algunos precedentes de resoluciones de la Agencia, el Reglamento excluye de su ámbito de aplicación a los empresarios individuales cuando actúen en calidad de comerciantes, industriales o navieros, es decir, cuando nítidamente quede claro que el tratamiento de sus datos personales está vinculado al ejercicio de su actividad empresarial. A veces el tratamiento de este tipo de información es complejo y en caso de duda, conviene ser prudente porque a veces una persona ejerce una actividad como autónomo, pero la realiza en su domicilio. Entonces, se confunde el dato de domicilio como empresario y como persona física y puede generar con-

fusiones o producir riesgos al entender que esta excepción es aplicable a esas personas con carácter universal. Esto no es así, ya que sólo es aplicable cuando concurran estas circunstancias específicas de que desarrollen su actividad como comerciantes, navieros o industriales.

También, aunque no lo diga, del Reglamento se desprende que hay una frontera de determinados colectivos cuyos datos sí están sujetos plenamente al régimen de garantías de la Ley de Protección de Datos, que son los profesionales que ejerzan su profesión de manera privada, es decir no organizados en forma de empresa como los ingenieros de Telecomunicaciones o cualquier otro tipo de actividad profesional o los datos de esos profesionales inclusive en el ejercicio de su actividad profesional. En la medida en que no están organizados como empresa o que no sean empresarios, sí están dentro de este sistema de garantías. Esto se pone de manifiesto porque en el Reglamento hay artículos que se refieren las fuentes accesibles al público, una de cuyas manifestaciones más directas son los listados de profesionales que pertenecen a un colegio profesional. Estos listados de profesionales, cuando se han publicado, se entiende que es una fuente accesible al público y por tanto se desprende que se pueden utilizar los datos sin consentimiento de las personas, pero lo que se deduce "a sensu contrario" de esa regulación específica, es que están plenamente sometidos al ámbito de aplicación de la normativa de protección de datos y no excluidos.

Ni el Reglamento, ni la ley se aplican a los datos de las personas físicas que sean contacto de otro tipo de organizaciones, es decir, personas jurídicas; siempre que estos datos sean el nombre, apellidos, puestos desempeñados, teléfono o dirección postal.

También en lo que se refiere al ámbito de aplicación de la Ley, el Reglamento ha venido a aclarar un concepto que en principio parecía muy nítido pero que ha dado problemas en la práctica. La Ley de Protección de Datos excluye de su ámbito de aplicación el tratamiento de datos personales o domésticos pero no está claro hasta dónde llega ese tratamiento. Hemos tenido algunos casos fronterizos, por ejemplo el de una persona que se dedicaba profesionalmente a una actividad de relaciones públicas, que utilizó datos de una agenda electrónica para invitar a personajes conocidos o populares a la inauguración de un establecimiento de ocio. Una de esas personas presentó una reclamación, se hizo una investigación y se abrió un procedimiento por infracción de la ley. Su ale-

gato como imputado era : “ustedes no me pueden aplicar esta norma porque este es un tratamiento de datos personales o domésticos porque es mi agenda personal lo que he utilizado”. En esa resolución se decía que: “efectivamente, la agenda privada estaría excluida del ámbito de aplicación de la ley pero cuando el uso de esa información se hace con un fin o en el marco de una actividad profesional, ya excede de lo estrictamente privado y, por tanto, el tratamiento de los datos de esas personas estaría sujeto al sistema de garantías de la normativa de protección de datos.

El artículo 4 del Reglamento trata de aclarar que sólo se considerarán excluidos los tratamientos relativos a actividades que se inscriban en el marco de la vida privada o familiar de los particulares. Una misma información en un mismo soporte tecnológico, si se utiliza en el ámbito de la vida privada o familiar estaría excluido, si se utiliza con fines profesionales, pasaría la frontera y estaría incluido dentro del ámbito de aplicación de la Ley.

El nuevo Reglamento excluye de su aplicación a los empresarios cuando nítidamente quede claro que el tratamiento de sus datos personales está vinculado al ejercicio profesional”.

Los listados de profesionales publicados permiten utilizar los datos de los miembros, por ejemplo, de un colegio profesional, sin consentimiento de las personas.

Dentro de las definiciones del Reglamento, que son muy numerosas, querría destacar algunas. La primera es la que se refiere a la definición de los datos de carácter personal relacionados con la salud. De la información de salud , como datos protegidos, se habla en la Constitución, en los convenios internacionales, en la normativa sectorial y en la ley de protección de datos pero cuando hemos tratado de obtener una definición, un concepto de qué son datos de salud, hemos tenido dificultades en la práctica, en particular cuando se trata de situaciones fronterizas. El caso específico que nos encontramos fue el de si los datos relativos a un porcentaje de discapacidad o de minusvalía de una persona se debe considerar por sí mismo un dato de salud y, por tanto, especialmente protegido, o no, y se alegaba en un caso concreto que tuvimos que no tiene por qué ser un dato de salud porque una persona discapacitada puede gozar de buena o de mala salud. En aquella resolución, tomando como antecedentes la Carta de la Organización Mundial de la Salud, el Convenio 108 del Consejo de Europa que ha sido suscrito por España y que forma parte de nuestro derecho interno y también sentencias del Tribunal de Justicia de las Comunidades Europeas, en particular una muy importante, que es el "caso Lindqvist". Se afirmó que el concepto de datos de salud como especialmente protegido o sensible es un concepto amplio y que estas categorías de información sobre un porcentaje de discapacidad o minusvalía o la información sobre datos genéticos son "per se" datos de salud y tienen ese sistema reforzado de protección. El Reglamento ha venido a aclarar específicamente estos casos y a poner de manifiesto este concepto expansivo de datos de salud.

También, aunque no haya una definición específica en el Reglamento pero puede tener importancia en algunos casos y desde luego ha habido muchas dudas en la práctica, aparece una figura que no está en la Ley, que son los entes sin personalidad jurídica diferenciada. El Reglamento aclara, a lo largo de sus definiciones, que dichos entes pueden tener la posición jurídica de responsable del tratamiento, encargado, cesionario, etc.

Por ejemplo, las comunidades de propietarios son entes sin personalidad jurídica pero tratan los datos de los comuneros y de todos los aspectos relacionados con lo que les reconoce la Ley de Propiedad Horizontal. O, por ejemplo, una junta de personal es un ente sin personali-

dad jurídica y desde luego en el ejercicio de la libertad sindical las posibilidades que tiene de acceso a información de los trabajadores es extraordinariamente amplia. O las comisiones de control de entidades gestoras de planes de pensiones son entes sin personalidad jurídica, pero por esas funciones de control tienen reconocidas unas posibilidades de uso de información personal muy relevantes. Pues bien, el Reglamento lo que viene a aclarar de una manera indirecta es que esos entes sin personalidad jurídica, cuando utilicen la información en los términos en que estén habilitados normativamente, por relaciones de todo tipo o por el consentimiento de las personas, también pueden ser responsables del tratamiento de esa información y pueden incurrir en una infracción en el caso de que incumplan la ley.

Otra definición importante en la normativa es la definición de fichero no automatizado. Esta no está en la Ley Orgánica de Protección de Datos y tiene su justificación el que se haya recogido en el Reglamento precisamente porque la Ley de Protección de Datos amplió el ámbito de aplicación de la originariamente conocida como LORTAD a los tratamientos no automatizados. ¿Por qué? Porque en la normativa europea, de la cual trae causa la Ley Orgánica de Protección de Datos, se dice que se aplicará a los datos que consten en ficheros en otros soportes, básicamente en soporte papel, pero también se dice que sólo se aplicará a los datos en soporte papel cuando tengan un cierto grado de estructuración y de organización. La directiva europea dice: “no se aplicará a las carpetas no estructuradas”. Y esto, ¿qué significa? Que a la información en soporte papel sólo le será de aplicación este régimen de garantías cuando esté estructurada con criterios de búsqueda que permitan con cierta facilidad identificar los datos de personas físicas y, si la información en papel no está estructurada, no constituye un fichero y entonces no se aplica esta normativa.

La agenda privada estaría excluida del ámbito de la aplicación de la ley, excepto cuando el uso de esa información se hace en el marco de una actividad profesional”.

Por eso, ha sido útil y práctico que el Reglamento haya incluido una definición de fichero no automatizado. Expongo un caso que tuvimos en la Agencia: Una sala de gobierno de un Tribunal Superior de Justicia de una Comunidad Autónoma quiso crear un fichero con determinados datos de los funcionarios de la Administración de Justicia y no aprobó una disposición previa de carácter general que creara ese fichero. Hubo una reclamación de los

sindicatos que derivó en una inspección y cuando los inspectores accedieron a la información había en un gran almacén , apiladas un montón de cajas, información de funcionarios que no estaba estructurada de ninguna manera. Evidentemente, se podía acabar encontrando la información de cada funcionario, sacando papel a papel, caja a caja. Y se archivaron las actuaciones porque esa información no estaba estructurada. A lo mejor, si hubiéramos hecho una inspección dos semanas después, la información habría salido de las cajas, habría un orden alfabético o por el criterio que fuera que permitía fácilmente identificar a esas personas. Habría pasado la frontera y estaría incluido dentro del ámbito de aplicación de la Ley.

También hay otra definición que afecta al ámbito de aplicación de la Ley que es el de "persona identificable", porque la Ley de Protección de Datos se aplica a datos de personas físicas identificadas o de personas físicas identificables. No hace falta que la identificación se produzca materialmente, basta con que potencialmente sea posible identificar a esas personas. Pero ¿cuándo es una persona identificable? El Reglamento viene a aclarar que una persona será identificable cuando la asociación de la información de que se disponga respecto de un individuo concreto se pueda realizar sin esfuerzos desproporcionados y añade dos parámetros para poder analizar si hay un esfuerzo desproporcionado o no. El primero, los plazos: si el periodo de tiempo para conseguir esa vinculación entre la información y la persona es muy extenso , entonces estaríamos más bien en presencia de una persona no identificable. Y otro, las actividades que haya que desarrollar. Si las actividades para conseguir esa asociación son muy complejas podría ser un esfuerzo desproporcionado y no serían datos de una persona identificable.

Hay un aspecto importante también en el Reglamento que es el artículo 6, que se refiere al cómputo de plazos. Este artículo viene a establecer la regla general de que todos los plazos del Reglamento fijados en días se computarán como días hábiles y viene a restablecer una situación de desequilibrio que hay en este momento entre los responsables de ficheros de titularidad pública y privada. Porque para el ejercicio de los derechos de acceso, de rectificación, de cancelación y de oposición hay unos plazos; y estos, hasta la llegada del

Los datos de salud, especialmente sensibles o protegidos, es un concepto amplio que incluye, por ejemplo, cuestiones relacionadas con la discapacidad o minusvalía de la persona".

Reglamento, cuando afectaban a ficheros de titularidad pública se computaban en días hábiles, con lo cual siempre había algún día más de plazo. Y cuando eran responsables de titularidad privada, se computaban conforme a las reglas del Código Civil por días naturales, y había un desequilibrio entre una y otra situación. El Reglamento viene a aclarar que se computarán siempre por días hábiles cualquiera que sea el responsable del fichero, aspecto que incide fundamentalmente en el ejercicio de los derechos.

Entrando en los principios de la Ley de Protección de Datos y dentro de ella en el principio de calidad de datos, hay un punto en el artículo 8.6, en el párrafo segundo de este artículo que, en mi opinión, es una aclaración que tiene una gran trascendencia práctica porque este artículo se refiere a la calidad de datos, por tanto a que los datos tienen que ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que se recabaron. Pero claro, la regla general en la Ley de Protección de Datos es que cuando hay que proceder a la cancelación de los datos, éstos se tienen que bloquear, lo que significa que sólo se pueden utilizar para atender responsabilidades administrativas o jurisdiccionales relacionadas con el tratamiento de la información. ¿Y qué pasa si uno ha terminado una relación jurídica con una entidad financiera y al día siguiente ha ejercido el derecho de cancelación y tiene alguna reclamación pendiente? ¿Qué ocurre? ¿No cabe utilizar esa información para enviarle una carta, para tratar de llegar a una transacción extrajudicial?. El concepto de bloqueo es muy estricto y dice “exclusivamente responsabilidades administrativas o jurisdiccionales”. Este párrafo segundo viene a aclarar que cabe una situación intermedia más flexible porque dice que aunque deban cancelarse “podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado”, es decir, que aunque se haya terminado esa relación jurídica, aunque procedería en principio a la cancelación de los datos, si queda alguna reclamación, algún aspecto derivado de esa relación jurídica pendiente, este artículo aclara que sigue existiendo una legitimación para tratar los datos para esa

Las comunidades vecinales, cuando utilizan la información de los propietarios, deben ser responsables del tratamiento de esos datos y pueden incurrir en una infracción en el caso de que se incumpla la ley” .

La LOPD se aplicará a los datos que consten en soporte papel que tengan un cierto grado de estructuración y de organización".

finalidad y poder utilizarlos para ponerse en contacto con un posible deudor y llegar a una transacción, etcétera. Y sólo cuando esa situación haya culminado es cuando procederá el bloqueo de la información.

Hay otro artículo (a. 10), que también tiene importancia. Parece que éste trata de sistematizar y de presentar pedagógicamente todos los supuestos que legitiman o que habilitan el tratamiento de información personal, pero el artículo tiene una finalidad que va más allá, y trata de dar respuesta a una duda que planteó la Comisión Europea sobre la ley española. La duda se refiere a una legitimación para tratar los datos que es el interés legítimo del responsable del fichero". Este artículo trata de aclarar cómo se ha traducido en nuestro sistema legal ese interés legítimo. El interés legítimo, además del poder utilizar los datos o la información que está en fuentes accesibles al público, inicialmente sin consentimiento, tiene dos canales fundamentalmente: uno, que la Ley de Protección de Datos española habilita el tratamiento de los datos y todos los tratamientos que sean necesarios para llevar a buen término cualquier tipo de relación jurídica, no sólo una relación contractual, cualquier tipo de relación negocial, inclusive precontractual, mientras que la Directiva Europea sólo lo legitima en base a ese fundamento cuando hay un contrato. Por tanto, hay un reconocimiento de que puede haber un tratamiento de datos basado en el interés legítimo que no sea sólo en los contratos sino en otro tipo de relaciones negociales.

En segundo lugar, este artículo aclara que siempre que una norma prevea , contemple o tenga por objeto el reconocimiento de un interés legítimo o el establecimiento de una obligación implícita en la norma, esa previsión legal habilitará el tratamiento de la información. Es decir, que aunque no haya una cláusula concreta, específica, rotunda sobre que "para este tratamiento los datos se podrán tratar sin el consentimiento de las personas" siempre que en la regulación el legislador haya reconocido intereses legítimos de alguien o le haya impuesto obligaciones que impliquen el tratamiento de los datos personales, hay que entender que existe una habilitación legal.

En algún foro en el que he estado recientemente hablando del Reglamento, alguien me preguntaba: "entonces, si una norma a una determinada empresa que a partir de un deter-

Una persona será identificable en una base de datos cuando el conjunto de información que se dispone del individuo se puede encontrar sin esfuerzos y en un plazo de tiempo determinado".

minado número de trabajadores tiene la obligación de reservar un cupo para discapacitados y contratarlos, ¿eso sería una obligación legal que estaría legitimada por esta aclaración que hace el Reglamento?". En mi opinión, sí responde a ese tipo de situaciones. La norma trata de conseguir un efecto y si eso implica el tratamiento de datos personales, reconoce un interés legítimo en la norma o impone una obligación, debe entenderse que es legítimo.

En relación con el consentimiento, el Reglamento ha introducido algunas novedades relevantes: la primera, es una regulación específica de los menores de edad. Esta regulación, en síntesis, lo que viene a señalar es, desde el punto de vista de la normativa de protección de datos, la regla general para considerar a una persona mayor o menor de edad son los 14 años y se reconoce que, a partir de esta edad, las personas pueden prestar por sí mismos el consentimiento sin necesidad de la concurrencia de sus padres o sus representantes legales, en general. Por debajo de los 14 años son menores.

Además de eso, introduce un elemento informativo y dice que la información que se facilite a los menores, cuando se trata de recabar su consentimiento o de que se obtenga de los padres, tiene que ser una información en un lenguaje claro, preciso, que le sea comprensible. Viene además este artículo a salir al paso de una práctica que cada vez se está haciendo más frecuente que es la de obtener de los menores datos de los mayores, de sus padres o de otros miembros del entorno familiar, y este artículo del Reglamento aclara que esa es una práctica ilícita y que la única solicitud de datos que se puede hacer a los menores sobre sus padres es exclusivamente aquella que permite identificarlos y dirigirse a los progenitores para tratar de obtener su consentimiento o utilizar los datos de los menores.

Y, finalmente, el Reglamento señala que al responsable del fichero de tratamiento le corresponderá articular los procedimientos que garanticen que se ha comprobado de un modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso por los padres, tutores o representantes legales. Esta es una cláusula general que no se ha podido precisar más porque los entornos y los canales a través de los cuales se puede tratar de obtener información de menores son extraordina-

riamente variados y habrá que ir a las especifidades de cada empresa, de los servicios, de los productos que se ofrecen a los menores para tratar de buscar algunos elementos que permitan discriminar y tratar de acreditar que efectivamente se ha intentado que el menor no dé el consentimiento por su cuenta.

Hay también un artículo importante que se refiere a la forma de recabar el consentimiento. Este artículo sobre la forma de recabar el consentimiento viene a introducir unos elementos de prueba que permitan como regla general, que tendrá excepciones luego en casos concretos, acreditar que se ha obtenido ese consentimiento y para eso se prevé la posibilidad de que se dirija una comunicación a las personas cuyo consentimiento se quiere obtener para una determinada finalidad, informando de todos los extremos necesarios (el responsable del fichero, la finalidad, la dirección para el ejercicio de los derechos, etcétera). Transcurridos treinta días desde que se recibió esa comunicación, más un periodo prudencial de lo que pueda retrasarse el correo si es que se utiliza el postal, y si no hay una negativa, se puede entender que se ha obtenido el consentimiento.

En relación con esta comunicación para obtener el consentimiento, el propio Reglamento en este artículo introduce tres elementos que tratan de facilitar la prueba: uno, que cuando hay una relación periódica con la clientela a través de facturación periódica, en compañías de suministro energético o de tipo de servicios, o entidades financieras que mandan habitualmente el extracto (los saldos, los movimientos de las cuentas corrientes), si se acompaña con esa factura o con esa información, hay un elemento probatorio adicional. En todo caso, se exige que haya dos elementos que permitan comprobar o acreditar que esa comunicación se emitió y llegó a su destinatario. El primero es que haya un sistema razonablemente auditable de emisión de esas comunicaciones y el segundo es que haya un sistema auditable del control de devoluciones. Las devoluciones que haya habido, suponen que no se ha recibido esa comunicación y, por tanto, que no se ha obtenido ese consentimiento. Este precepto introduce una cautela adicional: a base de mandar comunicaciones continuadas acaba venciendo la resistencia de cualquier persona, porque en un momento determinado alguien dirá “no res-

El Reglamento aclara que se computarán los plazos siempre por días hábiles, independientemente de si el responsable del fichero es público o privado”.

pondo, no digo nada" y ya se puede entender que han obtenido su consentimiento. Para tratar de atajar este tipo de situaciones se incluye una cláusula específica que dice que una vez que se haya solicitado el consentimiento de esta manera para una determinada finalidad por un determinado responsable, no se podrá volver a reiterar esta solicitud hasta que haya transcurrido un periodo de un año.

Los datos personales podrán conservarse durante el tiempo que pueda exigirse algún tipo de responsabilidad jurídica o derivada de la ejecución de un contrato".

También, sobre este artículo, he encontrado algunas preguntas que me han creado una cierta alarma por la interpretación que se puede hacer, por ejemplo: "pues ahora ya se puede utilizar los datos de cualquiera, se le manda una comunicación y si no contesta he obtenido su consentimiento y ya está, y se puede tratar la información". No, este artículo no trata de eso. Para hacer esta comunicación hay que tener previamente una legitimación conforme a las reglas generales de la Ley de Protección de Datos. Entonces, habrá que haber obtenido la información de una fuente accesible al público, habrá que tener una relación contractual o habrá que tener un consentimiento de las personas. Teniendo esa habilitación previa, por ejemplo, en el marco de una relación contractual, se podrá hacer una comunicación adicional diciendo: "y ahora quiero obtener un consentimiento para otra cosa distinta, que no tiene que ver con la relación contractual, para hacer publicidad de productos de terceros o para lo que se quiera", pero tiene que operar previamente un fundamento legal que legitime el tratamiento de la información. Este artículo no borra de raíz, porque no podría hacerlo, menos en una norma de rango reglamentario, estos requisitos previos de legitimación para el tratamiento de los datos.

En relación también con el consentimiento, el Reglamento sale al paso de una práctica que se ha generalizado, que es en contratos de adhesión extensos y masivos, incluir una cláusula que diga: "ya que hay que obtener el consentimiento, se incluye aquí que usted me autoriza a tratar los datos para otros fines, normalmente de promoción comercial; y además añado que ésta es una cláusula que forma parte del contenido esencial de este contrato". El que sea parte del contenido esencial del contrato, el que sea una cláusula fraudulenta o desleal, es algo que atenderá la jurisdicción civil y las consecuencias de su incumplimiento en su caso. Desde el punto de vista de la protección de datos, el Reglamento lo que viene a aclarar es

Asistentes a la Jornada organizada por la Asociación Navarra de Ingenieros de Telecomunicación

que en estas situaciones, cuando se quiere pedir un consentimiento para algo distinto que no tiene que ver con el objeto específico de un contrato, hay que poner esa solicitud separada de forma que se distinga con claridad, y hay que ofrecer una fórmula para que se pueda manifestar la negativa de la persona que no quiere prestar ese consentimiento.

A diferencia de la Directiva Europea, la ley española reconoce que puede haber un tratamiento de datos basado en el interés legítimo en contratos y otras relaciones de negocio".

En relación con el deber de información hay una novedad importante. Está incluida en este artículo con una sistemática dudosa, porque su contenido material, más que con la información, tiene que ver con otra cosa. En los artículos que se refieren al deber de información, en particular en el artículo 19, se aclara algo que

también ha planteado muchas dudas: cuando haya una fusión, escisión, cesión global de activos y pasivos o cualquier otra operación de reestructuración societaria de naturaleza análoga, no será necesario obtener de nuevo el consentimiento de las personas que eran clientes de la anterior empresa que ahora, por ejemplo, se ha fusionado. Bastará con facilitarles información sobre el cambio que se ha producido, los datos del nuevo responsable, su dirección, etcétera, pero no hace falta el consentimiento para este tipo de operaciones societarias. Y como el único requisito que se exige es el de información, por eso sistemáticamente está incluida en relación con el deber de información.

Uno de los aspectos más relevantes, que, a mi juicio, tiene mayores consecuencias prácticas o que va a tener y que da mayor flexibilidad del Reglamento de la Ley de Protección de Datos es el que se refiere al encargado del tratamiento, al prestador de servicios. La externalización de servicios se ha convertido en una práctica generalizada y habitual por parte de las administraciones públicas, y sobre todo de las empresas privadas. La dicción literal de la Ley de Protección de Datos puede parecer excesivamente rígida en algunos aspectos relacionados con esta prestación de servicios. El Reglamento viene a aclarar que las prestaciones de servicio pueden ser temporales o indefinidas y que estarán sujetas a este régimen de garantías tanto si son gratuitas como si son onerosas.

La regla general considera a una persona mayor de edad a los 14 años; a partir de ésta, el individuo puede dar su consentimiento sin necesidad de la concurrencia de sus padres o representantes legales".

Además viene a aclarar otro aspecto importante que se refiere a situaciones en las cuales lo que se pretende es simplemente cambiar el primer prestador de servicios por uno nuevo. Una prestación de servicios característica es la gestión de recursos humanos por un gestor administrativo que la lleva a pequeñas y medianas empresas y se puede querer cambiar de gestor administrativo. Para eso, el Reglamento, de una manera flexible, no exige necesariamente que se devuelvan los datos a quien encargó esa prestación y, a continuación, se vuelvan a facilitar al nuevo prestador de servicios, sino que tiene una expresión, que dice en el artículo 20.3 que "el encargado del tratamiento no incurrirá en responsabilidad cuando previa indicación del responsable comunique los datos a un tercero designado por aquel, al que hubiera encomendado la prestación de un servicio conforme

a lo previsto en el presente capítulo". Con esta fórmula alambicada de exención de responsabilidad, lo que se viene a aclarar es que por indicación del responsable cabe que al término de una prestación de servicios la información pase del anterior prestador al nuevo, si bien también ese nuevo contrato tendrá que tener todas estas garantías que para las prestaciones de servicios exige el artículo 12 de la Ley y desarrolla el Reglamento.

Un segundo aspecto donde la Ley y la interpretación de la Agencia en origen ha sido muy rígida fue respecto a la posibilidad de subcontratar posteriormente parte de esas prestaciones de servicios. Al principio, en la aplicación práctica de la Ley del año 99 sólo se admitía esta posibilidad si el que contrataba con el subcontratista actuaba en nombre y por cuenta de quien le encargó la prestación del servicio y se convertía en su representante. Esa fórmula se apreció enseguida que era excesivamente rígida y ha habido algunos precedentes que la han ido flexibilizando. El Reglamento aclara que se puede subcontratar. Si se conocía que se iba a subcontratar en el momento de celebrar el contrato principal, basta con determinar los servicios que se van a subcontratar, identificar la empresa que va a intervenir en la subcontratación y que toda la cadena de intervinientes esté en el marco de estos documentos contractuales que recogen las garantías del artículo 12 de la Ley. Si no se conoció en ese momento que había una necesidad de subcontratar algo y se aprecia con posterioridad, hay que ponerlo en conocimiento del responsable que encargó esa primera prestación porque a fin de cuentas es el que va a responder o puede responder del tratamiento de la información personal: se identifican los servicios, se identifica la empresa, se celebran unos contratos con estas garantías y se permite que haya subcontratación.

El encargado del fichero de datos es el responsable de articular los procedimientos necesarios para comprobar la mayoría de edad de la persona y la autenticidad del consentimiento en cada caso".

Y el Reglamento también viene a dar solución a una situación que afecta, en mi opinión, al propio derecho a la tutela judicial efectiva, como es el que ha prestado un servicio que supone el tratamiento de datos personales, por ejemplo, un gestor administrativo, y tiene que devolver o destruir la información. Si tiene posteriormente una reclamación sobre cómo hizo las nóminas, las altas, las bajas, las retenciones tributarias...., ¿se queda sin información y no se

puede defender? Esto sería disparatado. Entonces como en la Ley de Protección de Datos hay otro concepto que es el concepto del bloqueo, el Reglamento aclara que alguien que fue prestador de servicios puede y debe conservar esa información bloqueada para poder atender a responsabilidades administrativas o jurisdiccionales vinculadas al tratamiento de datos que él hizo mientras ejecutó ese contrato y mientras prestó esos servicios.

Respecto de los derechos, el Reglamento viene de alguna manera a recoger de una manera sintética previsiones que estaban en la Ley o en las vigentes normas de desarrollo de la LORTAD y en instrucciones del director de la Agencia. Quizá, los aspectos más relevantes de esta regulación sean, primero, que se contempla una especie de trámite de subsanación. Si alguien es responsable de un fichero y una persona ejercita cualquiera de los derechos respecto de él y hay un defecto formal, por ejemplo la identificación adecuada de esa persona o que no hay garantías de que esa persona es efectivamente el titular de ese derecho personalísimo, si no se dijera nada se podría denegar; esta persona acudiría a la Agencia, y en un procedimiento administrativo de seis meses, se le diría: "mire, lo que pasó es que había un defecto formal, que usted no acompañó el documento de identidad", y vuelta a empezar de nuevo en el ejercicio de ese derecho.

Cuando hay estos defectos subsanables se impone a los responsables ante los que se ejercitan los derechos que lo pongan de manifiesto directamente a la persona para facilitar ese ejercicio. También, se ha previsto qué pasa cuando los derechos a ejercer ante un prestador de servicios. Esto es frecuente, por ejemplo, en las empresas de recobro que son las que directamente se dirigen a una persona con sus propios anagramas comerciales a decir: "usted debe esta cantidad, póngase en contacto conmigo, ingrese en esta cuenta, etcétera". La persona reacciona y dice: "yo no le conozco de nada, usted no tiene ninguna legitimación para tratar mis datos y ejerzo el derecho de cancelación". Normalmente, hay una prestación de servicios por parte del acreedor principal y la empresa de recobro y el Reglamento aclara que, o bien esa prestación de servicios incluye la tramitación de esas solicitudes, o bien que ese prestador de servicios tiene que ser diligente y transmitir rápi-

Una vez que se haya solicitado dicho consentimiento con una determinada finalidad, no se podrá volver a reiterar esa solicitud hasta que haya transcurrido un año".

Cuando se quiere pedir un consentimiento para algo distinto que no tiene que ver con el objeto del contrato, el Reglamento determina que debe formularse por separado y con claridad".

damente esa solicitud al responsable para que la atienda o la deniegue motivadamente. El cómputo de los plazos, en días hábiles, ya lo hemos comentado.

Hay una novedad importante que trata de facilitar el ejercicio de los derechos porque, aunque éste está adornado de unos ciertos elementos formales que tratan de identificar unívocamente a la persona que lo ejerce (porque son derechos personalísimos), también se ha apreciado que en muchas ocasiones las distintas organizaciones públicas o privadas tienen fórmulas más flexibles que consiguen una identificación unívoca de sus clientes de una manera más sencilla. Y por eso, el Reglamento ha venido a introducir una aclaración en el sentido de señalar que cuando cualquier responsable de un tratamiento de datos dispone de servicios de atención al público o de servicios de reclamaciones a los clientes , los mismos procedimientos de identificación de sus clientes para ampliar sus servicios o para presentar una reclamación podrán ser utilizados para identificar a las personas que ejerzan los derechos de la Ley de Protección de Datos; de forma y manera que estos canales, servicios de atención al público, y servicios de reclamaciones, pasan a ser un canal más flexible para que las personas puedan ejercitar esos derechos.

En cuanto al contenido material de los derechos, quizá lo más relevante de todo el Reglamento sea el que se aclara en qué consiste este derecho que está en la Ley y es el de oposición. El derecho de oposición tiene un nombre muy rotundo pero es un derecho impreciso en la Ley de Protección de Datos. El Reglamento viene a aclarar que el derecho de oposición se produce en tres situaciones: la más habitual, cuando los datos se obtienen de fuentes accesibles al público y se utilizan para hacer publicidad (una persona recibe una comunicación publicitaria y a partir de ese momento no quiere recibir más y, por tanto, se opone y ejercita el derecho de oposición y ya no recibirá o no debe recibir más comunicaciones publicitarias). En el artículo 6.4 de la Ley hay una situación excepcional, que dice que, aunque sea legítimo el tratamiento de los datos, si concurren determinadas circunstancias particulares de una persona que haya que atender, y salvo que una ley no lo impida, se podrá oponer al tratamiento de la información. Y después hay una tercera modalidad del derecho de oposición que se refiere a algo que en la Ley se llama la impugnación de valoraciones,

es decir, la posibilidad de que con una herramienta informática se adopte una decisión sin intervención humana que pueda tener efectos jurídicos sobre una persona: por ejemplo, la corrección de un test psicológico en una prueba de selección de personal, sin ir más lejos, o el scoring en el ámbito financiero. El Reglamento viene a aclarar que esos derechos que se reconocen de impedir que esa decisión automatizada pueda ser utilizada como prueba en contra de uno es también una manifestación del derecho de oposición y se aplicará todo el régimen de plazos, etcétera, es decir, el resto de elementos comunes a ese derecho de oposición que desarrolla el Reglamento.

No será necesario obtener de nuevo el consentimiento de cada persona cuando se produzca una fusión, escisión, cesión global de activos o pasivos o cualquier otra operación de reestructuración de una empresa".

Voy a terminar brevemente mencionando algunos aspectos destacables de la nueva regulación de medidas de seguridad. La primera novedad del Reglamento en materia de seguridad es que hay medidas de seguridad para ficheros no automatizados pero también hay algunas novedades respecto de los ficheros automatizados. En relación con estos últimos, se han modificado niveles (básico, medio y alto): ha habido algunos cambios, ha habido datos que han subido de nivel y otros que han bajado. Entre los que han subido de nivel y se incorporan o exigen medidas de seguridad de nivel alto (y esto es una decisión lógicamente de política normativa del Gobierno que ha aprobado el Decreto), son los datos relacionados con la violencia de género.

En el nivel medio se aclaran dos cuestiones. El tratamiento de datos por parte de las administraciones tributarias y de las entidades financieras estaba ya sujeto al nivel medio de medidas de seguridad pero lo que el Reglamento aclara es que no todos los ficheros de la administración tributaria ni de las entidades financieras tienen que estar en el nivel medio; serán aquellos que respondan a esa finalidad tributaria o financiera. Un fichero de recursos humanos de un banco o de una caja de ahorros no se diferencia en nada de un fichero de recursos humanos de cualquier organización de una naturaleza equivalente y, por tanto, para ese fichero no es necesario el nivel medio.

La externalización del servicio de gestión de datos personales se ha convertido en una práctica generalizada y habitual por parte de las administraciones públicas y las empresas privadas".

También se incorporan al nivel medio, el tratamiento de datos de entidades gestoras de la Seguridad Social y de mutuas patronales de accidentes de trabajo. Aquí quiero hacer una aclaración porque lo que significa este artículo, que eleva esas medidas de seguridad, es que aquí sí, todos los ficheros de las mutuas patronales de accidentes de trabajo tendrán que tener por lo menos el nivel medio, excepto los que por la naturaleza de la información que contengan, por ejemplo, por tratar datos de salud, tengan que tener un nivel superior, que sería el nivel alto. Esta previsión lo que establece es el suelo mínimo. Siguen incluidos en el nivel medio los ficheros que permitan la elaboración de perfiles de las personas y también se han incorporado al nivel medio los ficheros de los operadores de servicios de telecomunicaciones. Para los operadores de servicios de telecomunicaciones, hay una regulación particular. Los ficheros tienen que cumplir las medidas de seguridad del nivel medio y, además,

tienen que incorporar una medida de nivel alto, que es el control de accesos detallado que permite saber el momento concreto en que se trató de acceder a la información, si se accedió, si se denegó el acceso y si se accedió a los registros a los que se accedió.

En cambio, hay otros ficheros que han bajado de nivel. Los de ideología, afiliación sindical, religión y creencias, vinculados fundamentalmente a la realización de transferencias dinerarias (el caso más habitual son las cuotas sindicales que voluntariamente el trabajador quiere que su empleador transfiera a su sindicato, aunque implican el tratamiento de datos especialmente protegidos de afiliación sindical o de ideología), están en el nivel básico. También lo están el tratamiento de datos de salud en algunos casos, como los relativos a la discapacidad o minusvalía.

Hubo una primera excepción que se propuso para que los ficheros de retenciones tributarias que implicaban tratamiento de datos de salud fueran a nivel básico pero, al final se ha adoptado una fórmula más amplia. En este sentido se cuestiona el por qué se ha hecho una ampliación con aquellos tratamientos que sean, por ejemplo, de la condición de discapacidad o invalidez relacionados con el cumplimiento de deberes públicos. Y la respuesta es que los datos de discapacidad y de minusvalía no sólo se tratan en el ámbito de las retenciones tributarias sino en otro abanico de medidas que tratan de favorecer la inserción, la educación, la vida normal de personas que tienen un grado de discapacidad o de minusvalía y, por tanto, no tendría sentido que se exigiera el nivel básico para los datos de discapacidad en el ámbito tributario y no para solicitar una beca en la universidad o para cualquier otra previsión legal que vaya asociada al tratamiento de ese tipo de información. Por eso, se señala que, cuando esté relacionado el tratamiento de estos datos con el cumplimiento de deberes públicos las medidas de seguridad serán de nivel básico.

Al término de una prestación de servicios, la información debe pasar del anterior al nuevo responsable, que deberá cumplir con todas las garantías que establece el artículo 12 de la LOPD".

También hay otra excepción, por la que los tratamientos de datos manuales no automatizados que, de forma incidental o accesoria supongan el tratamiento de esta información sensible, tienen que ir al nivel básico. Esto a lo que se refiere, como ejemplo paradigmático, es a un registro general de cualquier organización. Por un registro general de una organización puede entrar la información más sensible, por

ejemplo, a través de una solicitud en la que diga que es miembro de un partido, de una confesión religiosa, tales o cuales datos. Esa información simplemente sale de ese registro general y se redistribuye a los distintos departamentos donde efectivamente se va a tratar. Hacer que se exijan medidas de nivel alto por el riesgo de que esa información en papel en un registro general pueda tener datos especialmente protegidos, puede resultar desproporcionado; y por eso se ha introducido esta excepción.

La persona que ha sido prestador de servicios de gestión de bases de datos puede y debe conservar la información, de manera bloqueada, para poder atender a responsabilidades administrativas o jurisdiccionales".

Muy sintéticamente, de las novedades del Reglamento, en mi opinión, las principales en materia de seguridad han sido: primero, que el

documento de seguridad pasa a ser el instrumento básico (ya lo era, pero el Reglamento destaca con más precisión o con más nitidez) que es la herramienta básica de la política de seguridad de cualquier organización, y por eso ya no está como una de las medidas de nivel básico sino que tiene una regulación previa y aparte, y además es común a automatizados y a no automatizados. En segundo lugar, que se ha tratado de buscar sistemas que flexibilicen el cumplimiento de las medidas de seguridad, fundamentalmente a través de la posibilidad de delegar autorizaciones o la posibilidad de establecer perfiles de usuarios más genéricos, de forma y manera que no suceda como con el actual Reglamento que parece que el consejero delegado de una gran corporación tiene que estar autorizando todo en materia de protección de datos; o los responsables de seguridad. Cabe destacar que en el documento de seguridad se adopten políticas garantistas pero flexibles, definiendo perfiles de usuario y también incorporando, tomando nota o haciendo constar delegaciones de autorizaciones en unas y otras materias. Se ha venido a aclarar en particular la cuestión que se ha planteado en ocasiones en la Agencia con muchas dudas, de cuáles son las medidas de seguridad que deben adoptarse cuando hay una prestación de servicios. El Reglamento viene a aclarar que depende: si los servicios los va a prestar el encargado del tratamiento (el prestador de los servicios en los propios locales donde se está tratando la información del responsable), no tiene por qué adoptar unas medidas de seguridad adicionales sino que se haga constar que hay una prestación de servicios y que se cubra con esas medidas de seguridad y con ese documento de seguridad existente. Si por el contrario, va a hacer el tratamiento de datos fuera de sus propios locales, sí que tendrá que adaptar unas medidas de seguridad específicas o modular las que tuviera.

"Cualquier responsable de un tratamiento de datos que dispone de un servicio de atención al público o reclamación de clientes, podrá utilizar los mismos procedimientos para identificar a las personas".

Hay una indicación de carácter pedagógico en materia de seguridad que es precisamente para determinadas prestaciones de servicios que no tienen que implicar el tratamiento de datos personales, como los servicios de limpieza o los servicios de mantenimiento, pero que en la práctica se ha demostrado que al final a las personas que hacen estas funciones de limpieza en un momento determinado cogen la información y acaba en la calle en un

contenedor y ya tenemos un problema en materia de protección de datos. Por eso, se ha incorporado una advertencia de que hay que insistir a las personas que trabajen en esas prestaciones de servicios que no deben tener acceso a la información personal y que en todo caso, deben cumplir con las exigencias de seguridad y de secreto.

Se han reforzado o aclarado algunos aspectos en medidas de seguridad, fundamentalmente las relacionadas con la gestión de soportes. Cuando se hizo el Reglamento, no se habían multiplicado como en la actualidad se ha producido los soportes que permiten acceder a la información. Ahora hay dispositivos como los "pen drive", o simplemente un fichero anejo a un correo electrónico, que pueden contener información relevante y amplia cantidad de información; y por eso el Reglamento viene a aclarar que esas herramientas también son soportes y que deben cumplir con las medidas de seguridad previstas para cada uno de los niveles.

El derecho de oposición garantiza que un individuo no reciba, por ejemplo, más comunicaciones publicitarias aunque en un primer momento las haya aceptado".

Quizá otra de las principales novedades, y con esto termino, son las medidas de seguridad de ficheros no automatizados. Para estas medidas, el Gobierno ha optado por una solución lo más sencilla posible. Se distinguen tres niveles de seguridad también: básico, medio y alto. En el nivel básico, prácticamente lo único que se contempla es que los dispositivos donde se almacene la información (los archivos, los armarios), tienen que tener algunos dispositivos de cierre, que no es ni más ni menos que una llave. Se ha previsto también que haya una cierta diligencia en lo que es el tratamiento de la información desde que se recibe hasta que esa información se organiza y se incorpora a esos archivos.

En el nivel medio sólo son medidas organizativas: el que haya responsables de seguridad y el que haya una auditoría, exactamente igual que la que se puede realizar o que se exige como mínimo para los ficheros automatizados de nivel medio; porque sería un sinsentido cuando la mayor parte de los ficheros que vamos a encontrar serán mixtos, en parte automatizados y en parte no, que la auditoría fuera sólo parcial.

En el nivel alto, sí hay alguna previsión específica que se refiere fundamentalmente a los

locales donde pueda estar almacenada información particularmente sensible, por ejemplo, historias clínicas en papel en un centro sanitario, y sí se exige que haya una separación física de esas instalaciones. Pero al mismo tiempo, esas exigencias son también flexibles porque se prevé que si eso fuera de imposible cumplimiento, se puedan describir esas complicaciones, y se pueda motivar, por lo tanto, en el documento de seguridad que no se puede cumplir con esas medidas específicas y se pueden adoptar medidas alternativas. Si no se puede reorganizar toda la estructura física de una oficina, a lo mejor se puede poner un vigi-

Los datos relacionados con la violencia de género han subido al máximo nivel (alto) y se incorporan y exigen medidas de seguridad del mismo grado".

Las personas encargadas de limpiar o mantener los archivos no deben tener acceso a la información personal y, en todo caso, deben cumplir las exigencias de seguridad y secreto".

lante de seguridad en la puerta y podría ser una medida de efecto equivalente. También se hace una referencia a que hay que tener una diligencia adicional para las comunicaciones de la información sensible pero muy elementales, prácticamente el que los sobres vayan cerrados, que haya alguna garantía que dificulte el acceso a esa información y desde luego nada comparable con la exigencia de cifrado o de medidas equivalentes cuando se hacen las comunicaciones de información sensible a través de tratamientos automatizados.

El último aspecto que quería destacar es el relacionado con la copia o reproducción y la gestión de soportes en ficheros en soporte papel de nivel alto, que lo que se viene a exigir son unas medidas básicas de control de qué reproducciones se están haciendo de esa información o de quiénes son los destinatarios y cómo ésta tiene que volver a su depósito. En este caso, el ejemplo de las historias clínicas, que es uno de los más habituales de información sensible en soporte papel, es claro. No se puede fotocopiar y andar reproduciendo la historia clínica de las personas de cualquier modo. Si sale la información de los centros encargados de custodiarla en el ámbito de un establecimiento sanitario, tendrá que saber a quién va y habrá que reclamar que vuelva y que esté íntegra.

Con esto por lo menos he tratado de hacer un abanico de temas, novedades y aspectos destacables, en mi opinión, del Reglamento. Gracias por su atención y muchas gracias.

ANA MARZO: “ UN ANTES Y UN DESPUÉS CON LA LOPD, UNA NORMA DE OBLIGACIONES”

Yo no voy a entrar a detallar la descripción de las novedades del Reglamento sino más bien trataré de explicar en qué consiste el cumplimiento de la normativa sobre protección de datos en el día a día de las organizaciones. Efectivamente el Reglamento, como ha dicho Jesús Rubí, nos introduce, por un lado, una serie de criterios que doctrinalmente y en cuanto a jurisprudencia se refiere, ya estaban siendo admitidos tanto por la Agencia Española de Protección de Datos como por nuestros Juzgados y Tribunales; y, en segundo lugar, viene a aclarar puntos que realmente adolecían de una falta de desarrollo reglamentario, porque la normativa complementaria de la LOPD provenía fundamentalmente de los desarrollos reglamentarios de la primera Ley de Protección de Datos que tuvimos en nuestro país, la LORTAD, que es del año 92. Por tanto, efectivamente los reglamentos que teníamos estaban un poco obsoletos, salvo el Reglamento de Medidas de Seguridad que más o menos nació a la vez que la segunda Ley de Protección de Datos en el año 1999 y, por tanto, de alguna forma y en alguna medida sí que venía a estar más actualizado que el resto de la normativa.

Efectivamente, yo pienso que habrá un antes y un después con la publicación y aprobación de este Reglamento. Una cuestión importante que yo siempre mantengo frente a las organizaciones respecto a cómo debe cumplir la empresa esta normativa, es que la LOPD en mi opinión es una norma de obligaciones, es una norma de formalidades. Las empresas se asustan mucho y su sentir es que con la Ley Orgánica de Protección de Datos no se puede hacer prácticamente nada. Yo siempre defiendo lo contrario, que con la Ley Orgánica de Protección de Datos se puede hacer prácticamente de todo. El problema suele venir cuando una organización pretende ejecutar una serie de acciones para lo cual no está legitimada precisamente por la falta de cumplimiento previo de la normativa vigente. ¿Por qué? Porque el vicio está en origen, en no haber cumplido las formalidades previstas en la Ley Orgánica. Realmente reitero que en mi opinión, la Ley Orgánica de Protección de Datos es una ley de obligaciones, es una ley de formalidades previas y durante la ejecución de un tratamiento de datos. El Tribunal Constitucional lo ha explicado además, de una manera muy sencilla y clara: no se está prohibiendo, lo que la Ley ha establecido es un régimen de obligaciones y formalidades -que condiciona el tratamiento- dirigido fundamentalmente a proteger la privacidad y la intimidad de las personas, aunque muchas veces desde el lado empresarial cuesta creer que tratar un dato de carácter personal consistente en un domicilio o una cuenta de correo pueda invadir ningún tipo de privacidad o intimidad de las personas y además deba ser protegido a través de un sistema de garantías de medidas de seguridad.

Si otorgamos una lectura tranquila al nuevo Real Decreto, al nuevo Reglamento, lo que puede

Ana Marzo al inicio de su conferencia en la sede de la CEN.

constatar es que esta nueva norma pretende garantizar el cumplimiento de la Ley Orgánica de Protección de Datos a través de procedimientos en esta materia; es decir, obligar a las empresas a que trabajen con una serie de procedimientos, los cuales después puedan acreditar el cumplimiento de la normativa. Jesús Rubí ha dicho algo importante, en dos ocasiones, cuando estaba hablando de la forma en que un responsable del tratamiento se tiene que dirigir al afectado para solicitar su consentimiento o informarle de cuál es el contenido del tratamiento; y en un momento determinado ha hablado de sistemas auditables, tanto en el envío de comunicaciones como en la constatación de si el afectado las ha recibido o no. En el nuevo reglamento se recogen y regulan muchas situaciones similares. El reglamento de alguna manera traslada la carga de la responsabilidad administrativa en el responsable del tratamiento y en el encargado del tratamiento, en cuanto a que ellos tienen la obligación de poner de manifiesto que cumplen la normativa y las obligaciones derivadas de la ley y el propio reglamento, es decir, la presunción de cumpli-

La LOPD no está prohibiendo nada; lo que hace es obligar a que se cumplan una serie de formalidades que protegen la privacidad e intimidad de las personas.

miento se convierte en una obligación de demostración de que se está cumpliendo. Este objetivo solo puede alcanzarse de una forma, mediante la creación de procedimientos auditables –como ha explicado Jesús Rubí- destinados al cumplimiento de la Ley Orgánica de Protección de Datos en relación con todos los procesos de trabajo que tiene una organización que requieren el tratamiento de datos personales.

En este sentido, a la pregunta de cuál es mi experiencia cuando me encuentro ante una empresa grande, mediana o pequeña respecto a su nivel de cumplimiento de la normativa sobre protección de datos, la respuesta es que en general, el tamaño suele dar igual, lo relevante es el que el nivel de cumplimiento de la normativa suele ser escaso e insuficiente en cualquiera de ellas, bien por falta de recursos, bien por ignorancia del contenido de la normativa, o incluso de la normativa en sí.

En cuanto a cuál es la experiencia que tenemos en cuanto a cómo se aborda por parte de las empresas un proyecto destinado a garantizar el cumplimiento de la normativa sobre protección de datos, la respuesta es que en general, el desarrollo de un proyecto de adaptación a la Ley Orgánica de Protección de Datos en las organizaciones termina con un cumplimiento de la Norma dividido, descoordinado y parcelado, es decir, te encuentras con que hay departamentos que alcanzan un nivel óptimo de cumplimiento de la Ley y hay otros que no llegan ni a cimentar las

El Real Decreto obliga a las empresas a que trabajen con una serie de procedimientos o procesos de trabajo, los cuales pueden acreditar después el cumplimiento de la normativa.

bases. Es una casuística diversa pero que se repite mucho. A veces el departamento más diligente es el de recursos humanos porque tradicionalmente en su forma y organización de trabajar considera que tiene una serie de datos sobre los trabajadores por los cuales debe velar enormemente por su seguridad, confidencialidad, deber de secreto, etcétera. Sin embargo, te sueles encontrar con que los departamentos de marketing por su práctica, dinámica y su forma de trabajo, efectivamente son departamentos más descuidados, ya no solamente en las medidas de seguridad sino también en el cumplimiento de otras formalidades jurídicas tales como el principio de información en el momento de recogida de los datos o el principio de autodeterminación en relación con la obtención o no del consentimiento del interesado a quién se dirigen los envíos publicitarios. ¿Por qué? Porque el objetivo del departamento de marketing es distinto del departamento de recursos humanos. En general, cada uno cumple la ley un poco a la manera y buen entender que tiene, sin que por encima de los departamentos exista alguna directriz o normativa por parte de la empresa sobre cuáles deben

ser los criterios comunes acordes con los principios de la Ley Orgánica, tanto para un departamento como para otro. En principio, el reglamento de desarrollo de la LOPD viene a obligar precisamente a la determinación en las organizaciones de estos principios comunes a través de los procedimientos.

Asimismo, el cumplimiento de la normativa sobre protección de datos en las empresas es poco sistemático. Y me explico. Realmente el cumplimiento de la normativa está en manos de los trabajadores, en manos de los usuarios de la información, de forma que, cuando se constata que la organización no ha proporcionado a los usuarios de la información recursos suficientes para el cumplimiento de sus obligaciones, formación específica relacionada con la normativa vigente y no se han establecido las pautas básicas en el respeto de la Ley Orgánica en el tratamiento de los datos, la conclusión inevitable es que se convierte en inviable e imposible que los trabajadores o usuarios de los datos cumplan la LOPD o el nuevo reglamento. Otra cosa sería un milagro.

Te sueles encontrar que los departamentos de marketing, por su práctica y dinámica, son más descuidados en cuanto a seguridad se refiere; por el contrario, los de recursos humanos están más acostumbrados a tratar con datos personales.

Esta situación es evidente en los trabajos de auditoría de cumplimiento de la Ley, no ya de seguridad, sino una auditoría para determinar el nivel de cumplimiento que tiene la organización en relación con todos los principios y normas establecidas por la LOPD. En este sentido cuando los trabajadores auditados pertenecen a una gran empresa y les preguntas acerca de cuáles son sus obligaciones en materia de protección de datos o qué es lo que ellos consideran que son sus obligaciones, en la mayor parte de las ocasiones su contestación es que no están seguros aunque creen que disponen de una política en este sentido almacenada en algún lugar de la intranet de la empresa, pero que realmente tienen tantas políticas y normativas redactadas por la empresa, por una matriz, o por alguna otra filial del grupo, que no son capaces de distinguir ni de reconocer exactamente los supuestos de hecho en que requieren o tienen la necesidad de cumplir una política determinada, en este caso en particular, una política de protección de datos. La realidad es que los trabajadores no son ni conscientes de todas las políticas ni normativas a que están obligados o que son de aplicación al desarrollo de sus funciones. Esto es muy frecuente en el sector financiero y asegurador donde las normativas de los usuarios en relación con el desarrollo de sus actividades es muy abundante y por tanto, la normativa sobre protección de datos no deja de ser “una más”.

El enfoque en las pequeñas empresas es bien distinto. En estos casos la escasez de recursos conlleva que no exista ni siquiera una normativa elaborada en materia de protección de datos. Los usuarios se enfrentan en el día a día al tratamiento de los datos sin saber exactamente qué es lo que tienen que cumplir. Efectivamente, el primer problema está en que son los usuarios los que no han recibido los medios, ni la formación, ni las pautas ni las normas ante las cuales deben enfrentarse para poder cumplir la legislación.

Otro de los problemas que impiden un buen trabajo de adaptación a la Ley Orgánica de Protección de Datos internamente en las organizaciones es el empeño en hacer depender el proyecto exclusivamente de un único departamento. Generalmente, esta disputa suele estar entre el departamento legal y el departamento de informática o sistemas de información y desgraciadamente la disputa lo es no para liderar el proyecto sino para precisamente lo contrario, trasladar la responsabilidad de este liderazgo de uno a otro. En la mayor parte de las ocasiones nunca estos dos departamentos alcanzan el mismo nivel de responsabilidad frente a un proyecto de adaptación a la Ley frente al resto de la organización para hacer cumplir la normativa, lo cual para nosotros es una cuestión prioritaria y de la que depende el éxito o fracaso del proyecto.

Es frecuente que las empresas que tienen departamento legal no son capaces de abordar la materia de protección de datos porque los abogados no conocen la materia. El abogado interno de la empresa suele especializarse en el derecho que afecta a la empresa en el día a día, mercantil, laboral, civil, pero se terminan externalizando aquellas materias que el departamento jurídico internamente no conoce. Y entonces lo que ocurre es que en ocasiones, cuando un profesional externo va a dar apoyo a la empresa el problema con el que se encuentra es que el abogado no es un buen interlocutor porque éste delega en el externo ciertas responsabilidades que no se pueden llegar a cubrir desde fuera de la organización.

Con el departamento de informática o sistemas la situación es similar. El problema que suele tener el departamento de sistemas es que no cuenta con el apoyo de la dirección ni con el apoyo del abogado. Por eso muchas veces el departamento de sistemas contrata un proyecto para “limpiar su conciencia” o buscando “ese papel” donde un consultor externo ha determinado la obligación de cumplir la Ley o ha constatado que la LOPD no se está cumpliendo dentro de la organización”. El informático lo que va buscando de alguna manera es, en definitiva, salvaguardar su responsabilidad, encargando un documento a una entidad con credibilidad y externa a la organización, que manifieste cuál es la situación, los riesgos a los que se expone la entidad de forma que, si un día hay un problema, él pueda recordar que lo advirtió. De esta forma, si un día hay un problema en la empresa (una reclamación, una

denuncia, o una inspección), lo que nos vamos a encontrar es seguramente ante una situación muy desagradable donde se detecten infracciones y estemos sujetos a plazos, procedimientos sancionadores y quizá a posibles sanciones u otro tipo de responsabilidades.

Con cierta tristeza diré que, en toda la experiencia profesional que tengo, puedo contar con los dedos de una mano aquellos supuestos donde he podido trabajar un proyecto LOPD de forma coordinada y en colaboración con los departamentos de asesoría jurídica e informática o sistemas de información.

En mi opinión con el nuevo reglamento hay un departamento que se revela como "crucial". Es el departamento de calidad, y no tanto porque tenga una responsabilidad especial en cuanto a la generación o determinación de las medidas LOPD en sí, sino por cuanto este departamento está muy acostumbrado a determinar cómo deben cumplirse las políticas y normativas de una organización y sabe muy bien cómo hacer llegar o distribuir a todos los usuarios las políticas y normativas, cómo crear procedimientos para que efectivamente el cumplimiento de la normativa llegue a todos los empleados y que todos la cumplan. Creo que con el nuevo Reglamento, el departamento o departamentos de calidad o aquella persona que se integre en la organización con funciones de esta naturaleza va a tener mucho trabajo, un trabajo bonito y un trabajo de coordinación precisamente con los otros departamentos mencionados, el jurídico y el de sistemas de información.

El problema reside en que los mismos usuarios no han recibido ni los medios, ni la formación, ni las pautas, ni las normas ante las cuales deben enfrentarse para poder cumplir la legislación.

Otra práctica muy frecuente es nombrar un responsable de seguridad y delegar en él toda la responsabilidad. De alguna manera ya hemos dado a entender que esta situación efectivamente no tiene sentido. El responsable de seguridad no puede con todo. Además en general los responsables de seguridad tienen un problema añadido. En la mayor parte de las empresas el nombramiento de esta figura no recae en alguien ajeno a la organización sino que es el propio responsable de informática que trabaja en el departamento de sistemas de información a quien, precisamente por tener conocimientos de informática le ha caído la tarea o el sambenito del responsable de seguridad, con todas las tareas que marca el Reglamento y la legislación vigente. La realidad es que una persona que ya tiene asignadas unas funciones de trabajo en el departamento de informá-

tica difícilmente sin apoyo y sin más recursos podrá llegar a realizar y cubrir todas las obligaciones derivadas de la legislación vigente en protección de datos, en materia de seguridad (implantación de medidas físicas, técnicas, organizativas), obligaciones de control y de auditoría y obligaciones contractuales y de formación que se exigen en la organización al responsable de seguridad.

Los departamentos legales y de informática suelen tener disputas a la hora de abordar un proyecto de protección de datos; por desgracia, muchas veces éstos no están ni al mismo nivel, ni tienen la misma responsabilidad.

En cuanto a los usuarios, éstos no tienen conocimiento, no tienen formación y no son conscientes muchas veces de los requerimientos legales. Esto es una evidencia en los trabajos de auditoría cuando se entrevista a los trabajadores y se les efectúan preguntas del orden de sí conocen cuáles son las consecuencias o responsabilidades en que incurren en caso de incumplimiento de la LOPD, o cuales son las normativas que deben cumplir, te das cuenta de que no tiene una conciencia exacta de ello.

También tristemente diré que cuando la empresa se ve inmersa en la apertura de un procedimiento sancionador -a veces la multa no es muy alta pero en otras ocasiones la multa puede llegar a los 300.000 euros (la multa se gradúa entre otros parámetros en función del tipo de infracción y el tipo de infracción lo marca la normativa, la Ley Orgánica de Protección de Datos)- el trabajador o empleado se da cuenta de que por una negligencia de la cual él no era consciente, la empresa puede ser sancionada con 300.000 euros (o que de hecho es sancionada) y el trabajador también lo pasa mal porque él no ha llevado a la empresa a esa situación de forma consciente, por norma general no ha habido una situación de mala fe sino de negligencia por ignorancia.

Finalmente, y en el marco de los trabajos requeridos para la realización de un proyecto de adaptación a la LOPD, otro de los problemas de las empresas es que generalmente nunca se trabaja en equipo. Si hay una reclamación, como decía Jesús Rubí, o un afectado ejercita un derecho de acceso y de pronto salta la alarma en la organización, “oye, que nos ha llegado este papel”, se apaga puntualmente ese fuego. Se contesta a la persona, en ese momento se ponen en marcha todos los mecanismos de reserva, de protección o salvaguarda de los intereses de la empresa, se contrata todo lo que se puede contratar para “apagar ese fuego” puntual, pero una vez pasa la situación todo se olvida, no hay continuidad se olvida de que hay normativa por cumplir y ya no se vuelve a hablar del tema.

Ahora trataremos de analizar más o menos y con una visión esquemática cuáles son las obligacio-

nes que marca la Ley Orgánica de Protección de Datos en el tratamiento de la información de los datos de carácter personal y por tanto cuáles son los imperativos que debe respetar una organización en cuanto responsable del tratamiento.

Como he mencionado al inicio, tendríamos, por un lado, lo que son obligaciones, y por otro lado, lo que esas obligaciones al final nos van a generar: la necesidad de crear procedimientos.

En primer lugar existe la obligación de declarar los tratamientos responsabilidad de una organización. La obligación de declaración de los tratamientos a la Agencia Española de Protección de Datos es quizá es la más sencilla, la menos complicada. Su cumplimiento además se facilita por la propia Agencia a través de su página web "www.agpd.es" mediante la descarga del programa NOTA y la cumplimentación de los formularios público o privado de declaración de ficheros, que además ahora son simplificados (no son los formularios que existían hace unos años). Efectuada la cumplimentación del formulario por cada fichero a través de la propia página web se declara el fichero.

Ahora bien, no todo termina con declarar los ficheros, sino que se debe procurar su actualización continua. Para ello, una de las cuestiones que nosotros recomendamos en las organizaciones es que exista un procedimiento interno al

efecto. Que haya responsables que garanticen la custodia de las declaraciones obrantes en el Registro General de Protección de Datos (muchas veces las empresas ni siquiera disponen de la documentación original enviada a la Agencia). El hecho es que debe existir alguien responsable del mantenimiento de los ficheros a nivel registral de forma que, si efectivamente ha cambiado alguna de las características descritas en el formulario NOTA en relación con el contenido del tratamiento, actualice esta circunstancia en el Registro de la Agencia a través de una declaración de modificación o de supresión.

Por poner un ejemplo, sí la entidad responsable ha declarado un tratamiento de marketing para realizar campañas de publicidad postal pero a partir de un determinado momento comienza a realizar publicidad por e-mail (con lo cual se ha incorporado un campo más a ese tratamiento que estaba declarado y el cual adolecía del campo del correo electrónico) será necesario actualizar la declaración obrante en el Registro General de Protección de Datos. También es frecuente encontrarnos en la situación de que la empresa cambia de domicilio, de teléfono, de encargado del tratamiento y, sin embargo, en la información que se ha enviado a la Agencia Española de Protección de Datos no se actualizan estos datos. De manera que, de alguna forma, creo que es conveniente no solamente declarar los tratamientos en el momento de su creación sino también de comprobar permanentemente

Con cierta tristeza diré que llego a contar con los dedos de la mano los casos en los que los departamentos de sistemas de información, legal e informática trabajan de forma coordinada.

que no tenemos ni más ni menos ficheros en producción o en explotación que impliquen nuevas declaraciones de creación de ficheros y que, además, las declaraciones en todo momento estén actualizadas. La infracción por no tener el tratamiento o el fichero actualizado no se caracteriza por ser de elevada cuantía económica, pero de alguna manera también es sancionable el hecho de que la documentación que obra en el Registro General de Protección de Datos no esté actualizada y realmente lo que haga es poner de manifiesto la situación real de la empresa.

En segundo lugar, el principio de calidad. En mi opinión es uno de los más difíciles de cumplir en la normativa dentro de una organización. El principio de calidad exige tratar los datos de forma leal, lícita. A mi juicio y con una visión extensiva, tratar los datos lícitamente implica cumplir toda la normativa porque, si no estamos no cumpliendo alguna de las obligaciones que establece la ley, el tratamiento no es lícito.

Además el principio de calidad implica que los datos sujetos a tratamiento deben ser exactos y

puestos al día. ¿Qué quiere decir que sean exactos y puestos al día? Quiere decir exactamente lo que los adjetivos significan y cómo lo califican. Al hilo de esta obligación, creo que uno de los grandes aciertos de la LOPD frente a nuestra primera Ley de Protección de Datos, la LORTAD, fue precisamente el determinar que el no mantener la información exacta solo es infracción si ello causa algún perjuicio al interesado (en la LORTAD de todas maneras se constituía como infracción y, sin embargo en la LOPD en principio no es infracción, salvo que se demuestre que no mantener la información exacta ha causado algún perjuicio al interesado). En todo caso, el Reglamento y la Ley parten de la base de que si la empresa responsable del tratamiento ha cedido a un tercero previamente los datos rectificados o cancelados, el responsable debe igualmente comunicar los datos rectificados o cancelados al tercero cesionario para que de la misma forma actualice los datos en sus ficheros. El plazo para cumplir con esta obligación es ciertamente escaso, diez días.

Aquella persona de la organización que se encargue de estas funciones, va a tener mucho trabajo; un trabajo muy bonito y verdaderamente importante.

No obstante, creo que un acierto del nuevo Reglamento ha sido partir de la base o del hecho de que la información que te proporciona directamente el propio afectado está actualizada, pero normalmente las empresas tenemos muchas más vías de entrada de información. Sin ir más lejos, en los ficheros de recursos humanos muchas veces se recoge información de familiares del trabajador. En ese caso, la información no está proporcionada directamente por el propio interesado, por lo tanto, de alguna forma en la empresa se tienen que articular también procedimientos para poder llegar a todos esos colectivos de quienes no hay una recogida de datos directa para tener también la su información actualizada.

Quizá también es importante resaltar dentro del principio de calidad la proporcionalidad en el tratamiento y acopio de los datos, porque muchas veces en las organizaciones se van almacenando datos y, a veces, a la pregunta de sí toda esta información es necesaria y útil a los fines legítimos de la empresa la respuesta es “no, en principio no nos hace falta”. En realidad, el principio de calidad lo que establece es que la recogida y tratamiento de los datos debe ser necesaria y no desproporcionada para llevar a cabo el tratamiento conforme a una finalidad legítima del responsable del tratamiento. Creo que con este principio hay que ser especialmente cuidadosos y sobre todo insisto, porque muchas veces cuando un departamento se plantea la recogida de información -sobre todo los departamentos de mar-

keting- quizá recogen más información de la debida y ello puede viciar posteriormente el cumplimiento de otros principios que establece la LOPD, además del de calidad.

El tema de la cancelación es importante. Como decía Jesús Rubí, un gran acierto del RD 1720/2007 ha sido el determinar, más o menos cómo procede dentro de una organización, el cumplimiento del principio de calidad desde que se recoge el dato, está siendo tratado y cuando ya el dato no necesita se tratado, bien porque nos han ejercitado un derecho o bien porque ya no es necesario para la finalidad para la que fue recogido. En tal caso deberíamos establecer un proceso de bloqueo que no significaría la supresión física, sino que, terminados los plazos del ejercicio en curso durante el cual todavía tenemos algún tipo de relación con el interesado o estamos sujetos a un régimen legal de responsabilidades, el dato debe ser bloqueado, lo cual impide, en principio, cualquier acceso a la información incluso a modo de consulta. ¿Qué ocurre cuando han pasado los plazos por los cuales las leyes marcan los periodos de exigencia entre las partes de posibles responsabilidades? Entonces el dato debe ser suprimido físicamente, o disociado, que al fin y al cabo es una forma de supresión.

En tercer lugar nos encontramos con la obligación de cumplir con el principio de autodeterminación e información al afectado.

Los usuarios no tienen conocimiento ni formación, y muchas veces no son conscientes de la infracción, que puede llegar hasta los 300.000 euros.

En cuanto al consentimiento y la información, estos son los grandes pilares básicos de la normativa sobre protección de datos. El Tribunal Constitucional además así lo ha manifestado porque la información que se proporciona al interesado en relación con el contenido del tratamiento o con quién es el responsable que se va a hacer cargo y va a conservar la información, es lo que permitirá al interesado ejercitar toda una serie de derechos que marca la normativa y que son las garantías que al interesado le permiten controlar quién tiene o no los datos, permitir o no las finalidades de tratamiento, incluso autorizar la cesión de sus datos a un tercero o no hacer uso de este derecho. En definitiva, la información que se proporciona al afectado es lo que posteriormente le permitirá ejercer un control sobre el tratamiento de sus datos ante cualquier responsable.

En todo caso, el consentimiento yo diría que conlleva varias fases de regulación. En primer lugar, valorar si la Ley nos permite tratar el dato por algún tipo de excepción sin consentimiento del afectado o tenemos que “morir” en la norma general de la Ley que es que se requiere el consentimiento del afectado o interesado para efectuar el

tratamiento. En segundo lugar, tenemos que tener claro que el consentimiento no es indefinido, que cabe la revocación del consentimiento por parte del interesado y de hecho uno de las novedades del Reglamento es la determinación de un procedimiento para garantizar el derecho a la revocación del consentimiento otorgado para el tratamiento del dato por parte del interesado, es decir, que el afectado hoy puede consentir el tratamiento pero posteriormente y sin causa justificada (simplemente su voluntad) puede desear poner fin al tratamiento de forma que la empresa que estaba tratando el dato o el responsable del fichero deje de tratarlo. En el nuevo Reglamento lo que se establece es que además, es el responsable del fichero quien tiene que acreditar que obtuvo el consentimiento del interesado para poder tratar el dato.

En cuanto al principio de información, yo diría que es uno de los que más cuesta que las empresas entiendan. En mi opinión es realmente obvio este principio. Simplemente implica la obligación de información al interesado sobre el contenido del tratamiento de sus datos cualquiera que sea la forma de obtención del dato: del propio afectado, de una tercera entidad o de fuentes públicas. La obligación se establece en el artículo 5 de la LOPD y pretende otorgar al afectado un instrumento de conocimiento y control sobre el tratamiento de sus datos. El motivo por el que las empresas no alcanzan a comprender el significado de este principio puede ser diverso pero creo que básicamente en la mayor parte de los casos prima o prevalece simplemente la negativa a establecer los recursos que permiten su cumpli-

miento por lo costoso que puede llegar a ser y el trabajo que conlleva. Para los departamentos de marketing el espacio es fundamental por ello, a veces discuten la inserción de las comunicaciones informativas en los cupones de recogida de datos. Otras veces la empresa tiene miedo de informar por las posibles reacciones de los interesados, esto es frecuente en relación a los tratamientos de datos de personal. La información es lo que le permite al interesado poner fin al tratamiento, conocer quién está tratando los datos y en definitiva como hemos mencionado antes, ejercitar toda una serie de garantías que la Ley le otorga. La información que el responsable debe proporcionar al afectado para tratar sus datos debe ser expresa. Quiere decir que se debe poner de manifiesto expresamente, tiene que ser específica y también inequívoca. El interesado no puede tener ninguna duda en cuanto a qué se va a hacer y el alcance del contenido del tratamiento de sus datos de carácter personal. Desde el momento en que el responsable del tratamiento elabore algún tipo de comunicación informativa que pueda generar confusión o pueda dar lugar a un entendimiento equívoco al interesado, estará corriendo el riesgo de que dicho texto informativo sea declarado anulable o nulo de pleno derecho y, por tanto, ello es equivalente a no haber dado cumplimiento al principio de información.

El principio de calidad implica tratar los datos lícitamente. Para mí, es el más difícil de cumplir porque exige asumir todas las obligaciones que establece la Ley.

Además hay que tener en cuenta que es el responsable del fichero o tratamiento quien tiene la obligación de acreditar que ha cumplido con la obligación de información. ¿Cómo lo expresa el Reglamento? El nuevo Reglamento lo que dice es que aquellos deberán conservar el soporte a través del cual informó al interesado y además deberán hacerlo de forma que permanezca inalterado. Lo puede conservar en papel o lo puede escanear pero, de alguna manera, la carga de la prueba la va a tener el responsable del fichero o tratamiento.

El derecho de información es a mi juicio muy importante. El derecho de información se articula en la Ley Orgánica de tres maneras. El dato puede ser recogido directamente del propio afectado, en cuyo caso, sea la forma que sea o el canal a través del cual el afectado proporciona sus datos, debe ser informado en ese momento, si es por teléfono, por teléfono. La Ley Orgánica establece que si además la información te la proporciona porque te cumplimenta un formulario o cupón, un contrato, un cupón de publicidad o a través de cualquier formulario de recogida de datos por escrito, la comunicación informativa debe ir insertada en ese mismo formulario. Pero

la Ley Orgánica parte de la base de que el dato puede no ser proporcionado por el propio afectado sino facilitado por un tercero. En ese caso, la Ley Orgánica establece que en un plazo de tres meses el responsable del fichero debe dirigirse al afectado e informarle de que está procediendo a llevar a cabo el tratamiento de sus datos. Y finalmente habría una tercera situación que es cuando el dato procede de una fuente pública y es utilizado con fines de publicidad. En ese caso, lo que dice la Ley Orgánica es en el momento de la recogida del dato no hará falta informar pero en el momento en que se utilice el dato para hacer publicidad, en la propia comunicación publicitaria deberá ir insertado el texto informativo que proporcione al afectado la información suficiente como para poder poner fin al tratamiento, oponerse, cancelarlo e incluso rectificar los datos.

En materia de publicidad el derecho de información además se refuerza con otro abanico de obligaciones, como es que si el dato procede de una fuente pública editada en soporte papel con cada edición nueva que se efectúe de esa fuente habrá que consultar la nueva edición actualizada a ver si el dato se mantiene o no, o ha sido rectificado, y si el dato se ha obtenido de una fuente electrónica, con cada periodo anual a contar desde el momento de la obtención del dato de dicha fuente computado de forma natural también habrá que comprobar si el dato se mantiene o no, de forma y manera que mantengo otra vez

Los departamento deben establecer qué información debe ser recogida y no asumir más datos de los estrictamente necesarios para la finalidad establecida.

que hay determinadas obligaciones que si no es estableciendo un procedimiento será imposible que una organización pueda llegar a controlar.

En cuarto lugar la LOPD establece una serie de obligaciones para el responsable y el encargado del tratamiento en materia de seguridad.

En el tema de la seguridad estamos en las mismas, es decir, las obligaciones de seguridad del Reglamento y de la Ley Orgánica establecen una serie de propuestas, yo diría propuestas vinculantes, que al final nos llevan a hacer una clasificación de las medidas que hay que cumplir, como son medidas físicas, que al final son las más sencillas; medidas lógicas, que también son relativamente fáciles de implementar; las medidas organizativas, que requieren una labor de consultoría previa dado que con su implantación se alterarán procedimientos en la entidad, por lo que hay que efectuar una valoración de las necesidades, un diseño de las medidas y finalmente una implantación de las mismas. En cuanto a las medidas de control y auditoría, las primeras requieren de un esfuerzo y sobrecoste de recursos adicional durante todo el año, las segundas son las más

cumplidas por las empresas cada dos años (seguramente –como mencionaba anteriormente- por el ánimo del departamento de sistemas de información de trasladar a la dirección la preocupación por la protección de datos). El nuevo Reglamento introduce una nueva obligación de auditoría en supuestos en que exista un cambio sustancial en el sistema de información, y además añade como novedad que la auditoría se hará conforme a lo establecido, no solo en las medidas de seguridad del Reglamento sino que también en la propia Ley Orgánica. Realmente hay una confusión en el mercado en relación con la interpretación de este extremo:¿hay que revisar los principios normativos o legales o jurídicos en las auditorías o debemos revisar exclusivamente y en contra del reglamento lo establecido en relación con las medidas de seguridad?. En todo, caso la realización de la auditoría es una medida sencilla para las organizaciones.

Más difíciles son en mi opinión las medidas de control porque este tipo de medidas destinadas a garantizar un deber de diligencia mínimo no existen de forma periódica en las empresas. En las organizaciones del responsable y del encargado del tratamiento solo existe una preocupación real por la protección de datos y su nivel de cumplimiento cuando hay algún problema. Hasta entonces, no es una cuestión prioritaria.

Otro tipo de medidas de seguridad en mi opinión, son las de carácter contractual derivadas del artículo 12 de la LOPD y ahora también por las disposiciones concordantes del RD 1720/2007. ¿En qué consisten? En la suscripción de dos tipos de contratos para garantizar la seguridad y confidencialidad de la información: el contrato de acceso a datos para la prestación de servicios y el contrato sin acceso a datos para la prestación de servicios (novedad introducida por el nuevo Reglamento). En todo caso, debe existir un cierto control sobre la suscripción de estos contratos, la identificación de las partes contratantes y servicios prestados, el nivel de acceso a datos, el lugar de la prestación de servicios, el periodo de vigencia del contrato y la forma y consecuencias de la resolución. Además es preciso coordinar todos estos extremos con la información obrante en el documento de seguridad de la organización y mantener actualizado en el Registro General de Protección de Datos la declaración de los encargados del tratamiento más relevantes. Esta obligación por norma general no se mantiene al día en las empresas.

El Reglamento establece el derecho a la revocación al consentimiento, es decir, hoy puedo decir que sí y mañana me puedo arrepentir y anularlo.

Para terminar con el tema de la seguridad no podemos olvidar dos tipos de medidas más: la formación de los empleados y usuarios y la

Eduardo Zariquiegui, Jesús Rubí, Óscar Rived, Álvaro Abáigar y Ana Marzo.

implantación de medidas disciplinarias que sancionen el incumplimiento de las políticas y normas en la entidad. Se trata de una cuestión muy seria. En las empresas no se da formación a los empleados, sí se les reparte quizá a veces unas normas, unas pautas, se les dice que las pueden encontrar en la intranet pero a los usuarios hay que explicarles la legislación y las normativas, de otra forma no entienden cuál es el alcance de sus obligaciones. Y por otro lado las medidas disciplinarias; por norma general si los usuarios incumplen sus obligaciones "no pasa nada". El nuevo Reglamento insiste en esta cuestión y a pesar de que ya era una obligación establecida en el Real Decreto 994/99, el nuevo RD establece la obligación de explicar de forma "comprensible" a los empleados cuáles son sus obligaciones y las consecuencias de su incumplimiento. Sí los usuarios incumplen la normativa deben ser amonestados, porque, en definitiva, lo que la empresa no puede es tener un deber de diligencia tan mínimo que permita que dentro de la organización haya incumplimientos y no pase nada.

Las obligaciones de seguridad nos conducen a las obligaciones de confidencialidad y deber de secreto establecidas en el artículo 10 de la LOPD. La confidencialidad es en definitiva un deber moral de cada individuo, es un principio ético y en realidad es algo incontrolable materialmente, es decir, el que los usuarios que acceden a los datos que están almacenados en los sistemas de

información o en el papel de la organización después no divulguen esa información es, en primer lugar, una cuestión de conciencia, y, en segundo lugar, una cuestión de mentalización por parte de la organización a los propios empleados. Yo diría que hay alguna otra forma más represiva como es hacerles firmar acuerdos de confidencialidad o por lo menos compromisos de confidencialidad expresos donde los propios usuarios manifiesten por escrito que son conscientes de que la información debe ser custodiada y salvaguardada y no debe ser divulgada a terceros no autorizados. A veces la infracción y por tanto, la vulneración de los derechos de las personas, se produce no por saltarse una medida de seguridad física o lógica, sino por una mera divulgación de un dato.

En penúltimo lugar trataremos el tema de la atención a los derechos de los afectados. La nueva regulación establecida en el RD efectivamente tiene sus cosas buenas y sus cosas malas, pero desde luego en mi opinión es patente la necesidad de adoptar un procedimiento dentro de las organizaciones para la gestión de estos derechos, porque lo que sí se ha producido efectivamente con el nuevo Reglamento es la apertura y la permisión a los interesados (en especial a los clientes de una entidad) el ejercicio de los derechos a través de los canales implantados por una organización para atención de reclamaciones o canal de comunicación con los clientes. Por otro lado no es menos cierto que la aparente flexibilidad creada con el nuevo reglamento para la gestión de estos derechos creará dos tipos de situaciones no siempre claramente diferenciadas; la de los interesados que cursen su petición por los canales previamente determinados por la organización para la relación con clientes y la de los interesados que ejerciten sus derechos por otras vías más restringidas. La experiencia también me dice que hasta ahora, incluso muchas veces cuando llegan ese tipo de comunicaciones a la empresa, las cartas a veces se pierden, no existe alguien encargado de controlarlas, no se sabe en qué plazos y en qué forma hay que contestar.

La información que debemos dar al afectado debe ser expresa, específica e inequívoca.

En mi opinión uno de los derechos más importantes es el derecho de acceso. Su ejercicio es una cuestión muy seria. Los otros dos también pero el derecho de acceso permite al afectado conocer toda la información que el responsable tiene sobre su persona, la finalidad del tratamiento, si existen o no cesiones, en definitiva, el contenido del tratamiento. En línea con esto, en una empresa, muchas veces el dato de una persona no sólo se trata en un departamento, y a la hora de contestar a una carta de esta naturaleza muchas veces no basta con que indagues en un departamento, sino que debe coordinarse la información obrante con varias áreas o departa-

mentos a fin de comprobar si pudiera haber datos almacenados de una persona no sólo en alguna base de datos sino en otras tantas y verificar todas las finalidades de tratamiento. Luego, además, si el dato es rectificado o cancelado la rectificación y cancelación debe también proceder en todas las bases de datos que tiene la organización y no sólo en una, en dos o en algunas de ellas, sino en todas.

Cuando a mí me han preguntado acerca de cuáles son a mi criterio los ficheros más críticos en las organizaciones en materia de protección de datos mi respuesta siempre es la misma, a nivel de incumplimiento los más críticos son precisamente los ficheros de contactos que se tienen en las organizaciones porque son los más accesibles por los usuarios, los menos controlados, los más desactualizados y los más utilizados para hacer publicidad y spam.

En este asunto discrepo un poco con Jesús Rubí en el tema de que los ficheros de contactos a día de hoy puedan estar excluidos del ámbito de aplicación del régimen de protección de datos a la luz del RD 1720/2007.

La confidencialidad es algo incontrolable pero debe ser un principio ético y un deber moral del individuo.

Yo me he planteado muchas veces lo siguiente: "si yo soy una persona física, aunque pudiera entenderse que como fichero de contacto mi dato está excluido del ámbito de aplicación del RD 1720, a mí me ampara la Ley Orgánica que tiene rango jerárquico superior al RD y por supuesto además es Ley Orgánica. Si yo denuncio y solicito la tutela de la protección de mis datos a modo de mero contacto de una organización y al final mi reclamación no se cursa ante la Agencia Española de Protección de Datos, yo podría interponer el correspondiente recurso Contencioso-Administrativo ante la Audiencia Nacional para exigir de dicho organismo jurisdiccional la protección que al fin y al cabo la Ley Orgánica me otorga en cuanto que no está excluyendo los ficheros de contactos del amparo de la protección de datos, ni aún en la condición de dichos contactos como intermediarios en la relación con una persona jurídica. En definitiva, es un tema que solo los jueces podrán determinar pero mantengo que, en mi opinión los ficheros de personas de contacto más críticos y vulnerables y por supuesto, más ahora que se les ha excluido del ámbito de protección del RD.

Es muy habitual, mucho más de lo que seguramente piensan, que los empleados descarguen el listado de contactos del cliente de correo para hacer mailings en Navidad o se reutilice la información

para enviar publicidad, incluso a veces en correos electrónicos con listas abiertas de usuarios.

Es muy frecuente ver listas abiertas de contactos en los envíos masivos de correo electrónico y la cuestión es que no son datos especialmente protegidos sino un nombre, dos apellidos y una cuenta de correo electrónico pero, algunos se podrían preguntar ¿es tan grave?, en mi opinión sí. A nosotros se nos han dado casos en empresas en que muchas veces esos listados, como decía Jesús, juntaban agendas domésticas y profesionales, y a lo mejor se ha enviado un correo electrónico con una lista abierta de contactos donde había políticos porque a lo mejor la entidad es pública y tiene contacto institucional con otras entidades, por ejemplo corporativas o ayuntamientos, y resulta que se ha enviado un correo electrónico a toda una serie de destinatarios con lista abierta, que a su vez han accedido a más datos y que pueden también reutilizar; incluso muchas veces los contactos no estaban sólo en España, sino en Portugal, Iberoamérica y en otros países.

El derecho de acceso es serio: permite al afectado conocer toda la información que la empresa tiene sobre su persona, la finalidad del tratamiento y si existen o no cesiones del contenido.

Yo creo que la exclusión del reglamento no ha hecho más que complicar una situación que de por sí ya es delicada y en la que las empresas ya habían empezado a poner un orden. Ahora con la exclusión volvemos un paso atrás. Además la interpretación de la norma por las organizaciones se está haciendo en términos demasiado amplios. Mantengo que son ficheros que no tienen una especial protección de cara a la normativa porque son datos de nivel básico, pero sin embargo, están expuestos al acceso y uso de tantísimos usuarios que de alguna forma esta exclusión del reglamento ha perjudicado la labor de concienciación y de formación de los empleados y empresas en esta materia.

Y finalmente entraríamos en la última obligación –a grandes rasgos- que tienen las empresas: su responsabilidad administrativa frente a los órganos de control en materia de protección de datos.

Esa responsabilidad de la empresa se traduce en una necesidad para nosotros los abogados (tanto internos como externos) de que las organizaciones dispongan de información ordenada para contestar a requerimientos de la Agencia Española de Protección de Datos, defensa de la entidad en procedimientos sancionadores. Es decir, conocer ordenadamente de dónde se ha obtenido un dato, cuál ha sido la comunicación informativa proporcionada al afectado, por qué se ha efectuado un tratamiento o qué finalidad se le ha otorgado al

dato, etc. Esa responsabilidad administrativa que tienen las organizaciones debería conducirlas a documentar el cumplimiento de sus obligaciones en protección de datos, a disponer de procedimientos que garanticen que no se van a perder en el camino ni rastros ni pistas de cumplimiento y que se van a tener o poder utilizar después ante requerimientos de información o en procedimientos sancionadores por los abogados en defensa de los derechos de sus clientes.

Aunque no hemos entrado al detalle en la descripción de las medidas de seguridad de los ficheros, es curioso que las organizaciones tienen la obligación de clasificar la información de los ficheros manuales conforme criterios legales para posteriormente aplicar las medidas de seguridad. En mi opinión esta obligación tiene cierta lógica. Ello nos lleva en cada caso a determinar si el origen del dato, la finalidad del tratamiento y el contenido del mismo son legítimos y tienen amparo legal, a partir de lo cual se diseñan las medidas a aplicar, lo cual incluye determinar los plazos de prescripción, de posibles responsabilidades y toda una serie de criterios que ayudarán a implementar unas medidas de seguridad u otras. Entiendo que es a ello a lo que se ha querido referir el Reglamento.

Para ir terminando solo me resta decir que, al final, para que una organización pueda cumplir la Ley Orgánica de Protección de Datos y, por tanto, el Reglamento, creo que son básicas algunas circunstancias como:

Los ficheros de contactos que se tienen en las organizaciones son, para mí, los más críticos en materia de protección. He llegado a ver hasta cinco páginas de lista abierta por correo electrónico.

- En primer lugar, que se implique la alta dirección porque efectivamente nadie hace milagros. Si no hay recursos, no se puede cumplir ni esta ni otras muchas normativas.

- En segundo lugar, hay que asignar recursos, económicos si hicieran falta, pero también humanos. Yo diría que casi muchas veces los recursos humanos son mucho más importantes que los económicos. Efectivamente, tener personal que se ocupe de ello quizá supone, o crear nuevo empleo, o repartir en una persona funciones o tareas que hasta ahora no tenía: crear responsables internos en la organización, que no quede en saco roto el trabajo realizado para cumplir la normativa cada vez que un responsable abandona (por el motivo que sea) la empresa. Creo que deben nombrarse cargos y responsabilidades de forma indefinida. Al igual que la empresa paga impuestos periódicamente y está de alguna manera al tanto de cuándo cambian los tipos o los plazos, en esta materia la

empresa debería tener prácticamente la misma disposición.

- Y finalmente, hay que establecer procedimientos para el mantenimiento de un nivel óptimo de cumplimiento de la LOPD y del RD 1720: creo que con el nuevo Reglamento efectivamente si no hay procedimientos no va a poderse cumplir la normativa. Evidentemente, para las organizaciones habría una primera fase de identificación de necesidades, de creación y elaboración de medidas, jurídicas o de seguridad, una fase de implementación y finalmente el mantenimiento que no se puede olvidar.

En base a la experiencia ¿qué creo que es lo que se necesita para que funcione un proyecto de cumplimiento de la Ley Orgánica de Protección de Datos?:

- En primer lugar, que sea viable, es decir, que estemos hablando sobre realidades y sobre la circunstancia personal e individual de la empresa de la que estamos tratando.

- En segundo lugar, que se exija su cumplimiento y cuando digo que se exija el cumplimiento no digo sólo a nivel interno. A veces se crea un problema ya que la empresa cumple la normativa pero se relaciona con terceros que no cumplen la normativa y además pasa por alto el no cumplirla con tal de mantener relaciones comerciales o mercantiles con terceras partes. Este es un caso muy frecuente en los temas de contratos de prestación de servicios con acceso a datos. Es frecuente la consulta a Equipo Marzo de muchos responsables dentro de las empresas que nos comentan que "ya han enviado el contrato para firma una, dos y tres veces (por correo certificado, por burofax, etc.) y la otra parte no lo suscribe. Yo sé que pones a la empresa en una tesitura ciertamente muy difícil pero creo que la responsabilidad que se asume solo nos conduce a dos soluciones: o dejas de trabajar con ese proveedor o le mandas un requerimiento notarial (aunque sea impropio de "partes bien avenidas"). Pero, por otro lado, no es menos cierto que si una organización permite a un tercero tratar los datos de su responsabilidad para prestar un servicio y ese tercero no quiere asumir su compromiso de firmar un contrato de acceso a datos, el tercero con esta postura está manifestando que no merece la confianza del responsable y por otro lado el responsable del tratamiento no debería asumir el riesgo solidario de comisión de una infracción. En mi opinión, una de las medidas más beneficiosas de esta normativa es precisamente la del contrato de acceso a datos porque lejos de añadir obligaciones a las partes simple-

Si no hay recursos económicos y humanos, como en todo, no se puede cumplir con ésta y otras normativas. Por ello, es necesario la implicación de la dirección.

mente define responsabilidades para cada una de ellas el contrato ni añade ni quita obligaciones a las partes sino que simplemente verifica lo que establece la Ley, el reparto de responsabilidades que a cada uno incumbe, esto es, al responsable del fichero y al encargado del tratamiento.

- En tercer lugar debe impartirse formación. Creo que también es importante definir sanciones internas dentro de la organización y evidentemente valorar los riesgos. Hay muchas veces que la empresa prefiere asumir riesgos que cumplir la Ley. Pero, es importante entonces que la organización valore correctamente los riesgos que asume y analice sí realmente no hay nada que no pueda cumplir.

- Finalmente, tener todas las obligaciones y forma de cumplimiento claramente documentados sin perder de vista una cuestión muy importante: estamos respondiendo a una obligación legal y digo esto porque aunque parezca obvio hay muchas veces que las empresas y las organizaciones lo que hacen es plantearse sistemas de calidad o trabajar determinados puntos de cumplimiento solamente por obtener un certificado.

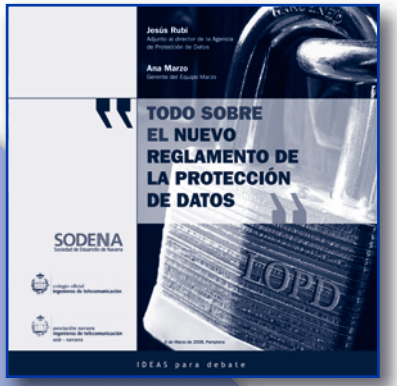
Tú, al cumplir con el contrato, estás asumiendo una norma que protege derechos fundamentales de las personas.

Yo siempre advierto de que aquí no se trata de cumplir un procedimiento de calidad (aunque nos vienen muy bien los procedimientos de calidad para cumplir la normativa sobre protección de datos). Se trata de cumplir y dar respuesta a un imperativo legal, a una norma que protege, como han dicho al inicio de la tarde, derechos fundamentales de las personas, de forma que las organizaciones deben plantearse el cumplimiento de una normativa más para la empresa o para la Administración Pública. Sí además se puede canalizar a través de procedimientos de calidad perfecto; pero lo prioritario es comprender lo que la Ley obliga.

En esta línea, solo me resta reiterar que el nuevo Reglamento exige que el responsable pueda acreditar el cumplimiento de sus obligaciones. A mi juicio el cumplimiento de la Ley está en gran medida de manos de los usuarios. Estos sólo pueden cumplir las normas si se les dota de medios y el peso de la regulación depende en gran y casi única medida de los departamentos jurídico y de sistemas de información y, sin perjuicio de que el de calidad pueda apoyar el cumplimiento a través de la incorporación de las normas de cumplimiento en los distintos procesos de la entidad.

Muchas gracias a la organización por su invitación y a los asistentes por su atención.

colección
Ideas para debate



Descargar pdf en:

www.sodena.com

SODENA

Avda. Carlos III, 36. 1º Dcha.
31003 PAMPLONA (Navarra)
Telefono: 848 42 19 42
Fax: 848 42 19 43
E-mail: info@sodena.com

Gobierno de Navarra