LA PROTECCIÓN DE DATOS PERSONALES Y LA SEGURIDAD DE LA INFORMACIÓN

Arturo Ribagorda Garnacho
Catedrático de Universidad
Director del Departamento de Informática
Escuela Politécnica Superior
Universidad Carlos III de Madrid

Bajo el punto de vista técnico, no así del legal, la protección de datos personales no es sino la seguridad de la información cuando ésta atañe a los datos de la naturaleza citada. Por ello, en el artículo se repasan las medidas de seguridad de la información con relevancia en la protección de aquellos, algunas de ellas, como el cifrado, cuya historia se remonta a siglos a.C., para mostrar después las peculiaridades de su aplicación a la materia que nos ocupa, según el Título VIII del vigente RD 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

Así, se comienza con la división clásica de las medidas de seguridad atendiendo, primero, a su forma de actuación y, después, a su naturaleza (medidas técnicas, administrativas y físicas). A continuación, se estudian las medidas técnicas más relevantes en la protección de datos: autenticación, control de accesos, cifrado de datos, registros de auditoría y borrado seguro, exponiendo tras cada una su desarrollo en el Real Decreto. Lo mismo se hace con las medidas administrativas y organizativas para concluir con la única medida de naturaleza física presente en la citada disposición legal, el control de acceso físico.

Al margen de esta exposición, a lo largo del artículo también se critican aquellos aspectos de estas medidas de seguridad que son cuanto menos discutibles en su tratamiento por el antedicho Real Decreto.

Arturo Ribagorda Garnacho

SUMARIO

1. LA SEGURIDAD DE LA INFORMACIÓN.
2. CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD.
3. LA CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD EN EL REGLAMENTO DE DESARROLLO DE LA LOPD.
4. MEDIDAS DE SEGURIDAD DE NATURALEZA TÉCNICA.
   4.1. La autenticación de usuarios.
   4.2. El control de accesos.
   4.3. El registro de auditoría.
   4.4. El cifrado de datos.
      4.4.1. Tipos de cifrado.
   4.5. Borrado seguro.
5. MEDIDAS DE NATURALEZA ADMINISTRATIVA Y ORGANIZATIVA.
   5.1. El documento de seguridad.
6. MEDIDAS DE NATURALEZA FÍSICA.
7. CONCLUSIONES.
   CITAS.

Desde tiempos ancestrales el hombre ha sido consciente del valor de la información, principalmente militar y política, que obviamente estaba condicionado al secreto de la misma. Naturalmente este secreto era más difícil de mantener si la información se plasmaba en un soporte escrito, y más aún según se iban incrementando las habilidades lectoras de los pueblos. Así, desde que en tiempos remotos el ser humano aprendió a escribir comenzó a desarrollar variados métodos de encubrimiento de lo que escribía, especialmente si ello era de naturaleza militar.

Unas veces eran procedimientos ingeniosos, pero de difícil generalización, como la escritura en el cuero cabelludo dejando tiempo para que el crecimiento del cabello ocultase lo escrito [HER 1], o en tablillas de madera que después eran cubiertas de cera [HER_2], o sobre seda envuelta en cera y luego engullida, o escritos mediante tintas simpáticas [1] (tintas aún usadas recientemente [2]), etc. Todos ellos trataban de velar el texto escrito a aquellos no autorizados a conocerlo.

Otras veces se trataba de métodos sistemáticos, antecesores remotos, pero antecesores, de métodos actuales. Es el caso de la sustitución de unas letras del alfabeto por otras distintas (como ocurre con el método César [3] [SUE], el de Polibio [4] [POL] o los atbash [5], albam [6] y atbah [7] de los judíos [KAH 67])

---

1. Composición líquida que tiene la propiedad de que no se conozca lo escrito con ella hasta que se le aplica el reactivo conveniente (DRAE, vigésima primera edición).
2. Aun siendo las tintas simpáticas conocidas desde la antigüedad, aún se empleaban en el siglo XIX (y aun el XX), por ejemplo durante las guerras carlistas.
3. Se reemplazaba cada letra por aquella situada tres posiciones por detrás en el alfabeto, dando la vuelta circularmente al llegar a aquellas últimas que no tenían letras por detrás suyo. Así, la «a» se reemplazaba por la «d», la «b» por la «e», …, y la «z» por la «c».
4. Consistía en una tabla en cuyas filas y columnas se numeraban del 1 al 5. En las entradas de la tabla se situaban las letras del alfabeto griego, sustituyéndose cada letra por el par de dígitos que encabezaban la fila y columna en cuya intersección se hallaba la letra en cuestión.
5. Véase como ejemplo: *Jeremías* 25:26, 51:41, 51:1.
6. Puede consultarse *Isaías* 7:6.
7. El Talmud proporciona varios ejemplos de este método.

o la reordenación del orden de las letras en las palabras (como la escítala [8] lacedemonia [PLU]). Métodos todos ellos cuya finalidad era encubrir el significado del texto, pero no el propio texto, que se podía ver aunque no interpretar.

Todos estos procedimientos y métodos han devenido, más o menos directamente, en otros usados en el presente y estudiados en dos disciplinas de enorme pujanza: la esteganografía y la criptografía. De ellas, la segunda juega un papel protagonista en la seguridad y en la protección de datos personales, por lo que dedicaremos cumplido espacio más adelante a sus fundamentos.

También nuestros antepasados fueron pronto conscientes de la importancia de los datos íntimos, aunque en principio solo los concernientes a la salud y la castidad eran citados en textos como merecedores de ser mantenidos a buen recaudo. Es el caso del juramento hipocrático [9], o del Kama sutra [VAT 02] que entre sus *«artes»* (prácticas que toda mujer debe conocer) recoge dos, anotadas como la 44 y 45, que recomiendan —sobre todo la última—, el aprendizaje de métodos de escritura secreta, supuestamente para ocultar a su pareja pensamientos o hechos de inconveniente conocimiento por la misma.

Siglos más tarde tenemos otra muestra, en esta ocasión en nuestro país, de la importancia que ya se concedía a los datos personales, y en esta ocasión de cualquier naturaleza, no solo los referentes a la honestidad. Nos referimos a la siguiente cita extraída de la obra de un ilustre hispanista: *«En 1581, el Rey (Felipe II) envió a un colegio de Salamanca una solicitud aparentemente simple, pidiendo le enviasen documentos confidenciales sobre un funcionario que acababa de nombrar para un consejo gubernamental. El colegio se negó. Los papeles confidenciales, alegó, eran totalmente confidenciales y ni siquiera el Rey podía violar el secreto. "Decid que a su Majestad no le obliga ningún precepto natural, que es el secreto cosa muy dura, porque en aquello todos somos yguales"»* [KAM 97].

---

8. Consistía en un bastón de radio predeterminado que era enrollado completamente por una cinta de papiro. Hecho esto se escribía el texto a ocultar escribiendo a lo largo del bastón. Bastaba con desenrollar la cinta del bastón para tener un conjunto incoherente de letras, que sólo era posible de interpretar nuevamente al volver a enrollarlo en un bastón de idéntico radio. Fue usado en primer lugar por los espartanos, de donde viene su nombre.

9. Guardaré secreto sobre lo que oiga y vea en la sociedad por razón de mi ejercicio y que no sea indispensable divulgar, sea o no del dominio de mi profesión, considerando como un deber el ser discreto en tales casos. HIPÓCRATES DE COS. Cos (s. V a.C.-s. IV a.C.).

En todo caso, es hacia mediados de la década de los setenta cuando los países más avanzados tecnológicamente y más respetuosos con las libertades individuales comienzan a reflexionar y preocuparse por el impacto que sobre la intimidad presenta la informática, y por extensión las tecnologías de la información. Así nacen las primeras leyes que tienen como objeto la tutela del derecho a la autodeterminación informativa [10] (o *habeas data*) recogido en el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948. Estas primeras normas se promulgan en Suecia y en el *land* de Hesse en la, por entones, llamada República Federal Alemana.

La situación hoy en día es la existencia en prácticamente todos los países avanzados de normas legales que, con mayor o menor empeño, amparan este derecho básico (reconocido como fundamental en nuestra Constitución, que lo recoge en su artículo 18.4 y donde se remite a un ulterior desarrollo legal). Aún más, en el caso europeo existe una directiva que ha permitido armonizar la tutela este derecho en nuestro entorno geográfico [DIR 95]. En España, la norma que transpone dicha directiva —y cumple el mandato constitucional aludido— es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (en adelante LOPD).

Naturalmente, por mucho que medidas de naturaleza legales traten de proteger un derecho tan sutil como el de la intimidad, sólo el concurso de otras medidas de seguridad permitirá garantizar unos niveles mínimos de confianza en que nuestros datos no serán conocidos, tratados o intercambiados sin contar con nuestra aquiescencia, o bien atendiendo a otros requisitos legalmente tasados. Tanto es así que el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD) califica en su preámbulo a estas otras medidas de: *«aspecto esencial para la tutela del derecho fundamental a la protección de datos».*

Por ello, se hace imprescindible volver la vista a la seguridad de la información, disciplina de carácter técnico y, en menor proporción (aunque no importancia) de carácter administrativo y organizativo para conocer y aplicar los mecanismos y procedimientos que permiten la protección de nuestros datos.

---

10. La formulación doctrinal de este derecho se realiza en 1890 por quienes pueden considerarse sus ideólogos: los juristas estadounidenses Samuel WARREN y Louis BRANDEIS. Éstos, en su tratado *The right to Privacy* [WAR 90], dan carta de naturaleza a lo que libremente traducido podríamos expresar como: *«que le dejen a uno en paz»* para caracterizar a lo que ahora a menudo se denomina autodeterminación informativa.

1. LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es una disciplina de reciente aparición [11] que trata de la protección de ésta frente a revelaciones —accidentales o intencionadas—, a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones. Así, podemos afirmar que su objetivo es el mantenimiento de la confidencialidad [12] (que sólo los usuarios habilitados puedan acceder a la información), la integridad (que la información permanezca exacta y completa) y la disponibilidad (que sólo los usuarios autorizados puedan utilizar la información en la forma y tiempo previstos) [13].

Por otro lado, la protección de datos personales trata de mantener el derecho de los individuos a determinar cuándo, cómo, a quién, qué y para qué información sobre ellos puede ser cedida a terceros, o como dice nuestro Tribunal Constitucional *«El derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»*[14]. Es por tanto una materia que requiere el concurso de la seguridad de la información, pues ésta se ocupa de la protección del dato, sea cual sea su naturaleza, lo que incluye a aquellos de carácter personal.

Así, los objetivos expuestos de la seguridad de la información: mantenimiento de la confidencialidad, integridad y disponibilidad, coinciden con los que la LOPD impone al responsable del fichero o encargado del tratamiento, que según su artículo 9, «Seguridad de los datos»: *«deberán adoptar las medidas de*

---

11. Aunque ya desde los primeros años de la informática (décadas de los cuarenta y cincuenta del siglo XX) se adoptaron medidas de seguridad, éstas se reducían a proteger aquellas máquinas frente a amenazas del medio físico, como incendios. Hay que esperar a la década de los noventa del pasado siglo para ver el desarrollo actual de la seguridad.

12. A menudo, al referirse a datos personales se habla de privacidad, en vez de confidencialidad. Más aún, cuando estos datos se corresponden con la esfera más sensible o crítica de nuestra personalidad, mejor que privacidad se usa intimidad.

13. Aunque algunos prefieren añadir a estas tres dimensiones de la seguridad: confidencialidad, integridad y disponibilidad, otras dos nuevas: la autenticación y el no repudio, es opinión mayoritaria que éstas se encuentran resumidas en las tres primeras.

14. STC 2000\292.

índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado […]». Es por tanto insoslayable para abordar la protección de los datos personales ahondar en el estudio de las medidas y mecanismos que la seguridad de la información nos proporciona, muchos de los cuales están contemplados en el RD 1720/2008, cuyo Título VIII lleva precisamente como rúbrica «De las medidas de seguridad en el tratamiento de datos de carácter personal».

2. CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD

Atendiendo a la forma de actuación (antes del ataque, durante el mismo, etc.) las medidas pueden ser de prevención (tratan de evitar que el ataque llegue a afectar al sistema), de detección (intentan descubrirlo en etapas tempranas de su ejecución), de corrección (pretenden contrarrestarlo mientras actúa) y de recuperación (tratan de restaurar el estado del sistema al que tenía antes del ataque). Ejemplos respectivos de estas medidas pueden ser, entre otros muchos, el cifrado de datos, los sistemas de control de accesos, los cortafuegos, los sistemas de detección de intrusiones (abreviados como IDS mediante sus siglas en inglés), los señuelos *(honeypot)* y los planes de contingencia, etc.

Sin embargo, si atendemos a su naturaleza, estas mismas medidas se clasifican en técnicas, administrativas y organizativas, y físicas. Las primeras se materializan en mecanismos que se implementan en el interior de los sistemas de información, y tratan de contrarrestar las amenazas que desde dentro de estos sistemas acechan a los programas y datos.

Las segundas medidas, administrativas y organizativas, se instrumentan mediante reglas y procedimientos que involucran a gestores que dictan las normas y pautas de alto nivel que incumben a la seguridad, técnicos que formulan los procedimientos que se deducen de las anteriores y usuarios responsables de cumplirlas. Son por tanto medidas que se refieren a la gestión de la seguridad.

Estrictamente existe un tercer grupo de medidas, de menor importancia, denominadas físicas, que pretenden proteger los equipos de amenazas provenientes del medio natural, del entorno operativo o de acciones humanas

deliberadas o no. Por ejemplo: incendios (contrarrestados mediante sistemas de detección y extinción), inundaciones (evitadas mediante una adecuada ubicación de los equipos y sistemas de evacuación), hurtos de soportes o equipos (controlados mediante la instalación de arcos y sistemas de alarmas), sabotajes materiales [15] (prevenidos mediante controles de accesos de personas y objetos), cortes de fluido eléctrico (soslayados mediante sistemas de alimentación ininterrumpida, abreviados por sus siglas en español, SAI, o en inglés, UPS), etc.

3. LA CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD EN EL REGLAMENTO DE DESARROLLO DE LA LOPD

Estos tres tipos de medidas están contemplados en el citado título VIII del vigente RLOPD, donde se estructun en tres niveles: básico, medio y alto, según la naturaleza menos o más sensible de los datos personales que deben proteger.

Así, los tratamientos de datos —o ficheros que contengan a éstos— relativos a infracciones penales o administrativas, o que sean responsabilidad de las Administraciones Tributarias, de las entidades financieras, de las Entidades Gestoras de la Seguridad (en estos casos siempre que estos datos se relacionen con sus potestades, prestaciones o competencias), así como otros detallados en el artículo 81.2 del RLOP se deberán custodiar con medidas de nivel medio.

Por su parte, aquellos ficheros con —o tratamientos de— datos referentes a ideología, religión, creencias, origen racial, vida sexual, salud, afiliación sindical, o derivados de actos de violencia de género o recabados con fines policiales sin consentimiento, entre otros que se precisan en el artículo 81.3, deberán dotarse de medidas de seguridad de nivel alto. Finalmente, el artículo 81.4 estable-

15. En el ámbito de la informática es frecuente referirse a los atentados a los programas o datos (que persiguen su borrado) como atentados inmateriales. Un ejemplo conocido se tiene en numerosas modalidades de virus informáticos que suprimen ciertos ficheros con determinadas extensiones o incluso formatean el disco duro para eliminar su contenido.

ce un nivel que, en sentido lato, podríamos denominar medio-alto, para los datos de tráfico y localización relativos a comunicaciones electrónicas, pues para éstos los operadores de telecomunicaciones deberán mantener las medidas de nivel medio complementadas con sólo una de las prescritas para el nivel alto, la establecida en el artículo 103, «Registro de accesos».

Estos tres niveles se aplican consecutivamente, de modo que los datos a los que corresponde proteger con medidas de nivel medio deben también dotarse de las de nivel básico. Del mismo modo, las medidas de nivel alto son todas aquellas de nivel medio —que como se ha dicho incluyen las de nivel básico— a las que se añaden otras específicas del alto. Este anidamiento de los niveles permite una más fácil aplicación de los mismos.

Es notable la matización que el vigente Reglamento ha realizado sobre estos niveles, pues establece excepciones notables —recogidas en los artículos 81.5, 81.6 y 81.8— que la experiencia acumulada de la aplicación del derogado Reglamento recomendaba [16].

4. MEDIDAS DE SEGURIDAD DE NATURALEZA TÉCNICA

Empezando por las medidas técnicas, para comprender su importancia capital en el ámbito de la protección de datos personales, basta con remitirse a lo manifestado por, la Comisión Europea en su «Primer informe sobre la aplicación de la Directiva 95/46, sobre protección de datos» [COM 03], donde puntualiza que *«la aplicación de medidas tecnológicas adecuadas constituye un complemento fundamental de los medios jurídicos y debe constituir una parte de cualquier esfuerzo destinado a obtener un grado suficiente de protección de la intimidad».*

Igualmente, la Comunicación de la Comisión sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad

16. El Reglamento derogado, RD 994/1999, de 11 de junio, desarrollaba tan sólo el artículo 9 de la también derogada Ley Orgánica del Tratamiento Automatizado de Datos de Carácter Personal, LORTAD. Por tanto, aquel Reglamento sólo se ocupaba de los datos automatizados (únicos tutelados por la LORTAD) y además se restringía a regular las medidas de seguridad, que era lo único previsto en dicho artículo 9.

(*Privacy Enhanced Technology*, PET) [COM 07] señala que un régimen de protección que contemplase sólo medidas legales podría resultar insuficiente *«cuando los datos personales se difunden por todo el mundo a través de las redes de TIC* [17] *y en su tratamiento intervienen varias jurisdicciones, a menudo fuera de la UE».* Así mismo señala que, *«gracias a dichas tecnologías, las infracciones de las normas de protección de datos y la vulneración de los derechos del ciudadano, además de estar prohibidas y sujetas a sanciones, resultarían más difíciles desde el punto de vista técnico».* Entre estas tecnologías destaca la Comunicación, los instrumentos de cifrado, el uso de anonimizadores automáticos, los anuladores de *cookies* [18], las plataformas de preferencias de privacidad (P3P) [19], etc.

Por su parte, el RLOPD, en su Título VIII, contempla expresamente varios de estos mecanismos: la autenticación (artículos 93 y 98), el control de accesos (artículo 91), el registro de accesos (artículo 103), el cifrado de datos (artículo 101 y 104), etc.

Sin duda, son muchas más las medidas existentes de naturaleza técnica no consideradas en el citado Reglamento, entre las cuales descuella la firma digital [20], a pesar de la importancia que está destinada a tener fundamentalmente por su incorporación al DNI electrónico que *«… es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular»* [21]. En todo caso, además de los existentes mecanismos son numerosas las iniciativas tendentes al desarrollo de mecanismos específicos para amparar la privacidad (aunque por extensión también se puedan usar para proteger cualquier tipo de dato, no sólo los personales).

---

17. Es usual abreviar por TIC las tecnologías de la información y comunicaciones.

18. Una cookie es un pequeño registro descargado en el ordenador de un usuario cuando se conecta a una web. Este registro va almacenando datos de la navegación por la correspondiente web para permitir una navegación más cómoda por la misma.

19. La plataforma de preferencias de privacidad P3P es un protocolo que permite a las sedes web formular sus políticas de privacidad en un formato normalizado que puede ser interpretado automáticamente por lo navegadores sin necesidad de que los usuarios lean y comprendan estas políticas para cada web que visiten.

20. Conocida como firma electrónica avanzada en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

21. Artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

4.1. LA AUTENTICACIÓN DE USUARIOS

La primera de las herramientas técnicas aludidas es la autenticación (habitualmente precedida de la mera identificación) de los usuarios. En términos del RLOPD la autenticación es el *«procedimiento de comprobación de la identidad de un usuario»* [22], es decir una actuación mediante la que el usuario corrobora ser quien se supone que es (a menudo por haber manifestado previamente su identidad). Como mecanismo de seguridad es quizás el más importante, pues una vez superado satisfactoriamente ya se puede acceder al sistema de información y aunque ya dentro de éste pueden salir aún al paso —y habitualmente así ocurre— otros mecanismos, no es menos cierto que ya dentro del mismo las posibilidades de acceder a informaciones indebidas aumentan notablemente.

La autenticación se suele materializar a través de uno —mejor, varios simultáneamente— de los siguientes sistemas (últimamente, y siguiendo la terminología anglosajona, conocidos como factores): un dato (contraseña o *pin*) que el usuario autorizado conoce (recomendablemente sólo él), un objeto que posee (como una tarjeta de banda magnética o de circuito integrado —comúnmente conocida por tarjeta-chip—) o una característica corporal suya (iris, huella dactilar, voz, etc.) [23]. O coloquialmente, la autenticación se consigue mediante algo que el usuario legitimado «sabe», «tiene» o «es». Sea como fuere, la autenticación debe garantizar la *«identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado»* [24]. Obviamente, siendo la autenticación un mecanismo tan elemental está comprendido entre las medidas de seguridad de nivel básico según el RLOPD, y por tanto aplicable a cualquier fichero o tratamiento que contenga datos personales.

De entre estos sistemas de autenticación hay uno de singular importancia —y rápida expansión— por ser, en mayor medida que los demás, a la vez su-

---

22. Artículo 5.2.b) del RLOPD.

23. También se comprenden aquí, aunque el nombre biométrico no lo sugiera, los sistemas de reconocimiento de características de comportamiento o aptitudes de los individuos como la cadencia de la pulsación de las teclas, los rasgos de la firma autógrafa, etc.

24. Artículo 93.2 del RLOPD.

jeto y objeto de la protección de datos. Se trata de la biometría, que pretende autenticar a los usuarios mediante la medición de algún rasgo corporal o fisiológico, y que permite obtener características personales de alto valor. Esta dualidad objeto-sujeto está dando lugar a numerosas controversias y estudios acerca de la licitud de su uso como instrumento de autenticación. En este sentido puede consultarse el informe 1999-0000 de la Agencia Española de Protección de Datos de título: *Tratamiento de la huella digital de los trabajadores* (25). Igualmente, la importancia de la biometría como mecanismo de autenticación y su impacto en la protección de datos motivó la elaboración de un documento monográfico de trabajo en 2003, por parte del conocido como Grupo de trabajo del artículo 29, constituido, entre otros, por los representantes de las Autoridades de control de los países integrantes de la UE (26).

Finalmente, no es posible concluir la referencia a la autenticación sin citar el documento nacional de identidad electrónico, DNI-e, una de cuyas funcionalidades es precisamente ésta. Su fiabilidad (exige dos factores: un objeto —la propia tarjeta que lo soporta— y una contraseña o característica biométrica), su modo de trabajo (en lo que no cabe entrar aquí), su alcance universal (en pocos años todos poseeremos uno), y la acelerada entrada en la sociedad de la información lo condena a convertirse en el instrumento de autenticación por excelencia (27).

Todos estos sistemas se combinan en ciertos entornos con la identificación del equipo —mediante su dirección física, IP, MAC, etc.— desde el que se desea acceder, de modo que sólo si esta dirección es correcta y la autenticación del usuario satisfactoria se concede el acceso.

---

25. Se entendió por esta Agencia Española de Protección de Datos que los datos biométricos tenían la condición de datos de carácter personal y que, dado que los mismos no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos. […]

En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado […] será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos *«se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento»* […].

26. El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales es el órgano asesor comunitario independiente sobre protección de datos y se creó en virtud del artículo 29 de la Directiva 95/46, estando fijadas sus tareas en el artículo 30 de la misma y en el 14 de la 97/66.

27. Como ejemplo, véase la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

4.2. EL CONTROL DE ACCESOS

Una vez que el usuario ha entrado al sistema —es decir, ha superado el mecanismo de autenticación— puede que trate de acceder a datos o recursos para los que no está autorizado. Para prevenir esto, el segundo mecanismo de seguridad que actúa es el control de accesos. Este mecanismo se define en el RLOPD como aquel *«que en función de la identificación ya autenticada permite acceder a datos o recursos»*. Su importancia hace que este Reglamento lo contemple entre los mecanismos de nivel básico, es decir obligatorio para cualquier sistema con ficheros de datos personales o que los trate.

Los modelos existentes de control de accesos se basan en dos principios contrapuestos. Según el primero, sólo se permite el acceso a aquellos datos y recursos que estén expresamente habilitados. Según el segundo, se permite el acceso a aquellos datos y recursos que no estén expresamente vedados. En otras palabras, el primer modelo prohíbe todo lo que no está autorizado, mientras que el segundo autoriza todo lo que no está prohibido. Estos principios se conocen como de mínimo [28] y máximo privilegio respectivamente.

Por su fiabilidad, los modelos de control de accesos imperantes son los de mínimo privilegio, pues permiten controlar mucho mejor qué usuarios acceden a qué datos o recursos. En este sentido, el RLOPD establece en su artículo 91: *«Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones».* De este modo, sólo los usuarios que para el desempeño de sus funciones requieran ineludiblemente acudir a un dato o manejar un recurso pueden hacerlo.

Para implementar esto, a cada usuario se le deben conceder derechos (o privilegios) de acceso que acoten qué puede hacer en el sistema (y por consiguiente, *sensu contrario*, qué no puede hacer).

En sistemas con multitud de usuarios se suelen crear perfiles constituidos por grupos de aquellos que comparten competencias y responsabilidades (y por

28. Principio que los autores anglosajones denominan concisa y expresivamente como de *need-to-know.*

tanto derechos de acceso), facilitando así la asignación de privilegios a cada usuario, pues basta adscribirlo a un grupo (perfil) para que automáticamente herede los privilegios del mismo. Esta práctica está tan extendida que se recoge en el RLOPD, cuyo artículo 5 define Perfil de usuario como *«Accesos autorizados a un grupo de usuarios».*

4.3. EL REGISTRO DE AUDITORÍA

El registro de auditoria, conocido por el RLOPD como registro de accesos, es un mecanismo ofrecido por los sistemas para recoger los datos de los accesos, intentos de acceso y tratamientos realizados. Por consiguiente, analizando este registro, es posible detectar quiénes y desde dónde acceden, cuándo y cómo lo han hecho, y qué acciones se han realizado. Es por tanto un mecanismo meramente disuasorio —siempre y cuando los usuarios sepan de su existencia— y no preventivo, lo que no disminuye su eficacia, sobre todo si se conserva durante un tiempo prudencial.

Todos los sistemas operativos mantienen un registro de auditoría, aunque no sea capaz de matizar más que quién y cómo ha accedido y a dónde lo ha hecho, sin precisar ulteriores detalles. Así, no es posible con este registro conocer qué datos se han tratado dentro del recurso accedido, por ejemplo una base de datos. Por ello algunos programas, por ejemplo las citadas bases de datos, mantienen sus propios registros, que recogen estos movimientos y permiten detectar cambios indebidos y los usuarios que los han realizado.

Desafortunadamente, es un mecanismo de mantenimiento complejo, por lo que el RLOPD lo reserva para los ficheros y tratamientos de nivel alto, tasando los datos que debe recoger de los accesos o intentos de acceso y estipulando un plazo de conservación de dos años. Este plazo crea fuertes quebraderos de cabeza a los responsables de sistemas de grandes empresas que deben salvar estos registros periódicamente para evitar su destrucción (antes de los dos años) debido al llenado de los mismos.

Precisamente por la dificultad de su llevanza, el RLOPD establece una notable excepción (no incluida en el Reglamento derogado) al deber de mantenimiento de este registro, que no será preciso cuando concurran las dos

circunstancias siguientes: que el responsable del fichero sea una persona física y que garantice que solo él tiene acceso y trata los datos personales [29]. Es una excepción que alivia las tareas de, entre otros, médicos o abogados que ejercen libremente su profesión. Así y todo, el mantenimiento durante dos años de estos registros por parte del resto de responsables parece una carga desproporcionada, más aun cuando otras normas legales cuya justificación es la seguridad pública sólo imponen la reserva de estos registros durante un tiempo sensiblemente menor. Es el caso de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, donde se prescribe la conservación de datos de tráfico y localización sólo durante un año [30].

4.4. EL CIFRADO DE DATOS

El cifrado [31] de datos, como instrumento para encubrir informaciones ha venido siendo usado desde tiempos ancestrales, aunque hasta hace escasos cuarenta años su uso ha estado restringido a ámbitos rodeados de un halo de misterio —servicios de inteligencia, diplomáticos, de seguridad— lo que ha hecho de esta herramienta una gran desconocida, a pesar de su antigüedad e importancia, por amplios sectores de la sociedad. No obstante, la irrupción de la era de la información lo ha convertido en un útil de ocultación omnipresente usado, a menudo inadvertidamente, en numerosas acciones cotidianas: emplear un teléfono móvil, hacer un reintegro de un cajero, pagar con una tarjeta de crédito o débito, introducir una contraseña en un ordenador, acceder mediante una conexión segura, https, a un servidor —por ejemplo, de un banco—, etc.

Al tiempo, la disciplina en la que se encuadra el cifrado, denominada criptografía [32] (del griego *kriptos* oculto y *grafía*, trazo o escritura) ha tomado carta

---

29. RD 1720/2008. Artículo 103. Registro de accesos.

30. La Directiva 2006/24 que esta Ley transpone deja al arbitrio de los países la determinación precisa del periodo de retención de datos, que sólo prescribe debe estar comprendida entre seis y veinticuatro meses.

31. Algunos prefieren el malsonante anglicismo encriptado (afortunadamente no recogida por la Real Academia) proveniente del no menos horroroso encriptar, a su vez transposición del inglés *to encrypt*, en vez del castellano cifrar (y cifrado), usada ya por los clásicos de nuestra Edad de Oro.

32. Definida como la disciplina que estudia los principios, métodos y medios de transformar los mensajes para ocultar su significado.

de naturaleza en las universidades, y son numerosos los acontecimientos científicos que la tienen como protagonista [33].

Además, si bien en un principio el cifrado tenía como único fin la ocultación de información, es también usado en la actualidad para mantener la integridad, y a través de la firma digital (que no es sino un proceso de cifrado), un medio de realizar la autenticación (como ya se indicó) y evitar el no repudio de los signatarios.

En cuanto a su estructura, un sistema criptográfico está compuesto, en un extremo, por un emisor de información y por un dispositivo cifrador controlado por un número denominado clave de cifrado. En el otro, por un dispositivo descifrador, así mismo controlado por una clave de descifrado y por un receptor de la información. Por tanto, es un sistema que presenta una gran simetría, más aún si se tiene en cuenta que (en caso de transmisión de la información, no así de almacenamiento) los papeles de emisor y cifrador, y descifrador y receptor, están permutándose continuamente, ya que una vez transmite uno y recibe el otro y un instante después la situación es la contraria. Tanto el cifrador como el descifrador implementan un algoritmo matemático muy complejo y pueden instrumentarse en un dispositivo *hardware*, como ocurre en los teléfonos móviles, o, más a menudo, un *software*, como sucede con los navegadores de los ordenadores, que permiten conexiones seguras —cifradas— con servidores. Finalmente, la información antes de transformarse en el cifrador se adjetiva de *«en claro»,* y así se escribe mensaje en claro, contraseña en claro, base de datos en claro, etc. [RIB 97]. Sin embargo, tras pasar por el cifrador el predicado que se usa es *«cifrado».* De ese modo, se menciona mensaje cifrado, contraseña cifrada, base de datos cifrada, etc. [RIB 97].

4.4.1. Tipos de cifrado

Atendiendo a las claves de cifrado y descifrado, los sistemas criptográficos reciben el nombre de simétricos —o de clave secreta— y asimétricos —o de

33. Como se apuntó anteriormente otra disciplina muy vinculada a la criptografía es la esteganografía, que trata de velar el propio mensaje en vez de ocultar su significado. Como también se indicó, las tintas simpáticas han sido su principal instrumento durante muchos siglos.

clave pública— [MOR 94]. En los primeros, las claves de cifrado y descifrado son iguales, mientras que en los segundos son diferentes y, sobre todo, de la una no es posible computacionalmente hablando (es decir, salvo que se tengan infinitos recursos) obtener la otra. Estos últimos sistemas son conocidos desde hace treinta años y adquieren una importancia capital por ser la base de la firma digital [34].

Naturalmente, el mecanismo de cifrado no podía estar ausente del RLOPD, donde figura expresamente en los artículos 101, «Gestión y distribución de soportes», 104 «Telecomunicaciones» (ambos correspondientes a las medidas de seguridad de nivel alto), y tácitamente en los artículos 93, «Identificación y autenticación» (medida comprendida entre las de nivel básico) y 102, «Copias de respaldo y recuperación» (medida comprendida entre las de nivel alto).

En el primero de dichos artículos se obliga al cifrado cuando los datos estén contenidos en un soporte que vaya a ser distribuido, o bien cuando se hallen en dispositivos (por ejemplo, ordenadores portátiles) *«cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero»,* indicando además que debe *«evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado».* El artículo segundo de los citados, el 104, impone el cifrado cuando los datos de carácter personal vayan a transmitirse a través de redes públicas o redes inalámbricas [35].

4.5. BORRADO SEGURO

Un último mecanismo de seguridad de importancia en la protección de datos es el borrado seguro. Como es sabido, la simple operación de eliminar o suprimir un fichero (mediante la mera pulsación de la tecla DEL, SUPR, etc.) no borra los datos correspondientes, sino que tan sólo marca el espacio ocupado por ese fichero en el soporte de almacenamiento como libre, y por tanto candidato a ser

34. Realmente también son muy usados como medio para transportar confidencialmente claves secretas.

35. La redacción de este artículo se ha mejorado respecto del derogado Reglamento, precisándose que es exigible el cifrado cuando la transmisión se haga por redes públicas (el adjetivo no figuraba en el extinguido Reglamento, lo que dejaba la duda de si la transmisión por redes de área local cableadas debía cifrarse) y añadiéndose las redes inalámbricas, como las redes locales de tecnología Wi-Fi o bluetooth, tan comunes hoy en día.

ocupado por nuevos archivos o documentos. Por tanto, es fácilmente recuperable con sencillas y numerosas herramientas al alcance de cualquiera.

Además, hoy en día una de las mayores amenazas a la información almacenada en equipos y soportes es el desecho de los mismos al término de su vida útil, pues usualmente se abandonan o donan manteniendo intactos sus datos o simplemente eliminándolos mediante una pulsación del ratón. Así, los medios de comunicación publican noticias de la aparición de datos personales en ordenadores donados por empresas a ONG, y por éstas entregados a sectores o colectivos de países subdesarrollados. O simplemente ordenadores abandonados en contenedores o revendidos al resultar obsoletos. A mayor abundamiento, algunos estudios de campo llegan a concluir que un tercio de estos ordenadores abandonados contienen en sus discos duros informaciones valiosas, casi siempre datos de carácter personal.

Otro tanto sucede con todo tipo de soportes (DVD, lápices de memoria, etc.) abandonados en papeleras, perdidos por sus propietarios o sustraídos por descuideros.

Para contrarrestar estos riesgos, la seguridad de la información pone a nuestra disposición numerosos programas que permiten un borrado seguro. Todos ellos sobrescriben el espacio ocupado por el fichero a eliminar con patrones aleatorios de ceros y unos. Para mayor confianza en la eliminación, esta sobreescritura se puede repetir varias veces, aunque ello comporta un mayor tiempo de proceso [36]. En algunos casos se puede recurrir a la destrucción física del soporte, como sucede con los CD's o DVD's, que pueden ser triturados en numerosos modelos de destructoras de papel.

5. MEDIDAS DE NATURALEZA ADMINISTRATIVA Y ORGANIZATIVA

Las medidas más relevantes para la seguridad son las denominadas administrativas y organizativas, responsables de la gestión de la seguridad. Ello es

36. Un popular y fiable programa que permite esto (además del cifrado y la firma digital) es el PGP, desarrollado por Phil ZIMMERMAN en 1991 y convertido desde entonces en el más conocido y prestigioso programa *freeware* de cifrado (<http://www.pgpi.org>).

así pues, contrariamente a lo que piensan los muy consagrados a la técnica, las medidas de esta índole sin el acompañamiento de una adecuada gestión no sólo pueden inútiles, sino incluso contraproducentes por la sensación de falsa seguridad (el tan manido: *«eso aquí no puede ocurrir»*) que su implantación suscita entre usuarios y responsables.

Estas medidas (mucho más numerosas que las de naturaleza técnica) se plasman mediante multitud de procedimientos y de acciones entre las que descuellan: la clasificación de la información, la asignación de responsabilidades, la concienciación en seguridad (para los más involucrados en el manejo de informaciones, mejor formación), la elaboración y el mantenimiento de planes de contingencia, la realización de análisis de riesgos y ulterior gestión de los mismos, la creación de la función de seguridad, etc.

Comenzando por la primera de las medidas citadas, resulta obvio lo difícil que resulta proteger adecuadamente los datos si no se conoce su grado de sensibilidad, para lo cual es preciso proceder a su clasificación. Ésta es una tarea laboriosa, que no sólo requiere analizar todas las informaciones manejadas, sino también su etiquetado (virtual si están en formato electrónico), la determinación de los órganos decisorios de esta clasificación, la identificación del personal que puede acceder según a qué nivel de clasificación, la elaboración de normas de almacenamiento, distribución y destrucción —o desclasificación cuando su valor haya decaído—, etc. Por ello, se requiere una decidida voluntad de los órganos directivos para llevar a cabo un plan de este tipo en cualquier entidad pública o privada. Respecto de los niveles, en el ámbito del Estado cabe citar a título indicativo que la vigente Ley de Secretos oficiales [37] reconoce sólo dos, que de menor a mayor sensibilidad son: reservado y secreto. Sin embargo, la Decisión del Consejo [38] por la que se adoptan las normas de seguridad del Consejo reconoce otros dos: difusión limitada y confidencial, por lo que en realidad son cuatro los niveles actuales de clasificación en la Administración General del Estado, que de menor a mayor criticidad son: difusión limitada, confidencial, reservado y secreto.

---

37. Ley 9/1968, de 5 de abril, Reguladora de los Secretos Oficiales, modificada por Ley 48/1978, de 7 de octubre.

38. Decisión del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo (2001/264/CE).

Naturalmente, una medida tan relevante como la expuesta debía tener cabida en el ámbito de protección de los datos personales, y efectivamente así se recoge —indirectamente— en el RLOPD donde, como ya se ha reseñado, lo que se clasifican son las medidas de seguridad según los tipos de datos que deban proteger. Así, el RLOPD divide las medidas en básicas, medias y altas, lo que por extensión permite denominar a los datos que deben ser protegidos por las primeras, de nivel básico, y medio y alto a los datos que respectivamente deben custodiarse mediante las segundas y terceras.

Por lo que respecta a la asignación de responsabilidades y a la formación del personal, ambas se hallan reflejadas en el RLOPD, concretamente en su artículo 89, «Funciones y obligaciones del personal», donde se indica que el responsable del fichero o tratamiento informará al personal de *«las consecuencias en que pudiera incurrir en caso de incumplimiento»* (de las normas de seguridad). Además de detallar las obligaciones del responsable del fichero en cuanto a la información de las medidas de seguridad implantadas que debe proporcionar al personal.

El plan de contingencia es una medida de seguridad que permite restituir al sistema de información a la situación anterior a la ocurrencia de un incidente [39]. Aunque tal no está previsto, con esta extensión, en el RLOPD, si que figura el elemento primordial del plan: las copias de seguridad, desglosadas en copias de respaldo y de recuperación. Las primeras vienen definidas en el artículo 5.e) como: *«copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación».* Sin embargo, incomprensiblemente, no define las segundas, que debemos convenir se refieren a las copias de los procedimientos y programas (no datos) que permiten volcar de nuevo en el sistema y hacer operativos los datos de las copias de respaldo. La obtención y conservación de estas copias viene regulada en los artículos 94 (para las medidas de nivel básico) y 102 (para las de nivel alto).

La función de seguridad aparece contemplada en la figura del responsable de seguridad, que debe crearse allí donde se deban instaurar medidas de nivel

39. Estrictamente se pueden definir como la: Definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización [RIB 97].

medio. Aunque con atribuciones muy reducidas, esta figura se asemeja a la del director de seguridad de cualquier organización. Así, mientras éste se responsabiliza de la determinación de las medidas a aplicar, su implantación y mantenimiento, el responsable de seguridad previsto en el RLOPD se encarga sólo, según el artículo 5, *«de coordinar y controlar las medidas de seguridad aplicadas»,* aunque ello no excluye que el responsable del fichero le asigne otras funciones. En cualquier caso, según se establece expresamente en el artículo 95, el nombramiento de responsable de seguridad, sea con las funciones exclusivas de coordinar y controlar o con otras conferidas por el responsable del fichero, *«no supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento».*

También el establecimiento de un registro de incidencias y la elaboración de unas reglas para su mantenimiento es una medida de naturaleza administrativa, cuya revisión periódica resulta muy útil para conocer los riesgos más prevalentes en una instalación específica (que a menudo no son los más presupuestos ni previsibles) y extraer las consecuencias de los mismos.

Esta medida se prevé en los artículos 90 (para las medidas de nivel básico) y 100 (para las de nivel alto). En el primero se precisan los datos a registrar (suceso, hora, quién notifica), el responsable de su anotación, los efectos consecuentes al suceso y las medidas correctoras. Mientras, el segundo impone consignar en el registro, entre otros, los procesos de recuperación, si son precisos, y quien los ejecutó.

La revisión de las medidas de seguridad implantadas y su nivel de cumplimiento, o sea la auditoría de seguridad, es también considerada como una medida de seguridad más. Aunque lo ideal es que estas auditorías se realicen por profesionales ajenos a la entidad para así garantizar —o disipar dudas acerca de— la imparcialidad de los resultados obtenidos, es también frecuente que se combinen auditorías realizadas por personal interno con otras ejecutadas por auditores contratados. Por ejemplo, si se establece la realización de auditorías anuales, cada dos o tres años podrían ser llevadas a cabo por personal externo y las restantes veces por empleados debidamente formados en las técnicas y reglas propias de este campo. Naturalmente, si no se dispone de los conocimientos necesarios —y no triviales— es evidente que la auditoría debería abordarse mediante un contrato de servicios con una empresa especializada.

Las auditorías de seguridad están reconocidas en el artículo 96 del RLOPD, donde se establece que su periodicidad debe ser bienal, salvo que se realicen modificaciones sustanciales del sistema de información *«que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas»* (artículo 96.1), en cuyo caso la auditoría deberá realizarse con carácter extraordinario. Además, se dictan instrucciones acerca del análisis del informe de auditoría y las consecuencias derivadas del mismo.

Sin embargo, sí se puede reprochar al RLOPD no haber concretado, siquiera someramente, el perfil del auditor (que sí se caracterizaba en sucesivos borradores del Reglamento, aunque desapareció en el RD aprobado), pues pudiéndose efectuar las auditorías por personal del responsable del fichero (no se impone lo contrario) es de temer que éstas sean ejecutadas por individuos escasamente —si algo— preparados para un proceso tan complejo como lo es el que nos ocupa, y con las consecuencias consiguientes que tal puede acarrear.

5.1. EL DOCUMENTO DE SEGURIDAD

Entre las medidas de esta naturaleza administrativa y organizativa recogidas en el RLOPD sobresale el «Documento de seguridad» al que se dedica todo un capítulo, el segundo, del título octavo. En contra de lo que algunos piensan, no se trata de un plan de seguridad en sentido estricto (aunque tiene aspectos comunes con éstos), pues no cubre el ciclo clásico de la planificación (planificar —diseñar—, hacer —implementar—, actuar —supervisar— y comprobar —mantener—) [UNE 07], careciendo además de previsiones de futuro (respuesta ante previsibles nuevas amenazas, inversiones, calendario, etc.). No obstante, tiene elementos comunes con un plan de seguridad de la información y, al igual que éste, debe ser un documento de carácter reservado [40], circulando sólo entre aquellos directamente implicados en su desarrollo y mantenimiento, además de estar a disposición de los inspectores de la

40. Aunque no se llega a calificar tan estrictamente, al menos el RLOPD reconoce, en su artículo 88.2 *(in fine)* que *«En todo caso, tendrá el carácter de documento interno de la organización»,* recomendación que no tenía cabida en el derogado Reglamento.

Agencia Española de Protección de Datos [41] o de los Órganos de Control de las CC.AA. Ello es así pues su revelación permitiría conocer en detalle la ubicación, características, etc., de los recursos que tratan los datos, así como las medidas de seguridad aplicadas.

Entrando en el contenido, este Documento debe comprender todos los recursos que tratan los datos personales (físicos, programas y personal), especificar estos datos y las medidas y mecanismos que los protegen. Adicionalmente, debe documentar los aspectos administrativos ya vistos: gestión de incidencias, los procedimientos de obtención de copias de seguridad, la gestión y distribución de soportes y documentos, responsable de seguridad, etc.

Pero el aspecto más relevante de este Documento son las responsabilidades del personal en lo que atañe a la protección de datos, que aparecen pormenorizadas en el artículo 89. Lamentablemente, es uno de los puntos más incumplidos, siendo no obstante los usuarios —por negligencia o malicia— el eslabón más débil de la cadena que constituye la seguridad, y en última, o primera, instancia sobre ellos (nosotros) recae la mayor responsabilidad de los incidentes relacionados con la seguridad [RIB 03].

De hecho, son muy pocos los responsables del fichero que, de conformidad con dicho artículo, tienen definidas y documentadas en el Documento las funciones y obligaciones de su personal en lo que atañe a la protección de datos. Pero aún son muchos menos los que han adoptado programas de sensibilización para que sus usuarios conozcan *«de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento»,* según prescribe el artículo 89. Y sin embargo, los humanos no entendemos los ordenadores, lo que hacen y cómo lo hacen, y mucho menos imaginamos los riesgos que comporta su uso, lo que explica que hasta el 70% de los incidentes de seguridad sean imputables a los usuarios. Por ello, sin programas de formación o sensibilización, difícilmente alcanzaremos a proteger convenientemente los datos personales, como bien se establece en una reciente Resolución del Consejo de la Unión Europea [RES 03], una de cuyas acciones

41. Artículo 28.1 del RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

recomienda a la industria y a todos los usuarios a que entablen con los Gobiernos un diálogo de desarrollo de una cultura de la seguridad.

6. MEDIDAS DE NATURALEZA FÍSICA

Como se señaló ya, estas medidas tienden a proteger a los sistemas de información, sus sistemas auxiliares (suministro de energía eléctrica, acondicionamiento de aire, etc.) y entorno operativo (salas de ordenadores, almacenes de soportes, etc.) de las amenazas que provienen del medio natural o de acciones humanas de naturaleza no informática, sean deliberadas o accidentales.

Son las medidas más antiguas de entre las que protegen los sistemas de información y se materializan en multitud de equipos y sistemas. Por ejemplo, los incendios, un problema latente en lugares con equipos consumidores de energía eléctrica y rodeados de materiales inflamables, se contrarrestan mediante sistemas de detección, alarma y extinción de incendios. Las inundaciones, una amenaza de más frecuente materialización que los incendios, se previenen por una correcta ubicación de los equipos y mediante sistemas de alerta y desagües.

Los hurtos, más raramente robos, y sabotajes materiales se compensan a través de arcos de detección de objetos y control físico de las personas que intentan acceder a los lugares donde se hallan los equipos y soportes de información.

Los cortes de fluido eléctrico, mediante la instalación de sistemas de alimentación ininterrumpida (abreviados por sus siglas en español, SAI, o en inglés, UPS), acompañados, en instalaciones críticas, por grupos electrógenos. La emanación de radiaciones electromagnéticas, un riesgo muy sensible en locales de alta seguridad (embajadas, locales de los servicios de inteligencia, instalaciones militares críticas) se amortigua o evita mediante el apantallado de salas o bien con equipos (ordenadores, pantallas, impresoras, escáneres, etc.) dotados de la certificación Tempest, que avala el mantenimiento de las radiaciones en un determinado nivel.

Como se habrá observado muchas de estas amenazas pueden ser de origen humano, y casi siempre el requisito para perpetrar el correspondiente ataque es acceder a la ubicación donde se encuentran los sistemas de información.

Por ello, una primera medida —que no debiera ser la única— para la prevención de ataques como los expuestos es la implantación de medidas que impidan acceder, salvo autorización, a aquellos locales que alberguen equipos informáticos.

Pues bien, estas medidas que impiden u obstaculizan la entrada en locales de tratamiento o almacenamiento de datos son las únicas de naturaleza física que contempla el RLOPD. En efecto, el artículo 99 del mismo, «Control de acceso físico», establece que *«Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información».*

No obstante ser el control de accesos una protección oportuna, la redacción del artículo es muy desafortunada, pues a menudo los equipos que cita son ordenadores personales situados en locales de acceso público, siendo de imposible cumplimiento lo preceptuado salvo que la autorizado del Documento sea genérica para todo el público que incidentalmente pueda acudir a aquellos locales.

Basta con pensar en los ordenadores instalados en las consultas de los Centros de Salud u Hospitales, o los situados en los bufetes de abogados o en los despachos del personal al servicio de los Juzgados, para comprender la inviabilidad de tal mandato, que hubiese más razonable de haber condicionado el acceso sólo a los locales con servidores o grandes sistemas con datos personales.

7. CONCLUSIONES

Como resumen se debe reseñar que el derecho fundamental a la protección de datos personales sólo se puede satisfacer —además de con disposiciones orden legal— con el concurso de las medidas que la disciplina de la seguridad de la información pone a nuestra disposición, tanto las de índole técnico como administrativo y organizativo o físico.

Sin ellas difícilmente podremos tutelar dicho derecho, ni dar confianza a la sociedad en las tecnologías de la información que tan aceleradamente nos están permitiendo entrar en esta nueva era denominada del conocimiento y con más propiedad —por ahora— de la información.

CITAS

[COM 07] *Comunicación de la Comisión al Parlamento europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad.* COM(2007) 228 final.

[COM 03] *Primer informe sobre la aplicación de la Directiva 95/46, sobre protección de datos.* Bruselas, 15-5-2003. COM(2003) 265 final.

[DIR 95] *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

[GPD 03] *Documento de trabajo sobre biometría (Adoptado el 1 de agosto de 2003).* Artículo 29. «Grupo de Protección de Datos». 12168/02/ES. WP 80.

[KAM 97] KAMEN, Henry: *Felipe de España*, Siglo veintiuno de España editores, 1997.

[KAH 67] KAHN, David: *The Codebreakers: The Comprehensive History of of Secret Communication from Ancient Times to the Internet*, Scribner, 1967 (ed. revisada 1996).

[HER 2] <http://es.wikisource.org/wiki/Los_nueve_libros_de_la_Historia:_ Libro_VII> (consultado: 13/04/2007).

[HER 2] <http://es.wikisource.org/wiki/Los_nueve_libros_de_la_Historia:_Libro_V> (consultado: 13/04/2007).

[MOR 94] MORANT, J.L.; RIBAGORDA, A; SANCHO, J.: *Seguridad y Protección de la Información*, Editorial Centro de Estudios Ramón Areces, Madrid, 1994 (Primera reimpresión, agosto de 1997).

[POL] POLIBIO: *Historia Universal* (3 vols.), Editorial Iberia.

[PLU] PLUTARCO: *Vidas Paralelas* (libro IV), Editorial Gredos.

[RES 03] *Resolución del Consejo de 18 de febrero de 2003 sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información* (2003/C 48/01).

[RIB 03] RIBAGORDA, A.: «El factor humano en la protección de datos personales», *Revista datospersonales.org*. Agencia de Protección de Datos de la Comunidad de Madrid, número 1, marzo de 2003.

[RIB 97] RIBAGORDA, ARTURO: *Glosario de términos de seguridad de las T. I.,* Editorial CODA, Madrid, 1997.

[SUE] SUETONIO: *Vida de los Doce Césares*, Espasa-Calpe.

[VAT 02] VATSAMI, Ivor (recopilador): *Kama sutra de Vatsyâyâna*, Círculo Latino, Barcelona, 2002.

[UNE 07] UNE-ISO/IEC 27001. *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.* ISO/IEC 27001:2005

[WAR 90] WARREN, S. y BRANDEIS, L.: «The Right to Privacy», *Harvard Law Review*, Vol. IV, 15 de diciembre de 1890, núm. 5.