Consideraciones adicionales sobre seguridad

El cambio fundamental que pudo percibir el profesional con respecto a la normativa anterior es la necesidad de mantener una conducta proactiva. En román paladino, no vale solo con tener un monedero, debemos asegurarnos de que si nos lo quieren robar, no lo tenga fácil el caco. Y esta proactividad debe ser común a todos aquellos que trabajen con los datos, de forma que prevean y se adelanten a los movimientos de "los malos" o, también, a circunstancias inesperadas que afecten negativamente a la seguridad de la información y la protección de los intereses de las personas cuyos datos ostentan.

De todo lo que implica la proactividad, el elemento fundamental para nosotros es la implantación de medidas de seguridad. Hemos hablado de amenazas, de riesgos, y ahora tenemos que hablar de escudos para protegernos. El RGPD hace mención, siquiera en ocasiones difusa, a las posibles medidas a aplicar (art. 32.1 RGPD):

- Seudonimización y el cifrado de datos personales: recordaremos que hemos dedicado unas páginas para tratar de la ambigüedad en la ley al respecto del uso de esta palabra. No vamos ahora a definirla de forma exhaustiva, no es el momento ni lugar, pero entendemos que en el contexto de la asignatura es sobradamente conocida por todos. Y si bien es cierto que no siempre es posible en todo tratamiento, bien sea por los recursos disponibles, bien porque no siempre es pertinente o factible. El cifrado se aplica generalmente con datos de elevada sensibilidad, de menores o interesados en situación de vulnerabilidad. Con su empleo tratamos de colocar una barrera a aquellos accesos no autorizados a los ficheros que alojen los datos. Sobre la seudonimización en particular, añadamos que su uso habitual es con los tratamientos de datos personales donde no es necesario mantener un nexo identificativo entre el interesado y el dato que se está tratando.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. Palabras que nos van a sonar mucho a lo largo de la asignatura, aunque dichas así, en bloque, parecen más una carta a los Reyes Magos que la plasmación de una realidad. Lo que en realidad se pretende es establecer la necesidad de monitorizar y vigilar las políticas internas de protección de datos de todos los operadores de los datos. Insistamos en esa necesaria conducta proactiva del profesional que, es natural, impide considerar a nuestro sistema y medidas de seguridad como algo estático, grabado en el mármol. Debe estar en constante evolución y adaptación a la realidad, a las tecnologías que aparezcan, a los usos sociales.
- Capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. Resiliencia de nuevo. ¿Y si perdemos un papel, y si se borra un fichero, y si se pega fuego un servidor?
- Verificar, evaluar y valorar de forma regular y frecuente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. En otras palabras: establecer procedimientos de auditoria, externa o interna, preparando y estableciendo listados de verificación y otros procedimientos más exhaustivos. Y no solo realizar esto en periodos concretos de tiempo, sino siempre que haga falta: cuando detectemos algún problema, cuando hayamos llevado a cabo algún cambio sustancial…

Hemos procurado protegernos. Tener un buen escudo. Vale. Pero llega la tragedia, el crujir de dientes y el quebrar de huesos. ¿Qué hacemos?

¿Y si nos roban datos? O, pongámoslo en su peor forma ¿y si se lesionan los derechos y libertades de nuestros usuarios?

Pues entonces, además de empezar a tapar agujeros, nos queda un duro camino a seguir. Camino que empieza para el responsable por comunicar esta violación a la AEPD y al interesado. Vamos a ver cómo y en qué circunstancias hay que hacerlo.

En primer lugar, pensemos en la AEPD. La primera pregunta que nos debemos plantear es si esa violación es de carácter grave (esto es, que puede constituir un riesgo efectivo para los derechos y libertades) (art. 33.1 RGPD). Solo si esa violación de seguridad supone un riesgo efectivo para el interesado debemos notificar, en un plazo de 72 horas desde que la hemos detectado, la incidencia a la AEPD. ¿Y qué le debemos remitir a la AEPD? Esto nos lo dice el artículo 33.3 del RGPD.

a) descripción de naturaleza de la violación de la seguridad de los datos personales
    a. Circunstancias en las que se ha producido (intrusión, borrado accidental…)
    b. categorías y el número aproximado de interesados afectados
        i. ¿Alguno de otro estado? Notificación a otras autoridades de control.
    c. categorías y el número aproximado de registros de datos personales afectados;
    d. Fecha y hora del incidente (si es conocida) y de detección del incidente
b) nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales
    a. medidas adoptadas para mitigar los posibles efectos negativos.
e) Indicar si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. En la notificación, avisar si es ampliación de una notificación anterior.
    a. En esta información, indicamos un resumen de la original

En segundo lugar, debemos notificar al interesado también que sus datos han sido expuestos a un riesgo. El cómo y qué nos lo dice el artículo 34 del RGPD.

De igual manera a la notificación que hacemos a la AEPD, ésta solo es necesaria si esa violación de seguridad conlleva un alto riesgo para los derechos y libertades de los interesados. Hay sin embargo una serie de excepciones que permiten no realizar esa comunicación:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Es de subrayar que si mantenemos esa proactividad tantas veces citada, nos ahorramos mucho trabajo.

¿Y si hemos de comunicar al interesado esa desagradable noticia?. Pues básicamente debemos mandarle un subconjunto de las cosas que ya hemos preparado para la AEPD, eso sí, de forma claro y sencillo, pues nos deben entender más allá de cualquier jerga técnica. Debemos indicarle:

a) nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información;
b) describir las posibles consecuencias de la violación de la seguridad de los datos personales; Incluimos la fecha estimada del incidente y la naturaleza y contenido de los datos personales en cuestión, además de las circunstancias en que se ha producido la violación de datos
c) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales
    a. medidas adoptadas para mitigar los posibles efectos negativos.
    b. medidas recomendadas para paliar los posibles efectos negativos.

Consideraciones de carácter general

Para cerrar este apartado, cabe hacer unas breves reflexiones, en su caso, reseñando los artículos relacionados de las normas.

Hablamos, claro está, de datos asociados a las personas, datos que permiten describir por ejemplo su comportamiento o su estado de salud, motivo que los convierte en una de las informaciones más críticas y por tanto a proteger, con más fiereza incluso a la composición química de un medicamento que una compañía farmacéutica acaba de sacar al mercado o en general los secretos comerciales de una empresa[1]. Eso quiere decir que cualquier medida que adoptemos para ese otro tipo de datos siempre será buena para los personales. Lo que debe primar siempre es su seguridad. Su seguridad y no solo evitar su divulgación masiva, con ataques esporádicos de grupos hacktivistas, sino su disponibilidad. Que no nos fallen. Imaginemos un hospital sin los datos de sus pacientes.

Vemos ya dos mitos caídos: los datos personales no son unos datos más a proteger: son los datos a proteger. Y su seguridad no solo pasa por evitar que se divulguen.

¿Qué tienen de particular pues? Partimos de tanta diferencia que el legislador a generó normas diferenciadas de los otros sectores. Leyes, reglamentos, normativa técnica, directivas, instrucciones de la Agencia Española de Protección de Datos… es un auténtico bosque que se entremezcla en la tupida selva del resto de normas jurídicas, relacionadas entre sí y sin límites claros muchas veces, con zonas donde se hace difícil poder trazar una línea de separación.

[1] A éste respecto, véase la directiva relativa a la "protección del saber hacer y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y divulgación ilícitas", disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52013PC0813 (Consultado 30 de julio de 2020)

A modo de conclusión, y limitándonos a la norma de mayor rango tantas veces citada, el RGPD, vemos como se nos establece la obligación de proteger los datos personales garantizando una seguridad adecuada (protección contra el tratamiento no autorizado o ilícito, contra su pérdida por destrucción o daño accidental, todo mediante la aplicación de medidas técnicas u organizativas apropiadas que aseguren la integridad y confidencialidad -art. 5.1.f-). Volvamos de nuevo al RGPD para saber… ¿Qué es esa «seguridad adecuada»?

Considerando 49:

Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, (…) En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

Artículo 32. Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

(…)

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

(…)

Lo hemos visto ya, pero conviene subrayarlo. Ahí lo tenemos en cuatro palabras: confidencialidad, integridad, disponibilidad y resiliencia. Cuatro que, dado que la resiliencia incluye la capacidad de resistir ante los ataques, engloba a las otras tres: confidencialidad, integridad y disponibilidad. Así los objetivos principales es el ya conocido acrónimo C.I.D., que todo profesional debe buscar en cualquier sistema de información, mantenga o no datos de carácter personal. Cuando además es así, debemos extremar el celo, pues pueden resultar gravemente perjudicados los titulares de los datos.

Ya tenemos a los dos agentes principales en juego: el informático, responsable del tratamiento, y el usuario, cliente, paciente… que son los titulares de los datos. Titulares que poseen unos derechos que son precisamente los que provocan que los responsables del tratamiento tengan unos deberes a cumplir.

Destaquemos las palabras «estado de la técnica», que se relacionan con los «costes de aplicación». Esto de hablar de los costes como elemento a considerar las mejores técnicas resulta una potencialmente peligrosa puerta trasera por donde tratar de saltarse la ley. Si se interpreta de forma perversa, podemos leerlo como que por abaratar los costes se permitiría de alguna manera crear riesgos de incumplimiento de los derechos de los interesados. De ahí la importancia de emplear como necesario criterio el tipo de datos de carácter personal que se están tratando, pues no es lo mismo una base de datos pequeña en tamaño con una relación de las matrículas de los vehículos de los vecinos, que las tablas que contengan los datos correspondientes a las pruebas genéticas de los pacientes de un gran hospital. Tengamos en cuenta que cuando se trata de estos datos tan sensibles (según el art. 9 RGPD) es obligatorio efectuar además de una valoración de los riesgos, una evaluación del impacto producido en caso de darse una violación de la seguridad. EIPD que ya conocemos con algo de detalle.

Sobre las medidas exactas a aplicar, hasta la entrada en vigor del RGPD y de la norma 3/2018 la cosa quedaba más o menos clara, con el RD 1720/2007 (RLOPD). Pero este Reglamento cuya vigencia se ha puesto en duda en alguna ocasión, es algo que ya no nos sirve, pues la propia Agencia Española de Protección de Datos (en adelante AEPD) indicó que las medidas de seguridad establecidas en los arts. 89 y ss. del RLOPD no eran aplicables, quedando bajo la responsabilidad de quien realiza el tratamiento la adopción de las medidas necesarias para garantizar la seguridad, lo que implica efectuar una evaluación de los riesgos del tratamiento, con las consiguientes fases de la misma(identificación, medición y comparación, y adopción de las medidas), a ser desarrolladas antes de seleccionar las medidas a implantar, previas al efectuar el tratamiento, de otra manera nos situaríamos al margen de la ley. Al escoger las medidas de seguridad, el responsable del tratamiento debe demostrar su diligencia a la hora de asegurar el tratamiento (incluyendo la acertada selección de medidas de seguridad en base a los riesgos evaluados).

Un tema de interés elevado es saber dónde ponemos el límite. Ha quedado meridianamente claro que, gracias al desarrollo del Big Data, el Internet de las Cosas (IoT) y la Inteligencia Artificial, nuestra sociedad, nuestros hábitos, están cambiando. Vivimos rodeados de sensores de los que en su mayoría no conocemos sus mecanismos de seguridad ni, en ocasiones, el destino real de los datos captados. Cada día se captan más datos de los ciudadanos, a niveles más profundos y en mayor cantidad y continuidad temporal. Esto nos da una respuesta a esa pregunta: ¿Dónde ponemos el límite? En realidad… no hay límite.