Las obligaciones de los responsables y de los encargados del tratamiento

PID_00250222

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Antoni Roig

Índice

1. El cambio de paradigma del principio de responsabilidad proactiva..... 5

2. Obligaciones previas al tratamiento..... 7
2.1. Evaluaciones de impacto sobre la protección de datos y consulta previa 7
2.2. Protección de datos desde el diseño y por defecto 12

3. Obligaciones durante el tratamiento..... 19
3.1. Registro y documentación de las actividades de tratamiento 19
3.2. Seguridad del tratamiento 20
3.3. Confidencialidad 21
3.4. Tratamientos de datos de menores 21
3.5. Notificación y comunicación de violaciones de seguridad 22

4. Obligaciones después del tratamiento: cooperación con la autoridad de control..... 25

Bibliografía..... 27

1. El cambio de paradigma del principio de responsabilidad proactiva

El responsable del tratamiento lo será por el cumplimiento de los principios de protección de datos (licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e integridad y confidencialidad), pero también por su obligación de demostrar su cumplimiento efectivo: responsabilidad proactiva. El registro del fichero, que en el pasado ha constituido el centro de gravedad del cumplimiento de la normativa de protección de datos, se ve ahora desplazado por las obligaciones del responsable, que deberá ahora no solo cumplir con el RGPD, sino además poder demostrarlo (art. 5.2 RGPD). En varios considerandos del RGPD, el legislador europeo se muestra crítico con el deber general de notificación a las autoridades del control de la Directiva 95/46/CE[1] (Kuner, 2012, vol. 6, págs. 1-15). En su lugar, deberán adoptarse medidas técnicas y organizativas más eficaces para los casos de tratamiento que entrañen un alto riesgo para los derechos de los interesados[2] (López, 2016, págs. 282-285). Como veremos, se impone la obligación de llevar registros de las actividades del tratamiento, evaluaciones de impacto y un número ampliado de obligaciones generales para el responsable y el encargado.

(1)Esto es expresamente manifestado en el considerando 89 del RGPD y, quizá, de manera indirecta en los considerandos 51 y 73.

(2)Quizá el legislador nacional pueda prever la notificación de los tratamientos sobre los ficheros que contengan datos especiales o que sirvan a objetivos de interés público general de la Unión Europea o de un Estado miembro.

Lecturas recomendadas

L. F. López (2016). «La responsabilidad del responsable». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 282-285). Madrid: Ed. Reus.

C. Kuner (2012, febrero). «The European Commission's proposed data protection regulation: A Copernican revolution in European data protection law». *Bloomberg BNA Privacy and Security Law Report* (vol. 6, págs. 1-15).

Esta nueva perspectiva, unida a la exigencia de prever y adaptar las medidas al nivel de riesgo para los derechos, incorpora por primera vez los escenarios más delicados para la protección de datos: organizaciones que manejan datos de millones de interesados, que en algunos casos pueden involucrar información personal sensible o consistir en un volumen de datos muy importante sobre cada afectado[3]. Esto supone unas obligaciones ampliadas, que empiezan ya antes del tratamiento, se prolongan durante el mismo e incluso se mantienen una vez que este ha concluido.

(3)Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos y Agencia Vasca de Protección de Datos (2016), *Guía del Reglamento general de protección de datos para responsables de tratamiento.* Puede ampliarse con el libro de E. Gil (2016).

Así, en la fase previa al tratamiento, el responsable deberá valorar la posibilidad de proteger los datos mediante el diseño (*privacy by design*) o por defecto (*privacy by default*). Durante el tratamiento, sus obligaciones consistirán, como veremos, en llevar un registro y documentación de las actividades de tratamiento, asegurar los datos y el tratamiento, confidencialidad y notificar y

comunicar las eventuales brechas de seguridad que se hayan producido. Una vez finalizado el tratamiento, el responsable sigue obligado a cooperar con las autoridades de control.

El responsable deberá elegir, como hemos visto, al encargado o encargados que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas adecuadas, de manera que se garantice y se pueda demostrar que el tratamiento es acorde a los dictados del RGPD. Para demostrar que el encargado ofrece las garantías requeridas, este se podrá adherir a códigos de conducta o certificarse de acuerdo con el RGPD, como veremos. Por otro lado, cabe mencionar que la Directiva 95/46/CE no contenía obligaciones expresamente dirigidas a los encargados, como en cambio sí contempla el RGPD. Ahora bien, la responsabilidad última recae en el responsable.

Las relaciones entre el responsable y el encargado se formalizarán en un contrato o acto jurídico vinculante. El contenido mínimo del contrato de encargo incluirá[4]:

- Objeto, duración, naturaleza y finalidad del tratamiento.
- Tipos de datos personales y categorías de interesados.
- Obligación del encargado de tratar los datos personales siguiendo las instrucciones del responsable.
- Condiciones para la autorización del responsable a hipotéticas subcontrataciones.
- Asistencia al responsable.

(4)La AEPD y las autoridades de protección de datos autonómicas han adoptado unas directrices transitorias sobre los contratos entre responsable y encargado, hasta que resulte aplicable el RGPD. Una vez que este último sea aplicable, la AEPD podrá adoptar cláusulas modelo que deberán ser aprobadas por el Comité Europeo de Protección de Datos. La Comisión Europea también podrá adoptar cláusulas contractuales modelo.

2. Obligaciones previas al tratamiento

2.1. Evaluaciones de impacto sobre la protección de datos y consulta previa

1) Evaluaciones de impacto

El RGPD ha acentuado la «aproximación basada en el riesgo» (*risk-based approach*) incluida ya, aunque con menor calado, en la Directiva 95/46/CE. Se trata de un elemento clave del nuevo principio de responsabilidad proactiva del art. 5.2 RGPD (*accountability*). Pues bien, en este contexto cobran especial importancia las evaluaciones de impacto en la protección de datos, o su casi equivalente anglosajón *privacy impact assessment* (PIA).

Lecturas recomendadas

Si queréis profundizar en el tema de la aproximación basada en el riesgo, podéis leer los siguientes trabajos:

M. Recio (2016). «Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 351-366). Madrid: Ed. Reus.

Grupo de trabajo del artículo 29 (2016, febrero). *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR).*

***WP29 Guidelines** on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679*. Aprobado el 4 de abril del 2017 (WP 248).

Centre for Information Policy Leadership (2014). «The role of risk management in Data Protection». *Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy* (23 de noviembre).

Se trata de «una metodología para evaluar el impacto en la privacidad de un proyecto, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos[5]. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iniciales que sea posible, cuando todavía hay oportunidades de influir en el resultado del proyecto»[6].

(5)La obligación de desarrollar PIA o DPIA en algunos casos (art. 35 RGPD) tiene notables implicaciones para la teoría general de la regulación. En efecto, parece claro que no se trata de una técnica de autorregulación, pues la obligatoriedad de cumplir con los contenidos del RGPD se impone. Tampoco es claramente una corregulación, pues el responsable no es propiamente un regulador. Por ello, la especial posición del responsable, debida al principio de responsabilidad, ha llevado a algún autor a considerar la DPIA como un supuesto de metarregulación (Binns, 2017, págs. 22-35).

(6)Wright y De Hert (2012) y Tancock, Pearson y Charlesworth (2013, págs. 73-123). El origen de los PIA parece estar relacionado con los análisis de impacto medioambiental, con los cuales comparten, en parte, la metodología. Junto con la AEPD, otras agencias han adoptado guías o documentos sobre PIA. Por ejemplo, la Commission Nationale de l'Informatique et des Libertés (CNIL) francesa ha publicado varios documentos: *PIA manual 1 - Methodology (How to carry out a PIA)*, *PIA Manual 2 -Tools (Templates and knowledge bases)* y *PIA Manual 3 - Good practices*. También puede consultarse el Dictamen 9/2011, del grupo de trabajo del artículo 29, relativo a la propuesta revisada de la industria para un marco de evaluación de impacto sobre la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia (RFID), adoptado el 11 de febrero del 2011; así como la Recomendación 2014/724/UE de la Comisión, de 10 de octubre del 2014, relativa al modelo de evaluación de impacto sobre la protección de datos para redes inteligentes (*smarts grids*) y para sistemas de contador inteligente (*smart metering*), de 18 de octubre del 2014. ISO/IEC 29134 (2017), *Information technology - Security techniques - Guidelines for privacy impact assessment*.

Concretamente, las características generales de toda evaluación de impacto en la protección de datos serían (AEPD, 2014):

- Se trata de un proceso más amplio que la mera comprobación del cumplimiento del RGPD.
- Debe ser sistemática y producir un informe final, identificando a los responsables de cada tarea.
- Empieza con una identificación y clasificación de la información para determinar los datos personales afectados.
- Concreta quién y cómo se accede y se tratan los datos personales.
- Se permite la participación de los afectados de la propia institución y externos.
- Se definen los controles para garantizar el tratamiento únicamente de los datos necesarios para las finalidades legítimas especificadas.

No todas las fases de la evaluación de impacto en protección de datos tienen que hacerse con la misma intensidad, pues dependerá de cada caso. Antes de empezar la evaluación de impacto, es necesario decidir quiénes son los encargados de llevarla a cabo y qué se espera conseguir. Esto servirá para constituir un equipo de trabajo interdisciplinar que obtenga la información necesaria, interactúe con los actores, planifique las tareas, lleve a cabo las consultas, evalúe los resultados, adopte las medidas y garantías y elabore el informe final. Tanto la formación como las tareas de los miembros del equipo deberían constar en un documento escrito. Es necesario que este equipo cuente con la colaboración y el apoyo de la dirección. Algunas indicaciones sobre las fases serían:

a) La descripción del proyecto y de los flujos de datos personales: se puede hacer una primera versión con la información inicial, y luego actualizarla a medida que se disponga de más elementos. Además de exponer de manera clara y comprensible, se incluirá material gráfico que explique de forma visual las características del proyecto y los flujos de información.

b) La identificación y evaluación de riesgos: aquí empieza concretamente la evaluación de impacto. Pueden existir riesgos generales; relativos a la legitimación de los tratamientos y cesiones de datos personales; en el momento de las transferencias internacionales; en la notificación o en la transparencia de los tratamientos; en la calidad de los datos; en lo relativo a datos especiales; en cuanto al deber de secreto; en los tratamientos por encargo; en los derechos ARCO; y en la seguridad[7].

[(7)]Véase el desarrollo de estos posibles grupos de riesgos en AEPD (2014).

c) Consulta con las partes afectadas: estas consultas son clave para obtener la información, y no es necesario revelar secretos industriales, aunque es posible prever cláusulas de confidencialidad. Las preguntas deben presentar opciones realistas y conviene informar a los participantes de los resultados al final del proceso.

d) Gestión de los riesgos identificados: se puede seguir el esquema de grupos de riesgos identificados para incluir medidas en cada uno. Así, por ejemplo:

- Análisis de cumplimiento del RGPD y otras normas.
- Informe final.
- Implantación de las recomendaciones.
- Revisión de los resultados y realimentación: se trata de establecer un ciclo o rueda (planificar, implantar, verificar y actuar).

Tabla 1. Ejemplo de gestión de riesgos identificados sobre los datos especiales

Datos especialmente protegidos	
Riesgos	Medidas
Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión.	Evitar el uso de datos especialmente protegidos, salvo que resulte absolutamente necesario. Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario), y que permitan probar que se cuenta con el mismo.
Asunción errónea de la existencia de una habilitación legal para el tratamiento o la cesión de datos sensibles.	Nombrar a un delegado de protección de datos, o *data protection officer* (DPO), para contar con asesoramiento cualificado.

Fuente: AEPD (2014).

Datos especialmente protegidos	
Riesgos	Medidas
Disociación deficiente o reversible que permita la reidentificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos.	Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de reidentificación es mínimo.

Fuente: AEPD (2014).

En el RGPD, este esquema no se menciona y se limita a indicar una obligación general para el responsable. Así, cuando el tipo de tratamiento pueda entrañar un alto riesgo para los derechos, el responsable llevará a cabo, antes del mismo, una evaluación de impacto del tratamiento en el derecho a la protección de datos (art. 35 RGPD). Para ello, se utilizará alguna de las metodologías de análisis de riesgos existentes, y se tendrán en cuenta los siguientes elementos:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados afectados.
- La cantidad y variedad de tratamientos efectuados.

La evaluación será necesaria cuando se lleve a cabo un tratamiento automatizado como la elaboración de perfiles, que permita adoptar decisiones con efectos jurídicos para las personas o que les afecten significativamente[8]. También será necesaria la evaluación de impacto cuando se traten a gran escala las categorías especiales de datos[9]. Por otro lado, también se requerirá cuando se incluyan datos personales relativos a condenas e infracciones penales, o a medidas de seguridad conexas. Asimismo, será precisa la evaluación en caso de observación sistemática a gran escala de una zona de acceso público. El delegado de protección de datos, si lo hubiere, asesorará al representante en la evaluación de impacto[10].

(8)El art. 30.2d APLOPD concreta el análisis o la predicción de aspectos referidos al rendimiento de trabajo, situación económica, salud, preferencias e intereses personales, fiabilidad o comportamiento, solvencia financiera, localización o movimientos.

(9)El artículo 9 RGPD prohíbe «el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física». El tratamiento se permite, pese a todo, de acuerdo con el apartado 2, cuando se dan algunas circunstancias como el consentimiento del afectado, la necesidad de proteger intereses vitales o un interés público, entre otros.

(10)El art. 30.2 APLOPD concreta y amplía los supuestos de mayor riesgo: cuando el tratamiento pueda generar situaciones de discriminación; usurpación de identidad o fraude; pérdidas financieras; daño para la reputación; pérdida de confidencialidad de datos sujetos a secreto profesional; reversión no autorizada de la seudonimización; o perjuicio económico, moral o social significativo para los afectados. Otro criterio es que pueda afectar a derechos de los afectados, o bien que les impida el control sobre sus datos personales. Finalmente, el art. 30.2e APLOPD contempla el supuesto de tratamientos de datos de grupos de afectados en situación de especial vulnerabilidad, como los menores de edad o las personas con discapacidad.

En algunos casos, el tipo de tratamiento y el tamaño de la empresa supondrán un menor riesgo para los derechos[11] y, por lo tanto, no se deberán poner en marcha las medidas para reducir estos posibles riesgos[12].

(11)La autoridad de control podrá publicar listas de tipos de tratamientos que no requieran evaluaciones de impacto (art. 35.5 RGPD). El art. 30.2c APLOPD, *acontrario sensu* , parece admitir lo meramente incidental o accesorio de estas categorías especiales de datos.

(12)La AEPD ha anunciado que adoptará alguna guía para que las PYMES puedan llevar a cabo procesos de valoración en supuestos que no impliquen, en principio, riesgos elevados.

Los factores de riesgo serían los siguientes:

- Datos sensibles.
- Datos de gran cantidad de personas.
- Elaboración de perfiles.
- Cruzar los datos con otros obtenidos de otras fuentes.
- Prever más de una finalidad.
- Uso de gran cantidad de datos o *big data*.
- Uso de geolocalización, drones, videovigilancia a gran escala o IoT (Internet de las cosas).

La evaluación de impacto de protección de datos incluirá los siguientes contenidos:

- Descripción de los tratamientos y su finalidad, así como el interés legítimo perseguido, en su caso.

- Evaluación de la necesidad y proporcionalidad de los tratamientos para su finalidad.

- Garantías y medidas de seguridad para afrontar los riesgos detectados.

El responsable deberá examinar si los riesgos sobrevenidos por los cambios en el tratamiento siguen cubiertos por la evaluación de impacto inicial. La gestión del riesgo identificado es crucial, pues se deberá mostrar la existencia de diligencia: si se muestra la ausencia de riesgo, entonces bastarán las medidas generales del artículo 32 RGPD. Pero en otro caso, se requieren las medidas de los artículos 30 y 35 RGPD. La decisión sobre las medidas de seguridad más adecuadas en cada caso debe facilitarse con la adhesión a códigos de conducta (art. 40 RGPD) y mecanismos de certificación (art. 42 RGPD).

2) Consulta previa

La consulta previa a la autoridad de control es otra novedad en relación con la Directiva 95/46/CE. El responsable consultará a la autoridad de control, antes de empezar el tratamiento, cuando una evaluación de impacto concluya que existe un alto riesgo si no se toman medidas para mitigarlo (art. 36.1 RGPD). El encargado está obligado a cooperar con el responsable cuando sea necesario, y a petición suya (considerando 95 del RGPD). La autoridad de control puede estimar, en ese momento, que no se ha identificado lo bastante el riesgo en cuestión o bien no se han diseñado garantías adecuadas para mitigarlo. La autoridad entonces tendrá 8 semanas, ampliables según el nivel de dificultad en 6 semanas más, para asesorar al responsable o, en su caso, al encargado. Puede suspender el plazo para solicitar información suplementaria al responsable. Finalmente, de acuerdo con el artículo 36.5 RGPD, el Derecho nacional podrá obligar a los responsables a consultar a la autoridad de control en el ejercicio de una misión en interés público, en particular, en relación con la protección social y la salud pública. En este caso, además, el responsable requiere autorización previa de la autoridad de control[13].

[13]La autoridad de control también será consultada cuando se elaboren propuestas legislativas o reglamentarias sobre tratamiento de datos personales (art. 36.4 RGPD).

La información que el responsable debe adjuntar, ya desde la consulta, es la siguiente:

- Descripción de las distintas responsabilidades del responsable, o corresponsables, si los hubiera, así como de los encargados.
- La finalidad y los medios.
- Las garantías y medidas de seguridad previstas.
- Si hay un delegado de protección de datos, sus datos de contacto.

2.2. Protección de datos desde el diseño y por defecto

1) Protección de datos desde el diseño

El Derecho no parece suficiente protección, sin más, para la privacidad[14]. El principio de *privacy by design* y el de *privacy by default* pretenden ofrecer una respuesta, desde el Derecho, a esta nueva situación: «Con el principio de privacidad por diseño, se quiere mostrar que la privacidad no puede asegurarse solamente mediante el respeto de la ley y los distintos marcos reguladores, sino más bien asegurar la privacidad debe ser el modo de actuar organizativo por defecto»[15]. La tecnología, siempre considerada en el ámbito jurídico como un riesgo para los derechos, pasa ahora a proteger la privacidad desde el diseño de cualquier aparato, hasta el tratamiento técnico de los datos personales (Duaso Calés, 2016, págs. 295-320). En este contexto, el RGPD hace una mención expresa, en su considerando 108, a los principios de protección de datos desde el diseño y por defecto. Se busca un enfoque proactivo o preventivo, y no tanto una reacción cuando se ha producido ya la vulneración del derecho. Normalmente, se quiere hacer un uso más extenso de las *privacy enhancing technologies* (PET), o tecnologías garantes de la privacidad. Sin embargo, existe otra concepción alternativa del concepto de *privacy by design*, que tiene en cuenta los procesos, procedimientos y políticas para proteger la privacidad (Rubinstein, 2011, págs. 1409 y sigs.). El RGPD parece tener presente que ciertos tratamientos presentan mayor riesgo y podrían requerir una protección tecnológica de refuerzo: por ejemplo, los datos sensibles, como son los datos médicos o financieros[16]. En función de los riesgos, deberá valorarse en qué medida el principio debe ser aplicado (Duaso, 2016, pág. 319).

(14)«Regulation and policy are no longer sufficient to safeguard privacy», 32nd International Privacy of Data Protection and privacy Commissioners, *Privacy by Design Resolution* (Jerusalén, 27-29 de octubre).

Lectura recomendada

R. Duaso (2016). «Los principios de protección de datos desde el diseño y protección de datos por defecto». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 295-320). Madrid: Ed. Reus.

(15)A. Cavoukian, *Privacy by Design* (2009, enero, pág. 1) y *Privacy by Design. The 7 Foundational Principles* (2009, agosto), disponibles los dos en www.ipc.on.ca. El concepto de *privacy by design* fue desarrollado desde los años noventa por la autoridad de control de Ontario, Canadá, y aparece por primera vez en un informe conjunto de esta y su homóloga holandesa, en 1995: Information and Privacy Commissioner, Ontario, Canada, and Registratiekamer, The Netherlands (1995). *Privacy-enhancing technologies: the path to anonimity* (vol. I). Technical Report. En el 2012, la Federal Trade Commission de Estados Unidos considera el principio de *privacy by design* uno de los tres pilares de su *privacy framework* (junto con la simplificación de opciones para el consumidor, y una mayor transparencia): Federal Trade Commission (2012). *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Business and Policymakers*. También el supervisor europeo de protección de datos y el grupo de trabajo del artículo 29 se mostraron favorables a la inclusión de los principios de *privacy by design* y *privacy by default* durante la discusión del RGPD.

(16)Ann Cavoukian (2009, agosto), *Privacy by Design. The 7 Foundational Principles*.

El responsable, con anterioridad al inicio del tratamiento, pero también durante el mismo, incluirá la protección de datos en el propio diseño del tratamiento de datos, del producto o del servicio. De nada puede servir la diligencia del responsable si los desarrolladores del hardware y del software no aplican, igualmente, el principio de protección de datos por el diseño y por defecto[17] (Duaso, 2016, pág. 316). De cualquier manera, el responsable tomará medidas organizativas y técnicas para garantizar el cumplimiento del RGPD. Se podrá usar un mecanismo de certificación para acreditar el cumplimiento de la protección de datos por el diseño (art. 25.3 RGPD)[18]. Estos principios resultan de aplicación en el sector privado, pero también en el contexto de los contratos públicos (considerando 78 del RGPD). Antes de abordar las técnicas concretas

mencionadas en el RGPD, conviene mencionar la conexión de la protección de datos por el diseño y por defecto con dos garantías generales: la minimización de datos y la obligación de transparencia (considerando 78 del RGPD).

(17)El considerando 78 establece esta necesidad, ya que estima que hay que alentar a los productores de productos, servicios y aplicaciones que están basados en el tratamiento de datos personales o que tratan datos personales para que tengan en cuenta la protección de datos. Por consiguiente, deben garantizar que los responsables podrán cumplir *a posteriori* sus obligaciones de protección de datos. La aplicación del RGPD, a partir del 25 de mayo del 2018, mostrará hasta qué punto se cumplirán los principios de protección por el diseño y por defecto, por parte de los distintos actores.

(18)El mecanismo de certificación se aprobará de acuerdo con el art. 42 RGPD. La certificación puede ayudar a establecer criterios claros y uniformes a la hora de aplicar principios tan generales como son los de protección de datos por el diseño o por defecto.

El artículo 25.1 RGPD concreta algunas posibles medidas, como la seudonimización. La seudonimización consiste en reemplazar un atributo por otro. La técnica más habitual es la encriptación mediante clave secreta; en este caso, quien posea la clave secreta podrá desencriptar sin ningún problema el dato. También se utiliza la función *hash*, que retorna un resultado establecido desde una entrada variable, y no puede revertirse. Su punto débil es que podemos deducir la entrada haciendo pruebas por fuerza bruta, hasta obtener el resultado del *hash*. Otra posibilidad es la tokenización, usada en el sector financiero para el procesamiento de tarjetas de crédito. Se suele crear un identificador (token) que sustituye los números del DNI por otros valores que no son de utilidad para el atacante, pero que sirven para la finalidad deseada.

Los seudónimos no son equivalentes a los datos anónimos, pues el seudónimo permite siempre la reidentificación y, por tanto, es un dato personal que debe protegerse. De este modo, hay que evitar el error de pensar que sustituyendo un atributo por otro ya hemos anonimizado el dato. Un ejemplo histórico lo constituye la publicación en el 2006, por parte de American On Line (AOL), de una base de datos de 20 millones de búsquedas de palabras por parte de más de 650.000 usuarios durante un periodo de 3 meses. La única medida de protección de los datos personales consistía en un seudónimo: la identificación de usuario de AOL se había cambiado por un número. Evidentemente, no tardaron en lograr identificar a los usuarios reales y sus localidades. En efecto, los seudónimos, combinados con las direcciones IP u otros datos del cliente, pueden ser fácilmente reidentificables. Otro error habitual es usar la misma clave para varias bases de datos, o para varios usuarios, o no guardar la clave en un lugar seguro. Una de las grandes virtudes del uso de seudónimos consiste en que, pese a no identificar a un individuo, se permite asociar múltiples bases de datos a un mismo individuo. Esto facilita los llamados estudios longitudinales, que solo pueden hacerse cuando diferentes datos pueden asociarse de forma fiable al mismo individuo.

Otra de las tecnologías garantes de derechos más usadas es la anonimización[19]. De acuerdo con la ISO 29100:2011, la anonimización debería ser irreversible e impedir la identificación directa o indirecta del interesado. Ahora bien, como se verá, siempre existe un factor de riesgo residual que hace que en ocasiones se prefiera usar la expresión más modesta de «técnicas de anonimización» en lugar de «anonimidad» o «dato anónimo», que podrían llevar a pensar en un anonimato definitivo, absoluto e irreversible. El dato anonimizado sería el que anteriormente se refería a una persona, pero que ahora ya no es posible vincularlo a esta. Los tipos de datos y de tratamiento pueden exigir una técnica de anonimización más avanzada. Por ejemplo, pensad en un perfil a partir de datos genéticos. En este supuesto, podría existir un riesgo de reidentificación si la técnica de anonimización consiste únicamente en borrar la identidad del donante. Una combinación de datos sobre registros genealógicos o resultados de búsquedas, junto con los datos de cuándo tuvo lugar la donación de ADN, la edad o el lugar de residencia, puede, de hecho, revelar la identidad del donante «anónimo».

(19)Grupo de trabajo del artículo 29 sobre la protección de datos, Dictamen 05/2014, sobre técnicas de anonimización, adoptado el 10 de abril del 2014 (WP216).

Para ofrecer más garantías, algunas técnicas de anonimización alteran de manera aleatoria los datos, para camuflar el vínculo entre el dato anonimizado y el dato original. Ahora bien, conviene llevar a cabo un compromiso para que el dato anonimizado continúe sirviendo para estudios estadísticos o de perfiles, pese a no ser absolutamente idéntico al original. Una forma de alterar el valor es añadir ruido, es decir, datos no reales. Otra forma de lograrlo consiste en la permutación: se cambian los valores de algunos atributos, que se vinculan ahora a otros sujetos. Al igual que en el caso anterior, debe haber un correcto calibrado de las permutaciones para permitir la eficiencia de los datos resultantes para su estudio de perfil. Por otro lado, se usa también otra técnica denominada *differential privacy*, 'privacidad diferencial', que permite al controlador añadir el ruido *ex post* en función de las búsquedas efectuadas, con una indicación del nivel de ruido que hay que añadir para mantener el nivel de privacidad deseado. Por tanto, aquí será necesario hacer un seguimiento de las búsquedas que se van haciendo para determinar la información que se pueda tener sobre un usuario. Esto reduce su uso en caso de motores de búsqueda abiertos que no ofrecen trazabilidad de las búsquedas.

Otra familia de técnicas se basa en la generalización. Su finalidad es evitar que se pueda individualizar a un usuario dentro de un grupo. Por ejemplo, la agregación y la K-anonimización pertenecen a este grupo de técnicas. Una posibilidad consiste en bajar el nivel de granularidad de una localización, es decir, en el atributo lugar, la ciudad se sustituye por el país; en la fecha de nacimiento, el día se sustituye por el mes o el año; los valores del sueldo se indican por intervalos (por ejemplo, 20.000-30.000 euros/año). Para que funcione, hay que evitar elegir un valor pequeño para K, es decir, no crear grupos demasiado pequeños, pues entonces es posible la reidentificación dentro del grupo. Por otro lado, esta anonimización no protege frente a inferencias, una

vez que se conoce que alguien pertenece al grupo, pues todos sus datos están entonces disponibles. Por ello, se ha refinado la técnica de K-anonimidad con L-Diversity y T-Closeness.

La AEPD ha publicado una guía para orientar a los responsables en los procedimientos de anonimización de datos personales[20] (AEPD, 2016). La anonimización de datos persigue eliminar la posibilidad de identificación de personas. Las técnicas sirven tanto en los procesos de anonimización, como para dificultar la reidentificación. El avance de la tecnología impide la garantía del anonimato absoluto y perdurable. Por consiguiente, debe buscarse un nivel de protección suficiente para desincentivar al atacante, y actualizar de manera regular las técnicas usadas para ello. La obligación para los responsables queda limitada a adoptar todas las medidas razonables, de acuerdo con el nivel tecnológico del momento. Por consiguiente, se trata de un proceso continuo, a veces denominado cadena de anonimización o de confidencialidad, cuya ruptura implica la posibilidad de reidentificación de los interesados. De manera opuesta, el proceso de anonimización rompe la cadena de identificación de las personas. La identificación puede ser directa, a través de datos de identificación directa; o indirecta, cruzando datos de otras bases de datos, de redes sociales, buscadores, etc., hasta lograr la reidentificación de las personas. Por consiguiente, la anonimización debe proteger frente a intentos de identificación directa, pero también indirecta.

(20)La valoración de los diferentes riesgos en cuestión requerirá, por parte de las autoridades de control, la adopción de documentos de orientación para los responsables como el aquí mencionado. El Comité Europeo de Protección de Datos, que sustituye al grupo de trabajo del artículo 29, también tiene un rol importante en este cometido.

Es útil desarrollar un esquema cuantitativo de clasificación de los datos, basado en tres niveles de identificación de personas: identificación directa o microdatos, datos de identificación indirecta y datos especiales. La evaluación de impacto en la protección de datos indicará un índice de riesgo residual de reidentificación. Este índice deberá ser conocido por el destinatario de la información anonimizada y, si es de uso público, se dará a conocer a las personas o entidades que utilicen la información.

La técnica utilizada para la anonimización no debe comprometer la plena utilidad o funcionalidad de los datos. A veces, el proceso de anonimización requerirá distorsiones de los datos geográficos, temporales o de otro tipo, que deberán comunicarse al destinatario. Durante todo el ciclo de vida de la información, desde antes de la anonimización hasta su destrucción, se garantizará la privacidad de los interesados. Uno de los aspectos que hay que tener en cuenta respecto a estos efectos es la necesaria formación del personal involucrado en el proceso de anonimización.

Las fases de la anonimización son las siguientes:

a) Definición del equipo de trabajo: conviene definir diferentes roles como, por ejemplo, responsable; delegado; destinatario o responsable del tratamiento de los datos anonimizados; equipo de evaluación de riesgos; equipo de preanonimización y de anonimización; y equipo de seguridad de la información.

b) Independencia de funciones: cada profesional obrará en el ámbito de sus funciones, aunque a veces será inevitable acumular varios roles. Por ello, es necesario documentar las distintas funciones donde se especificarán las razones que impiden la total independencia o segregación de funciones.

c) Evaluación de riesgos de reidentificación: se identificarán los datos personales que hay que anonimizar, los elementos técnicos necesarios, y se categorizarán en función del grado de sensibilidad de la información; se concretará el grado de participación de los miembros del equipo; se identificarán los riesgos como conocidos, potenciales y no conocidos, con una probabilidad de ocurrencia; se propondrá una garantía para cada riesgo y se cuantificará el impacto. Con el informe de riesgos resultante, se decidirá el umbral de riesgos aceptable y se llevará a cabo el informe final, que será revisado de forma periódica.

d) Definición de objetivos y finalidad de la información anonimizada: cuando la información anonimizada sea de uso restringido, se podrán elaborar cláusulas contractuales, códigos de conducta y certificaciones para asegurar que el destinatario no intente la reidentificación de los datos.

e) Selección de las técnicas de anonimización: *hash*, cifrado, sellos de tiempo, perturbación o reducción de los datos.

f) Proyecto piloto y anonimización definitiva: es conveniente un proyecto piloto antes de llevar a cabo la disociación definitiva e irreversible de los datos.

Resulta imprescindible que el personal con acceso a la información anonimizada sea informado de la política de anonimización, de las medidas de control o trazabilidad y de las obligaciones y deberes en caso de ruptura de la cadena de anonimización. Es conveniente prever, además, auditorías periódicas del proceso de anonimización, en las cuales se haga constar:

- El objetivo de la auditoría.
- El equipo auditor y los recursos utilizados.
- Las fases y planificación.
- Las pruebas efectuadas.
- La valoración de los resultados.
- Las propuestas de mejora.
- La auditoría de la explotación de la información anonimizada.

La política de anonimización deberá ser documentada y accesible al personal implicado en el tratamiento de datos anonimizados.

Sin embargo, la privacidad por diseño no se reduce a la seudoanonimización y a la anonimización. Hay otras técnicas posibles, entre las cuales destacamos las tecnologías *sensemaking*, que permiten a las empresas obtener una mejor comprensión de su entorno. Para ello, toman en consideración datos que las empresas ya poseen, así como otros que se encuentran fuera de la empresa. Se analizan fuentes muy distintas, y su finalidad es acabar sirviendo para la toma de decisiones mejores y más rápidas, creando así valor a partir de los datos. Pues bien, una estrategia consiste en favorecer los falsos negativos –es decir, perder algunas cosas–, con la finalidad de evitar falsos positivos –es decir, tomar menos decisiones sobre un individuo que tengan trascendencia sobre su vida (Jonas y Cavoukian, 2012).

2) Protección de datos por defecto

El responsable adoptará medidas técnicas y organizativas tendentes a garantizar que, por defecto, se traten solo los datos necesarios para la finalidad indicada[21] (art. 25.2 RGPD). Algunos criterios que hay que considerar consistirán en reducir los datos recopilados a los estrictamente necesarios –minimización de datos–, ya sea en cuanto a la cantidad de datos, el tipo de tratamiento, el periodo de conservación de la información y su accesibilidad. De este modo, se garantizará por defecto que los datos personales no sean accesibles a un número indeterminado de personas.

(21)Un antecedente lejano de este principio de protección de datos por defecto puede encontrarse ya en la Recomendación 1/99 del grupo de trabajo de protección de datos del artículo 29, sobre el tratamiento de datos personales en Internet efectuado por software y hardware, de 23 de febrero de 1999 (Poullet, 2005, pág. 12).

La idea es que, de manera automática, se ofrezcan las opciones más favorables para la privacidad cuando el usuario adquiera un nuevo producto o servicio. Por consiguiente, no será necesario que este último tenga que modificar la política de privacidad establecida para obtener estas ventajas, sino que ya se le ofrezcan sin necesidad de tocar nada, por defecto. También sin necesidad de *opt in*, es decir, sin tener que hacer nada, el tiempo de conservación de los datos debería limitarse al estrictamente necesario para proveer el producto o el servicio. Por consiguiente, si alguien quiere menos privacidad, entonces debería hacer *opt out* a la protección por defecto. Imaginemos una red social en la que nos piden que publiquemos en nuestro perfil el nombre y el correo electrónico; en cambio, el servicio automáticamente publica también la edad y la localización, no solo para los amigos, sino en abierto. Esto infringe el principio de privacidad por defecto, pues se publica más información de la necesaria para el servicio. Como criterio, se prohíben las políticas de privacidad por defecto que publiquen datos personales a un número indeterminado de personas.

Una certificación, que veremos más adelante, podrá acreditar el cumplimiento de las obligaciones tanto de la protección de datos por diseño, como de la protección de datos por defecto.

3. Obligaciones durante el tratamiento

3.1. Registro y documentación de las actividades de tratamiento

Tanto el responsable como el encargado deben mantener un registro escrito –incluso en formato electrónico– de operaciones de tratamiento, con la siguiente información, que pondrán a disposición de la autoridad de control que lo solicite:

- Nombre y datos de contacto del responsable, así como del delegado, si lo hubiera.
- Finalidad.
- Categorías de interesados, de datos y de destinatarios.
- Transferencias internacionales de datos, si las hubiera.
- Plazos para la supresión de las diferentes categorías de datos, si fuera técnicamente posible.
- Cuando sea posible, una descripción de las medidas técnicas y organizativas de seguridad.

En principio, las empresas de menos de 250 trabajadores están exentas de esta obligación, a menos que el tratamiento sea de riesgo, o incluya categorías especiales de datos o datos de condenas o infracciones penales. Las empresas pueden partir de la actual organización de sus ficheros, y entonces detallar las operaciones efectuadas[22]. Pueden agrupar estas operaciones por criterios habituales como «gestión de clientes», «gestión contable», o bien por otros criterios que crean más convenientes. La AEPD pone a disposición de cada responsable la información o tratamientos notificados al registro general.

(22)De hecho, el contenido del art. 88 del Reglamento LOPD establece los contenidos del «documento de seguridad», y puede servir a estos efectos.

Como reflexión final, los responsables excluidos del deber de mantener un registro escrito de los tratamientos de datos deberán, en todo caso, aplicar medidas de seguridad de acuerdo con su política de protección de datos. Para demostrar el cumplimiento del RGPD, el respeto a las medidas del reglamento LOPD, o mejor a las de un nivel superior, puede servir temporalmente hasta que se adopten directrices de desarrollo del RGPD (López, 2016, págs. 284-285). La posibilidad de usar medidas técnicas, como el registro de control de acceso a los ficheros, también puede ser de utilidad.

3.2. Seguridad del tratamiento

El responsable y el encargado aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32 RGPD). Aunque el delegado de protección de datos tiene en el RGPD un perfil jurídico, deberá también colaborar estrechamente con el responsable de seguridad de la información (CISO) y, si se trata de una empresa designada como operador de infraestructura crítica, también con el responsable de seguridad y enlace (Carpio, 2016, págs. 335-349, especialmente pág. 338). Algunas de las posibles medidas podrían ser:

Lectura recomendada

M. Carpio (2016). «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 335-349). Madrid: Ed. Reus.

- Seudonimización y cifrado de los datos personales.
- Confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios.
- Capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente.
- Verificación regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad.

La adhesión a un código de conducta, o una certificación, podrán acreditar el cumplimiento de los requisitos indicados. De hecho, la ausencia de un listado de controles, que sí aparece en cambio en el título VIII del reglamento LOPD, lleva a afirmar a algunos autores que se persigue una corregulación, con posibles códigos de conducta sectoriales, que posteriormente las autoridades de control y, en su caso, el Comité Europeo de Protección de Datos aprueben (Carpio, 2016, pág. 339). El responsable y el encargado deberán velar por el cumplimiento de sus instrucciones por parte de cualquier persona que actúe bajo su autoridad.

A la espera de que la AEPD dicte las directrices sobre las concretas obligaciones para cada tipo de datos de acuerdo con el RGPD[23], teniendo en cuenta un eventual dictamen del Comité, se plantea la duda sobre si se mantendrán o se suprimirán las actuales medidas de seguridad del reglamento LOPD[24] (López, 2016, págs. 287-288). Quizá la AEPD plantee al Comité estas medidas como punto de partida para el dictamen del Comité o para la aprobación de los códigos de conducta (Carpio, 2016, pág. 339).

[23]De acuerdo con la disposición adicional primera del APLOPD, el Esquema nacional de seguridad incluirá las medidas de seguridad en el ámbito del sector público, en cumplimiento de los criterios de determinación del riesgo del art. 32 RGPD.

(24)Arts. 89 y siguientes del RD 1720/2007, de desarrollo de la Ley orgánica 15/1999 (LOPD). El considerando 77 del RGPD aconseja proporcionar directrices para mostrar el cumplimiento del mismo, lo cual podría ser una base para mantener varias de las actuales medidas del reglamento LOPD, a la espera de posibles medidas de armonización, mediante el mecanismo de coherencia, por parte del Comité Europeo de Protección de Datos, que sustituye al grupo de trabajo del artículo 29. Una posibilidad alternativa, basada en códigos de conducta, podría sustentarse en el art. 40 RGPD, aunque algún autor duda de la conveniencia de reducir la armonización de las medidas de seguridad europeas a códigos tipo.

3.3. Confidencialidad

La garantía de la anonimización puede incluir acuerdos de confidencialidad que impliquen al responsable del fichero, el responsable del proceso de anonimización, el responsable del tratamiento de datos anonimizados y el personal con acceso a la información anonimizada. Esta garantía es complementaria de los deberes de secreto profesional (art. 6.2 APLOPD). Tanto una como otra serán indefinidas, incluso después de finalizar la relación con el responsable o el encargado (art. 6.3 APLOPD).

3.4. Tratamientos de datos de menores

El consentimiento de los menores solo será válido a partir de los 16 años y, por debajo de esa edad, los padres o los tutores legales deberán autorizar al menor[25] (Piñar, 2016, págs. 187-203). Los estados miembros pueden rebajar esta edad, siempre que no sea por debajo de los 13 años[26]. Por tanto, los menores de 16 y mayores de 13 años podrán otorgar válidamente su consentimiento, si así lo establecen los estados miembros en su normativa nacional. El art. 8 APLOPD establece un consentimiento válido a partir de los 13 años. Pese a todo, esta regla general puede quedar exceptuada por una ley concreta que exija la asistencia de los titulares de la patria potestad o del tutor para algunos negocios. El tratamiento de los datos de los menores de 13 años requerirá siempre el consentimiento del titular de la patria potestad o del tutor[27]. Por otro lado, el art. 4.1 RGPD no distingue por razón de nacionalidad, con lo cual se incluyen los no europeos, o de situación jurídica en Europa. Hay un tema no resuelto en el art. 8 RGPD: ¿qué sucede con los datos del menor recabados con el consentimiento de sus representantes, una vez pasa a ser mayor de edad[28]? ¿Se prorroga este efecto a pesar de la mayoría de edad?

(25)Grupo de trabajo del art. 29, documento de trabajo 1/08, sobre la protección de datos personales de los niños (WP29). Art. 8 RGPD. Ni la Directiva 95/46/CE, ni tampoco la Directiva 2002/58/CE, de privacidad y comunicaciones electrónicas, hacían mención expresa a la protección de datos de los menores. Esto no significa que no gozaran de protección en los principios generales de las directivas, al ser, evidentemente, personas físicas. En EE. UU., en cambio, se adoptó en 1998 la *Children's Online Privacy Protection Act* (COPPA).

(26)Art. 8.1, segundo aparatado RGPD. Hay otras referencias a menores en el RGPD: considerandos 38, 58, 65 y 75; arts. 6.1f, 12.1, 40.2g, y 57.1b RGPD.

(27)En caso de conflicto, deberá garantizarse el interés del menor: por ejemplo, en España, disponemos del art. 163 del Código civil.

(28)El considerando 65 hace referencia a una situación parecida, pero no idéntica: el consentimiento dado por el menor, y que luego quiere suprimir.

Portal de menores

La AEPD tiene un portal especial para jóvenes (www.tudecideseninternet.es), así como la Autoridad Catalana de Protección de Datos. El Instituto Nacional de Ciberseguridad (INCIBE) también gestiona el sitio https://www.is4k.es/.

Pues bien, los responsables deben hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar que el consentimiento de los menores se ha producido válidamente o con la autorización de los padres o tutores legales[29]. Otro aspecto importante es usar un lenguaje adaptado a la comprensión de los menores.

(29)Siguiendo el Informe 46/2010 del gabinete jurídico de la AEPD, el art. 13.2 del RLOPD no establece un procedimiento determinado para que el responsable compruebe la edad y su autenticidad, y lo deja a criterio del mismo. Parece, pues, que es una responsabilidad de hacer y no de resultado, en el sentido de que se cumple con un procedimiento documentado y que se comprueba, aunque luego se pudieran haber producido falsificaciones (Zabía, 2008, págs. 187-191). Quizá la previsión de una especificación de criterios y condiciones a los métodos de obtención del consentimiento por parte de la Comisión, que existía en la redacción del RGPD de 2012, hubiera sido útil a estos efectos.

3.5. Notificación y comunicación de violaciones de seguridad

Una brecha de seguridad suele consistir en una destrucción accidental o ilegal de datos, su pérdida, alteración, difusión no autorizada, acceso, transmisión, guardado o tratamiento no autorizado. Un ejemplo puede mostrar los riesgos vinculados a una brecha o violación de seguridad[30]. Imaginemos que un administrador de un proveedor de servicios de Internet le diese a un tercero el nombre de usuario y contraseña, sobre la base de datos de clientes. Usando estos datos, el tercero accede a todos los datos de los usuarios: nombres, dirección, correo electrónico, número de teléfono, nombres de usuario, contraseñas, número de identificación y datos económicos como números de cuentas y de tarjetas de crédito, estos últimos encriptados, aunque el administrador tiene privilegios de acceso. La compañía tiene más de 100.000 clientes. Los riesgos son evidentemente el mal uso de los datos de las tarjetas de crédito. El tercero también puede usar los correos electrónicos y las contraseñas en otros servicios, pues suele ser habitual que se repita su uso en más de un servicio en línea. Al tener acceso a los datos, puede haber modificado, borrado o alterado cualquier dato de las cuentas. También puede haber dado por terminada cualquier relación comercial con algún cliente. Además, al poder acceder el tercero a los datos desencriptados, la notificación al interesado deberá hacerse igualmente. Cuando se han comprometido las contraseñas, hay que comunicar a los interesados la necesidad de cambiarlas. En el procedimiento de renovación, hay que indicar la brecha de seguridad que fuerza a hacerlo ahora. También sería útil indicarle al interesado que sustituya en los otros servicios las contraseñas que sean idénticas a la comprometida. Ahora bien, si los seguimientos de los *logs* de comunicación muestran que un archivo no ha sido comprometido, entonces no se deberá comunicar la brecha al interesado.

(30)Dictamen 03/2014 sobre notificación de las brechas de seguridad del grupo de trabajo del artículo 29, de 25 de marzo del 2014 (WP213), aunque basada en la Directiva 2002/58/EC y no en el RGPD.

1) Notificación a la autoridad de control

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control[31] en un plazo máximo de 72 horas, a menos que resulte improbable que sea un riesgo para los derechos[32]. Si la notificación se produce después de las 72 horas, entonces se acompañará de los motivos de la dilación[33]. Si es el encargado el que detecta la violación de seguridad, lo pondrá inmediatamente en conocimiento del responsable.

(31)De hecho, la notificación se extiende a otras autoridades regulatorias nacionales, en virtud de la legislación sobre protección de infraestructuras críticas (Ley 8/2011, de 28 de abril), y el Real Decreto 704/2011, de 20 de mayo, que aprueba el Reglamento de protección de las infraestructuras críticas.

(32)La interpretación del RGPD deberá extenderse a los procedimientos de notificación existentes en un ámbito europeo, que se aplican a los prestadores de servicios de comunicaciones electrónicas: Directiva 2009/136/CE, de 25 de noviembre, que modifica la Directiva 2002/58, relativa al tratamiento de datos y protección de la intimidad en el sector de las comunicaciones electrónicas; Reglamento 611/2013, de 24 de junio, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, sobre la privacidad y las comunicaciones electrónicas; Directiva 2009/140/CE, de 25 de noviembre, relativa a la autorización de redes y servicios de comunicaciones electrónicas.

(33)La AEPD ha previsto, en su sede electrónica, el procedimiento para que los proveedores de servicios de comunicaciones electrónicas informen de las quiebras de seguridad. Este procedimiento deberá también adaptarse al RGPD.

Pues bien, la notificación a la autoridad de control[34] deberá contener los siguientes aspectos:

- Describir la naturaleza de la violación, incluyendo las categorías y el número aproximado de interesados y registros afectados.
- Indicar el nombre y los datos de contacto del delegado de protección de datos, u otro punto de contacto para obtener más información.
- Avanzar las posibles consecuencias que puede acarrear la violación de la seguridad de los datos.
- Describir las medidas y los remedios adoptados.

(34)Las distintas guías existentes de ayuda a la implementación de los procedimientos de gestión y notificación de incidentes deberán adaptarse al RGPD. C. Galán; J. A. Mañas; Innotec System, CNN (2015). *ENS Guía de seguridad. Gestión de Ciberincidentes, Gobierno de España* (vols. CNN-STIC, 817). ENISA (2014). *Technical Guideline on Incident Reporting*. CNPIC-INCIBE. *Guía de reporte de incidentes para operadores críticos. Categorías para el reporte de incidentes según los niveles del PNPIC, Gobierno de España*.

(35)Existen también buenas prácticas, de adopción voluntaria, para el intercambio de información sobre incidentes. ISO/IEC 27035:2011. *Information technology - Security techniques - Information security incident management*.

Si no se dispone de toda esta información en el primer momento, puede irse enviando de manera gradual, aunque sin dilaciones. El responsable documentará la violación de seguridad, con los hechos relacionados con la misma, sus efectos y las medidas correctivas adoptadas. De esta manera, la autoridad de control podrá verificar el cumplimiento de las obligaciones del responsable[35].

2) Comunicación al interesado

Cuando sea probable que la violación de seguridad entrañe un alto riesgo para los derechos de los interesados, el responsable lo comunicará sin dilaciones indebidas. Para ello, describirá con un lenguaje comprensible la naturaleza de la violación de seguridad, e indicará el nombre y los datos de contacto del

delegado de protección de datos u otro punto de contacto para obtener más información; avanzará las posibles consecuencias que puede acarrear la violación de la seguridad de los datos; y finalmente, describirá las medidas y los remedios adoptados. Si solo existe un afectado, se le notificará igualmente. Aunque se pueda pensar que los datos son públicos y se encuentran ya a disposición de todo el mundo, hay que tener en cuenta si el nivel de disponibilidad o accesibilidad de los datos ha cambiado, en el sentido de que se afecta negativamente al interesado, pues esto mantiene el deber de notificación.

No se comunicará, en cambio, al interesado la violación de seguridad de los datos en los siguientes casos:

- Si el responsable ha adoptado medidas de protección técnicas y organizativas apropiadas, como el cifrado.

- Si el responsable ha tomado medidas que garantizan que ya no se concretará el probable alto riesgo para los derechos de los interesados.

- Si la comunicación a los interesados supone un esfuerzo desproporcionado o no razonable para el responsable. En este caso, se optará por una comunicación pública o similar, aunque esto no excluye tampoco el hecho de que se pueda avisar a otro responsable que tenga los datos de contacto para que se ponga en contacto con los interesados.

La autoridad de control podrá pedirle al responsable que comunique la violación de la seguridad de los datos a los interesados, o bien que adopte algunas de las medidas indicadas[36]. Algunos autores sostienen la necesidad de que la autoridad de control actúe con diligencia al recibir las notificaciones, ya sea para no entorpecer investigaciones judiciales, o también para no causar daños a la reputación de la empresa, después de notificar esta una violación de seguridad (Carpio, 2016, pág. 343).

[36]No queda claro si, a raíz de la comunicación, la autoridad de control puede iniciar un expediente sancionador a la empresa. Si así fuera, la notificación a la autoridad de control podría tenerse en cuenta como atenuante.

4. Obligaciones después del tratamiento: cooperación con la autoridad de control

Como reflexión final, no por obvia menos importante, el responsable y el encargado, así como sus representantes, colaborarán con las autoridades de control que soliciten su ayuda. Un aspecto interesante es la voluntad de comunicación creciente de las autoridades de control con el responsable. En este sentido, la Agencia Española de Protección de Datos ofrece una lista de verificación para que los responsables y encargados puedan hacerse preguntas y buscar respuestas adecuadas en el momento de aplicar el RGPD. Los contenidos principales que hay que verificar son:

- Legitimación: comprobar la base legal para el tratamiento y verificar que el consentimiento reúna los requisitos necesarios.

- Información y derechos: presentada de forma clara, completa, con mecanismos para ejercer los derechos ARCO, con procedimientos para responder y colaboración en el procedimiento entre el responsable y el encargado, y atendiendo a los nuevos derechos, como la portabilidad.

- Relaciones responsable-encargado: valorar si los contratos de encargo respetan el RGPD.

- Adopción de medidas de responsabilidad proactiva: verificar que se haya hecho una evaluación de riesgos, incluyendo las medidas paliativas correspondientes, así como un registro actualizado, unas medidas de seguridad adecuadas y corregidas en función de los sucesivos análisis de riesgo efectuados; y una detección y reacción adecuadas frente a las quiebras de seguridad, con un registro de las mismas e indicación de la figura del delegado u otro punto de contacto a la autoridad de control y a los interesados.

La AEPD proporcionará unas herramientas simplificadas para las organizaciones que tengan un número limitado de tratamientos que presenten un riesgo bajo para los derechos de los interesados. Por el momento, se ofrece a las mismas una lista de verificación simplificada (AEPD, 2014).

Bibliografía

AEPD (2014). *Guía para la evaluación de impacto en la protección de datos personales*.

AEPD (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*.

Binns, R. (2017). «Data protection impact assessments: a meta-regulatory approach». *International Data Privacy Law* (vol. 7, núm. 1, págs. 22-35).

Carpio, M. (2016). «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 335-349). Madrid: Ed. Reus.

Centre for Information Policy Leadership (2014). «The role of risk management in Data Protection». *Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy* (23 de noviembre).

Duaso, R. (2016). «Los principios de protección de datos desde el diseño y protección de datos por defecto». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 295-320). Madrid: Ed. Reus.

Gil, E. (2016). *Big Data, privacidad y protección de datos*. AEPD, BOE.

Grupo de trabajo del artículo 29 sobre la protección de datos, dictamen 05/2014 (2014, 10 de abril). *Técnicas de Anonimización*. WP 216.

Grupo de trabajo del artículo 29 (2016, febrero). *Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)*.

López, L. F. (2016). «La responsabilidad del responsable». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 282-285). Madrid: Ed. Reus.

Jonas, J.; Cavoukian, A. (2012). «Privacy by Design in the Age of Big data». *Privacy by Design (PbD)*.

Kuner, C. (2012, febrero). «The European Commission's proposed data protection regulation: A Copernican revolution in European data protection law». *Bloomberg BNA Privacy and Security Law Report* (vol. 6, págs. 1-15).

Piñar, A. (2016). «Tratamiento de datos de menores de edad». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 187-203). Madrid: Ed. Reus.

Poullet, Y. (2005). «Pour une troisième génération de règlementations de protection des données». *Jusletter* (núm. 3, octubre).

Recio, M. (2016). «Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 351-366). Madrid: Ed. Reus.

Rubinstein, I. S. (2011). «Regulating Privacy by Design». *Berkeley Technological law Journal* (vol. 26, págs. 1409 y sigs.)

Tancock, D.; Pearson, S.; Charlesworth, A. (2013). «A privacy impact assessment too for cloud computing». En: *Privacy and Security for Cloud computing* (págs. 73-123). Berlín: Springer.

Wright, D.; Hert, P. de (eds.) (2012). *Privacy Impact Assessment*. Berlín: Springer.

Zabía, J. (2008). «Consentimiento para el tratamiento de datos de menores de edad». En: J. Zabía (coord.). *Protección de datos: Comentarios al Reglamento* (págs. 187-191). Lex Nova.