ARI 23/2018
20 de febrero de 2018

La entrada en vigor del Reglamento General para la Protección de Datos desde la perspectiva de ciberseguridad

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

En mayo de 2018 entrará en vigor el nuevo Reglamento para la protección en el tratamiento de los datos personales. Obligará a numerosas organizaciones a adoptar medidas para su protección y para evitar las elevadas sanciones y el daño reputacional ocasionados por las brechas de seguridad que afecten a esos datos.

Resumen

El 25 de mayo de 2018 entrará en vigor el nuevo Reglamento para la protección en el tratamiento de los datos personales de las personas físicas (RGPD), cuya implantación en los Estados miembros será obligada con carácter inmediato. Presenta retos de armonización con otras regulaciones europeas, como la Directiva para garantizar la seguridad de las redes y sistemas de información (Directiva NIS), cuya transposición al ordenamiento jurídico nacional entrará en vigor el 9 de mayo de 2018. Ambas normas y otras que propone la Comisión representan un salto cualitativo en las exigencias sobre la seguridad y la gestión del riesgo de la información para empresas y administraciones públicas. El RGPD tiene por objetivo la salvaguarda del derecho fundamental de la privacidad de los ciudadanos en el marco del Mercado Digital Único europeo y en el contexto de la economía digital global, que precisa del procesamiento de una gran cantidad de información mediante la aplicación de algoritmos de inteligencia artificial (*Big Data*) junto a nuevos modelos de negocio basados en el intercambio y explotación comercial de datos.

A continuación se analizan las implicaciones de la entrada en vigor del RGPD desde el punto de vista de la gestión de la seguridad de la información, señalando las obligaciones, procesos y riesgos que se plantean a las organizaciones. También se analiza su solapamiento con regulaciones como la de Directiva NIS de reciente trasposición y otras propuestas regulatorias que la Comisión ha puesto en marcha.

Análisis

La UE acordó reformar la Directiva de 1995 para la protección de datos adoptando en abril de 2016 el Reglamento para la protección en el tratamiento de los datos personales de las personas físicas (RGPD). Es una regulación que no se aplica a datos personales relacionados con la seguridad nacional de los Estados miembros o con la política exterior y de seguridad común de la UE sino a la protección de los datos personales de los ciudadanos en salvaguarda del derecho de la privacidad, reconocido en la Carta de

los Derechos Fundamentales de la UE (art.8). Por esa razón, su protección es mayor en la UE a la establecida en otras regiones donde se haya vinculada, por ejemplo, a la protección del consumidor en el curso de las transacciones comerciales. Esta diferenciación o fragmentación de loa marcos jurídicos para la protección de la privacidad plantea, por sí misma, importantes retos jurídicos y operativos a las corporaciones multinacionales que operan en el ámbito de las TIC e Internet.

En España el RGPD establecerá a partir de mayo de 2018 significativas novedades con relación al régimen de la Ley orgánica de 13 de diciembre de 1999 para la Protección de Datos de Carácter Personal (LOPD) vigente hasta entonces. Responde a los principios de responsabilidad (*accountability*), por el que las organizaciones tendrán que implementar las medidas necesarias para tratar los datos personales y acreditar su cumplimiento, al de protección de datos por defecto y desde el diseño (*privacy by design*)[1] del producto o servicio y al de transparencia para asegurar la completitud y legibilidad de los avisos legales y políticas de privacidad a los usuarios.

El Reglamento refuerza los derechos de los ciudadanos a recibir una información inteligible, completa y sencilla (transparencia), a ser consultados de forma inequívoca, libre y mediante un acto afirmativo y claro (consentimiento), a revocar éste o a exigir la supresión y eliminación de los datos en redes sociales o buscadores de Internet (derecho al olvido) y a trasferir los datos de unos proveedores de servicios en Internet a otros (portabilidad).

El RGPD incorpora garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fuera de la UE e implanta elevadas sanciones por incumplimiento. También establece nuevas obligaciones a empresas y administraciones, tales como la designación de un delegado de Protección de Datos (DPO), la evaluación de los riesgos y la adopción de las medidas adecuadas para mitigarlos.

En relación con los incidentes de seguridad –extravío, robo o acceso no autorizado a los datos de carácter personal– cada organización deberá comunicar la brecha de seguridad a la autoridad de protección de datos y en casos graves a los afectados tan pronto sean conocidas en un plazo máximo de 72 horas. En este sentido, la organización deberá detectar, registrar y decidir si procede comunicar el incidente a la autoridad de protección de datos, así como facilitar la información sobre el mismo ante la solicitud de la autoridad, para lo que precisa contar con sistemas de detección, investigación, actuación y reporte internos confiables y ágiles. Además, tendrán la obligación de comunicar las brechas de seguridad a los afectados en los casos graves tan pronto

[1] En relación a la aplicación del principio de privacidad por defecto, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha publicado dos guías para facilitar la implantación del principio de privacidad por diseño (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design) de los servicios y productos a proveedores y en segundo lugar a empresas de Big Data (https://www.enisa.europa.eu/publications/big-data-protection), notable foco de atención de las autoridades (por ejemplo, Forbes –véase https://www.forbes.com/sites/gilpress/2017/11/09/10-predictions-for-ai-big-data-and-analytics-in-2018/#2ffa5304403c– estima un ritmo de crecimiento del 40% en el almacenamiento de datos, de los cuales actualmente el 90% son no estructurados, indicando que el uso de inteligencia artificial desdibujará la frontera entre datos estructurados y no estructurados).

como sean conocidas. Las empresas multinacionales que proveen servicios y productos a ciudadanos europeos contarán en la UE con una ventanilla única o país de establecimiento principal.

El GDPR diferencia el papel de los controladores de los datos (las organizaciones que determinan el propósito y los medios de procesamiento de los datos personales) del de los procesadores de datos (aquellas que procesan los datos en nombre del controlador) con el claro propósito de mantener las garantías regulatorias a lo largo de toda la cadena de suministro. Los controladores de los datos sólo podrán dejar de informar sobre el incidente si consideran que no afecta a los derechos y libertades de los individuos, aunque en cualquier caso deberán registrar el incidente y facilitar la información en respuesta al requerimiento del regulador. Este modelo de actuación ante una brecha de seguridad exige a las organizaciones dotarse de procesos y sistemas confiables y ágiles para poder adoptar una decisión respaldada sobre si informan del incidente a la autoridad regulatoria.

Las empresas de menos de 250 empleados se benefician de algunas excepciones, tales como la obligación de llevar registros sobre sus actividades de procesamiento de datos personales, a menos que el procesamiento constituya una actividad regular que pueda suponer una amenaza para los derechos y libertades de las personas, o se relacione con datos confidenciales o antecedentes penales. Del mismo modo, no estarán obligadas a nombrar un DPO salvo que la actividad presente riesgos específicos de protección de datos, como el manejo de datos confidenciales a gran escala, en cuyo caso podrán designar a un consultor calificado en calidad de DPO.

Ámbito territorial del RGPD

El RGPD será de aplicación a toda organización (controlador y/o procesador de datos) que ofrezca servicios a ciudadanos europeos, con independencia del emplazamiento de la empresa que realice el procesado de los datos. Esto obliga a numerosas organizaciones que carecen de presencia física en Europa a declarar un emplazamiento principal en un país de la UE, incluyendo las empresas de comercio *online*, aquellas que ofrezcan productos y servicios por Internet (gratuitas o de pago) o cuya actividad se centre en la monitorización de comportamientos o la explotación comercial de los datos (*Big Data*) y que utilicen datos de ciudadanos europeos. Como consecuencia, es previsible que el RGPD desencadene significativas modificaciones en el desarrollo de servicios y productos de empresas multinacionales.[2]

Con el tiempo, el RGPD podría transformarse en una referencia mundial para la protección de la privacidad de las personas físicas si se acaba adoptando por un número significativo de organizaciones multinacionales que operan en otras regiones además de en Europa para unificar sus servicios, procesos y arquitecturas IT. De esta forma,

[2] Por ejemplo, y en el ámbito de servicios *cloud*, el Instituto Ponemon estima que el 80% de las empresas consultadas de cobertura mundial necesitarán cambios para adaptarse al nuevo Reglamento. Véase “The 2018 global cloud data security study”, https://www2.gemalto.com/cloud-security-research/.

podrían ganar competitividad ofreciendo a sus clientes un nivel de protección tan alto como el europeo.

El RGPD desde la perspectiva de la gestión de riesgos

El Reglamento no prescribe procedimientos o medios técnicos específicos. La regulación europea ha evolucionado desde el modelo garantista de la legislación precedente, la cual establece qué medidas de seguridad concretas han de adoptarse (por ejemplo, la LOPD) a otro modelo de regulación basado en la gestión de riesgos, donde cada organización habrá de establecer las medidas acordes al tipo de información que procese y a los riesgos específicos incurridos en el procesamiento.

Así, el RGPD establece que las compañías tendrán la flexibilidad de adoptar, caso a caso, los medios técnicos y organizativos que consideren apropiados para garantizar la integridad y confidencialidad de los datos de carácter personal y demostrar ante el regulador el cumplimiento de los principios establecidos en el RGPD. Son medidas que tendrán que evitar el tratamiento no autorizado o ilícito de los datos personales, su pérdida, destrucción o daño accidental, pero que tendrán que tener en cuenta su adaptación a la evolución tecnológica, los costes de implantación de las mismas, la naturaleza, alcance, contexto y finalidades del tratamiento, así como la probabilidad y gravedad de los potenciales incidentes en relación al daño de los derechos y libertades de las personas (las medidas de seguridad regladas en la LOPD pasaran a ser opcionales).

Por otra parte, el Reglamento faculta al responsable del tratamiento de datos personales para adoptar aquellas medidas –estrictamente necesarias y proporcionadas– que garanticen la seguridad de la red y de la información al hacer frente a acontecimientos accidentales, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales y la seguridad de los servicios ofrecidos. Estas medidas se prestan a través de los sistemas y redes por parte de las autoridades, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas o proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas o la distribución malintencionada de códigos, así como frenar ataques de denegación de servicio y daños a los sistemas informáticos y de comunicaciones electrónicas.

Retos para las organizaciones durante la implantación del RGPD

En las fases iniciales de la adaptación de las organizaciones al nuevo RGPD, éstas habrán tenido que realizar y documentar una pormenorizada evaluación del estado de su organización en relación a los riesgos que se derivan del tratamiento de los datos personales, tales como, por ejemplo, la destrucción, pérdida o alteración accidental o ilícita de datos personales, la comunicación o el acceso no autorizados a dichos datos que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales. Igualmente, habrán tenido que realizar y documentar una evaluación sobre los riesgos tecnológicos concretos, las potenciales vulnerabilidades de los procesos y sistemas, así como el

impacto potencial sobre la integridad y disponibilidad de los datos. La evaluación de conformidad habrá de hacerse extensible al intercambio de datos con terceras empresas externas subcontratadas que procesen datos de carácter personal de ámbito nacional o a la transferencia internacional de datos entre organizaciones, en caso de producirse.

Realizada esta evaluación, cada organización se hallará en disposición de valorar los controles existentes, su efectividad y la exposición al riesgo de sus diferentes áreas para introducir las correcciones organizativas, de procesos y tecnológicas apropiadas para garantizar el nivel de riesgo asumido.

Entre las posibles medidas de seguridad cabe destacar:

- Tecnologías para la mejora de la privacidad (*Privacy-Enhancing Technologies*, PET) tales como el cifrado y la (pseudo)anonimización, teniendo en cuenta la difusa frontera existente entre los datos de carácter personal anonimizados y los datos pseudo-anonimizados, es decir, aquellos cuya anonimización puede ser reversible gracias a la evolución tecnológica y la disponibilidad de datos adicionales.

- Capacidades organizativas, tecnológicas y de inteligencia implantadas por la organización que faciliten la confidencialidad, integridad, disponibilidad y resiliencia de la información.

- Capacidades para restaurar la disponibilidad y acceso a datos tras un incidente.

- Procesos y tecnologías de monitorización para la verificación, evaluación, valoración y documentación continua sobre la eficacia de las medidas implantadas.

Hay que señalar que esta evaluación debe llevase a cabo con una periodicidad dependiente, entre otros factores, de la actualización incremental de las medidas de seguridad acometidas en cada iteración con el fin de alcanzar un ajuste óptimo a los objetivos de seguridad identificados por la organización y en consonancia a la continua evolución de las amenazas. Como resultado de este proceso de evaluación continua, cada organización deberá documentar el grado de cumplimiento de la Regulación, implantar las mejoras de los procesos, tecnologías y personal encargado del tratamiento de los datos de carácter personal, así como establecer canales institucionales para el seguimiento sectorial de buenas prácticas y la interlocución proactiva con la autoridad de protección de datos.

Las medidas de seguridad adoptadas por las organizaciones en cumplimiento del RGPD serán verificadas por la autoridad regulatoria cuando la organización notifique una brecha de seguridad o ante una brecha no notificada y que por su relevancia se haya detectado desde el exterior de la organización. En este sentido, el nuevo Reglamento aumenta notablemente la exposición de las organizaciones a elevadas sanciones que pueden llegar a un máximo de 20 millones de euros o el 4% de la facturación global anual y a los daños reputacionales. Por consiguiente, la notificación de una brecha de seguridad (no siempre evitable incluso adoptando estrictas medidas de seguridad)

puede exponer a la organización a la sanción en el curso de la investigación por incumplimiento o mala praxis a pesar de que ésta no guarde relación directa con el incidente notificado.

Para las organizaciones es de máxima importancia intensificar y automatizar la monitorización de los procesos y las tecnologías que intervienen en el procesado de datos de carácter personal con el doble objetivo de detectar las brechas de seguridad en el curso de las primeras fases, así como resolver con la adecuada proporcionalidad brechas de seguridad que puedan desencadenar una auditoría por el Regulador y llegado el caso, demostrar el cumplimiento del RGPD a las autoridades. Igualmente, tendrán que asegurar que las compañías subcontratadas que intervengan en el procesado de datos cumplen con lo establecido en el Reglamento y son capaces de demostrarlo. Las organizaciones también tendrán que estar en disposición de demostrar el cumplimiento del RGPD ante las autoridades judiciales ya que se exponen a que se presenten demandas colectivas por brechas de seguridad que denuncien, por ejemplo, asociaciones de usuarios y consumidores de la UE.

Motivado por el gran número de organizaciones de distintos sectores a los que afecta el RGPD, junto a la complejidad que conlleva implantar una gestión de riesgos basada en la aplicación de principios generales, preocupa especialmente a las autoridades nacionales y a la Comisión Europea la implantación de esta metodología, especialmente en las PYME que forman parte de la cadena de suministro de las grandes organizaciones. Para paliarlo, la Agencia Española para la Protección de Datos (AEPD) proporciona un conjunto de guías y orientaciones dirigidas a profesionales, empresas y administraciones públicas, así como una herramienta (FACILITA) para la adecuación al RGPD de empresas y profesionales responsables o encargados de tratamientos que traten datos personales de escaso riesgo. En el ámbito de la UE, cabe destacar las directrices para la implantación del RGPD en las PYME publicadas por ENISA y el conjunto de buenas prácticas y recomendaciones, resumidas en el documento *10 Steps to Cyber Security* ofrecidas por el Centro de Ciberseguridad Nacional del Reino Unido.

Por su parte, la Comisión Europea, consciente de la complejidad que supone la implantación de esta normativa para los Estados, administraciones públicas y empresas privadas, ha publicado el 24 de enero de 2018 un documento de orientación con el propósito de facilitar estos últimos meses de la implantación y su posterior aplicación a partir de la fecha de entrada en vigor (*Commission Guidance on the Direct Application of the GDPR as of 25 May 2018*). En ella ofrece un balance del camino recorrido y resume el trabajo aún pendiente por parte de las autoridades comunitarias, las de protección de datos y las administraciones nacionales. Asimismo, la Comisión ha anunciado el lanzamiento de una herramienta en línea en apoyo de las PYME.

A pesar de que el RGPD pretende una implantación rápida, armonizada y directa en los Estados miembros (el Reglamento no requiere la trasposición de una Directiva), son necesarios importantes ajustes en las leyes nacionales vigentes en los Estados miembros, así como la creación de un Consejo Europeo de Protección de Datos. En el ámbito nacional, la aplicación del principio de gestión de riesgos en las administraciones públicas españolas tendrá en consideración los criterios establecidos para el tratamiento

de los datos por el Esquema Nacional de Seguridad, las metodologías de análisis de riesgos utilizadas por las administraciones y las directrices establecidas por la Agencia de Protección de Datos (Orientaciones sobre el nuevo RGPD para Administraciones Públicas y para Entidades Locales).

Solapamiento del RGPD con la trasposición de la Directiva NIS

La Directiva NIS define mecanismos para afrontar los riesgos de seguridad que afectan a las redes y sistemas de información que utilizan y tiene como objetivo prioritario garantizar la continuidad en la prestación de los servicios esenciales. Asimismo, establece la obligación de notificar los incidentes de seguridad que puedan tener un impacto significativo en sus servicios, previéndose la posibilidad de informar sobre estos incidentes a la población cuando sea adecuado para prevenir incidentes, actuar sobre uno en curso o cuando su divulgación sea de interés público. La Directiva también facilitará la prestación de servicios con alcance transfronterizo estableciendo requisitos similares para los operadores y proveedores en todos los Estados miembros. De esta forma se reduce la fragmentación nacional y se facilita la coordinación de las actuaciones o el intercambio de información entre los países de la UE a través de una red de CSIRT nacionales.[3]

El RGPD y la Directiva NIS tienen varios puntos de confluencia. Por una parte, la Directiva NIS incorpora mecanismos para garantizar la coordinación con el RGPD cuando la notificación de incidentes o su gestión, análisis o resolución requiera comunicar datos personales, restringiendo el tratamiento a los términos que sean estrictamente pertinentes y limitados éstos a la finalidad de la notificación que se persiga en cada caso. La cesión para estos fines se entenderá autorizada únicamente en los casos que indica el Anteproyecto. Los datos personales intercambiados deberán cancelarse cuando dejen de ser necesarios para la finalidad que motivó su cesión y, en todo caso, tras la notificación de cierre del incidente. Con posterioridad, éstos deberán ser anonimizados. Por otra, un determinado incidente de seguridad puede desencadenar obligaciones de notificación establecida por la Directiva NIS y el RGDP, poniendo de manifiesto la necesidad de armonizar a nivel nacional las normas que regulan las obligaciones y competencias de los operadores con las establecidas en las normas sectoriales concurrentes de ámbito nacional e internacional en materia de ciberseguridad, evitando, por ejemplo, el solape entre regulaciones que exijan unos mismos controles, la multiplicidad de notificaciones o la acumulación de sanciones ante un mismo incidente.

Otros desarrollos regulatorios de la CE actualmente en curso para la protección de datos

La Comisión Europea ha considerado que el cumplimiento del RGPD es condición necesaria –aunque no suficiente– para la protección de datos en el sector de las comunicaciones electrónicas, por lo que ha propuesto la actualización de la Directiva ePrivacy de 2002. En enero de 2017 la Comisión publicó el borrador para la Regulación

[3] La transposición nacional de la Directiva NIS se encuentra actualmente en fase de Anteproyecto de Ley. Véase http://www.minetad.gob.es/telecomunicaciones/es-ES/Participacion/Paginas/anteproyecto-ley-seguridad-redes-sistemas-informacion.aspx.

en materia de privacidad en el sector de las comunicaciones electrónicas (*Proposal for an ePrivacy Regulation*) con el objetivo de reforzar la confidencialidad de las comunicaciones y metadatos de las mismas, así como regular el tratamiento autorizado de datos y metadatos de las comunicaciones de personas jurídicas llevados a cabo por los proveedores de telecomunicaciones, los proveedores de Internet (OTT) o terceras empresas subcontratadas por éstos con el fin de realizar el procesado de los datos, aunque sean ajenas a este sector.

La propuesta, además de alinear la Directiva de 2002 al nuevo RGPD, tiene por objeto el proteger a los usuarios (ciudadanos y empresas) de la explotación masiva de los datos de carácter personal por parte de proveedores de Internet y operadores de telecomunicaciones, así como ofrecer a éstos un marco competitivo en el desarrollo de servicios europeos de *Big Data* en un marco de competencia global. Una vez finalizado el trámite en el Parlamento y Consejo de Europa, la entrada en vigor derogará la actual Directiva ePrivacy de 2002. En su borrador actual, la propuesta prevé:

- Adoptar una regulación única y armonizada en la UE de implantación inmediata tras su publicación (no necesita transposición).
- Incorporar y equiparar las obligaciones de los proveedores de Internet y proveedores de servicios IoT a los operadores de telecomunicaciones (únicos sujetos obligados en la Directiva ePrivacy de 2002 en vigencia).
- Exigir el consentimiento del usuario para el tratamiento de los metadatos asociados a la comunicación (incluyendo geolocalización).
- Simplificar las disposiciones actuales sobre *cookies*.
- Fortalecer la protección del usuario frente a los distintos tipos de *spam* (telefónico, sms y correo electrónico).

El borrador también establece que los proveedores deben informar a los usuarios sobre los riesgos que puedan comprometer la seguridad de las redes y los servicios de comunicaciones electrónicas y, cuando queden fuera del ámbito de las medidas que debe adoptar el proveedor de servicios, informar a los usuarios finales de las posibles soluciones, junto a una indicación de los posibles costes. En el ámbito de la seguridad e incidentes de seguridad de los datos, los proveedores de comunicaciones electrónicas habrán de cumplir lo establecido en el RGPD.

Los operadores señalan que la superposición de los regímenes regulatorios en RGPD e ePrivacy para el tratamiento de datos y metadatos creará barreras adicionales que dañarán la competitividad de los operadores, en particular relativas al uso de metadatos para innovar los servicios de comunicaciones y los desarrollos europeos en torno a *Big Data*, pudiendo resultar contraproducente para la efectiva protección de los ciudadanos europeos. En este sentido es muy significativo el dictamen emitido en abril de 2017 por el Supervisor Europeo para la Protección de Datos (*European Data Protection Supervisor*, EDPS) en el que refuerza la visión de la Comisión al señalar que la nueva GDPR establece un marco horizontal adecuado –aunque insuficiente– para garantizar

la confidencial y privacidad en el sector de las comunicaciones electrónicas recogidos en el artículo 7 de la Carta de Derechos Fundamentales de la UE.

Finalmente, la Comisión presentó en septiembre de 2017 el borrador de Directiva que regula el libre flujo de datos no personales en la UE (*Proposal for a Regulation for the free flow of non-personal data in the EU*) con el objetivo de facilitar el almacenamiento y procesado de datos no personales entre los Estados de la UE, impulsar la competitividad de las empresas europeas y modernizar los servicios públicos.

Conclusiones

La entrada en vigor del RGPD en mayo de 2018 representa un salto cualitativo en las exigencias sobre la seguridad y gestión del riesgo para empresas y administraciones públicas que tendrá un notable impacto en los nuevos sectores de la economía digital cuya actividad económica se fundamenta en la explotación de datos (*Big Data*).

Obligará a numerosas organizaciones a adoptar medidas para asegurar la protección de los datos de carácter personal y las libertades civiles amparadas por el Reglamento en evitación de las elevadas sanciones y el daño reputacional. El Reglamento es extensible a empresas subcontratadas que procesen datos de carácter personal de ámbito nacional e internacional, así como a la transferencia internacional de datos entre organizaciones. Las organizaciones que carecen de presencia física en Europa obligadas por el Reglamento deberán declarar un emplazamiento principal en un país de la UE, siendo previsible que el RGPD desencadene significativas modificaciones en el desarrollo de servicios y productos globales de empresas multinacionales.

Corporaciones, PYME y administraciones públicas disponen de flexibilidad para adoptar, caso a caso, en base a los principios establecidos en el Reglamento las políticas de gestión de riesgos y los medios técnicos y organizativos que consideren apropiados para garantizar la integridad y confidencialidad de los datos de carácter personal, así como demostrar ante el regulador el cumplimiento del RGPD. Es de máxima importancia para las empresas intensificar y automatizar la monitorización de los procesos y sistemas IT que intervienen en el procesado de los datos, para obtener una detección temprana confiable de las brechas de seguridad.

Por último, se observan puntos de solapamiento entre el RGPD y la Directiva NIS que –salvo una armonización adecuada– exponen a los operadores de servicios esenciales a la realización de unos mismos controles, la multiplicidad de notificaciones o la acumulación de sanciones ante un mismo incidente.