ARI 47/2020
17 de abril de 2020

El impacto del Brexit en la ciberseguridad y la protección de datos

Carlos Galán | Licenciado y doctor en Informática, licenciado en Derecho y abogado especialista en Derecho de las TIC, profesor de la Universidad Carlos III de Madrid

Tema

El Acuerdo de Retirada (Withdrawal Agreement) del Reino Unido de la Unión Europea (UE) establece las propuestas y decisiones que deben adoptarse durante el periodo de transición para mitigar el impacto de la salida definitiva sobre la ciberseguridad y la protección de datos europea.

Resumen

La salida definitiva del Reino Unido de la UE provocará la inaplicabilidad formal en su territorio de las regulaciones que sobre la ciberseguridad y la protección de datos ha venido promulgando la UE. A falta de un acuerdo que lo impida, se corre el riesgo de que se incrementen las violaciones de datos y los ciberincidentes afectando el modo de vida de las sociedades europeas si ambas partes no logran materializar acuerdos sólidos que aseguren que las medidas adoptadas hasta ahora van a mantenerse –o mejorarse incluso– tras el Brexit.

La base de partida para materializar esos acuerdos es el Acuerdo de Retirada (Withdrawal Agreement). Este ARI analiza el impacto de la salida del Reino Unido de la Unión Europea en dos cuestiones de capital importancia para el normal desenvolvimiento de las instituciones, empresas y ciudadanos del continente europeo, británicos o no: la ciberseguridad y la protección de datos.

Análisis

En la medianoche del 31 de enero de 2020, el Reino Unido abandonaba formalmente la UE, provocando la entrada en vigor del denominado "*Withdrawal Agreement*", un acuerdo de retirada que inicia un período transitorio que durará hasta el 31 de diciembre de 2020. El propósito del acuerdo es doble: en primer lugar, determinar los principios que sustentan su desarrollo para garantizar una salida ordenada; además, en él se desarrollan las medidas oportunas para posibilitar la adaptación a los cambios de las instituciones, empresas y ciudadanos de ambas partes. Las medidas irán desde la protección de los derechos de los ciudadanos de la UE que viven en el Reino Unido –y, correlativamente, de los ciudadanos británicos que residen en la UE– hasta el acuerdo financiero entre el Reino Unido y la UE y las garantías para evitar una frontera difícil entre la República de Irlanda e Irlanda del Norte, entre otras.

Como es fácil imaginar, el impacto del Brexit en el inmediato desenvolvimiento de la UE se aventura muy importante, lo que obliga a prever las consecuencias indeseables y

adoptar las medidas oportunas para evitarlas o, al menos, mitigarlas. El presente trabajo desarrolla unas primeras reflexiones en torno a dos asuntos de capital importancia: la ciberseguridad y la protección de datos. En un mundo conectado como el nuestro, donde las amenazas provenientes del ciberespacio no se detienen en fronteras terrestres, la ciberseguridad y la protección de datos no son meras cuestiones locales: interesan y preocupan a todos y, en consecuencia, deben ser tratadas coordinada y conjuntamente por todos los que, de una manera u otra, se ven afectados. Durante años, la UE y el Reino Unido como Estado miembro han sido conscientes de esa realidad y de cómo abordarla, construyendo un modelo de regulaciones capaz de dar una respuesta común a un problema asimismo común. Juntos han analizado los riesgos del ciberespacio para la seguridad de los ciudadanos europeos, sus empresas y sus instituciones en aspectos tan importantes como la privacidad y la protección de datos o la seguridad de las redes y los sistemas de información.

La ciberseguridad y la protección de datos en el Acuerdo de Retirada

El acuerdo tiene escasas precisiones sobre la ciberseguridad y sólo dedica unas pocas acciones específicas dentro del epígrafe IV (“Thematic Cooperation”) de la parte III (“Security Partnership”) del documento. Ambas partes mantienen la cooperación, pero sobre una base voluntaria, incluso en un asunto de capital importancia para la ciberseguridad europea como es el intercambio de información sobre incidentes[1]. La misma voluntad de colaborar pero sin compromisos firmes se formula en relación con la participación del Reino Unido en la Agencia Europea de Ciberseguridad (ENISA, por sus siglas en inglés), en el Grupo de Cooperación de la Directiva de Seguridad en Redes y Sistemas de Información (NIS) y en la red europea de Equipos de Respuesta a Incidentes (CERT-EU)[2]. De cara al futuro, ambas partes se comprometen a seguir dialogando y colaborando en la gobernanza internacional del ciberespacio[3].

Las previsiones en torno a la protección de datos ofrecen, sin embargo, más motivos para el optimismo. En el epígrafe I (“Basis for Cooperation”) de la parte I (“Initial Provisions”), las dos partes se comprometen a proteger los datos de sus ciudadanos y facilitar la trasferencia entre ambos sistemas, pero con autonomía para decidir los estándares de cada sistema[4]. Para ello, la Comisión y el Reino Unido tendrán que

[1] “The Parties reaffirm their commitment to promote security and stability in cyberspace through increased international cooperation. The Parties agree to exchange information on a voluntary, timely and reciprocal basis, including on cyber-incidents, techniques and origin of the attackers, threat-analysis, and best practices to help protect the United Kingdom and the Union from common threats”, p. 108.

[2] “In particular, the United Kingdom should cooperate closely with the Computer Emergency Response Team – European Union (CERT-EU) and, subject to the conclusion of an agreement as provided for in Union law, participate in certain activities of the Cooperation Group established under the Union's Directive on Security of Network and Information Systems and of the European Union Agency for Network and Information Security (ENISA)”, p. 109.

[3] “The Parties should cooperate to promote effective global practices on cyber security in relevant international bodies”, p. 110. “The United Kingdom and the Union will establish a cyber dialogue to promote cooperation and identify opportunities for future cooperation as new threats, opportunities and partnerships emerge”, p. 111.

[4] “In view of the importance of data flows and exchanges across the future relationship, the Parties are committed to ensuring a high level of personal data protection to facilitate such flows between them”, p. 8.

acreditar los estándares de protección de sus respectivos sistemas de protección de datos, que serán autónomos a partir de la retirada (p. 9).

La protección de datos

Como es sabido, el Reglamento General de Protección de Datos (RGPD)[5], además de resultar de aplicación a todas las entidades con sede en la UE y a las que tienen como usuarios/clientes a ciudadanos de la UE, tiene efecto extraterritorial, por lo que también puede afectar a los países no pertenecientes a la UE. Por este motivo, mientras se mantenga el periodo de transición, además de cumplir con el RGPD, las empresas del Reino Unido que tras él sigan tratando datos personales deberán seguir cumpliendo con el RGPD si quieren evitar las correspondientes sanciones[6].

En la actualidad y hasta el final del periodo de transición, las organizaciones que tratan datos personales en el Reino Unido están obligadas a cumplir dos regulaciones: el RGPD y la Ley de Protección de Datos (*Data Protection Act, DPA*) de 2018[7] y sus modificaciones, operadas por el Reglamento de Protección de Datos, Privacidad y Comunicaciones Electrónicas de 2019[8], que integra las exigencias del RGPD con la DPA en lo que se ha venido conociendo como "UK-GDPR". Las diferencias entre este último y el RGPD no son muy significativas, pero algunas merecen un comentario.

En relación con los derechos de los titulares, la DPA protege el derecho a una copia de los datos personales propios (acceso); a impedir el tratamiento de datos que cause o pueda causar daños u otros perjuicios (limitación); a impedir el tratamiento para *marketing* directo (prevención); a impedir que las decisiones se tomen por medios automatizados (oposición); a que se rectifiquen, bloqueen, borren o destruyan los datos personales inexactos en determinadas circunstancias (rectificación), y a reclamar una indemnización por los daños y perjuicios causados por el incumplimiento de la ley (indemnización). El RGPD, por su parte, contempla nuevos derechos y refuerza algunos de los derechos actualmente presentes en la DPA británica, a saber: el derecho a ser informado sobre los datos que se solicitan, los tratamientos previstos, las posibles cesiones a terceros, el tiempo de custodia de los mismos, etc.; a acceder a los datos que están siendo tratados de la forma descrita anteriormente; a la rectificación de los datos personales que sean inexactos o incompletos; a la supresión de los datos personales propios (derecho al olvido) y a impedir su tratamiento en determinadas circunstancias; a bloquear o suprimir el tratamiento de los datos personales; a obtener y reutilizar datos personales propios para fines propios (portabilidad), y otros derechos,

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[6] El Acuerdo de Retirada prevé la aplicación de la "legislación de protección de datos de la UE" hasta el 31 de diciembre de 2020, pudiendo prorrogarse este período durante dos años más. El Reglamento General de Protección de Datos (RGPD), la Directiva de aplicación de la ley (UE) 2016/680, la Directiva sobre la privacidad electrónica y cualquier otra disposición que regule la protección de los datos personales se consideran "legislación de protección de datos de la UE" (European Data Protection Supervisor: "Information note on international data transfer after Brexit", 16 de julio de 2019).

[7] Data Protection Act, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

[8] Data Protection, Privacy and Electronic Communications (EU Exit) Regulations, https://www.legislation.gov.uk/ukdsi/2019/9780111178300/contents.

como que se automaticen decisiones potencialmente perjudiciales sin intervención humana.

En relación con los procedimientos, se pueden señalar las siguientes diferencias:

- El ámbito de aplicación. Mientras la DPA británica solo es de aplicación al Reino Unido, el RGPD se aplica a cualquier organización que trate datos personales de ciudadanos de la UE, aunque dicha organización no tenga su sede en la UE, lo que significa que las organizaciones de Reino Unido que traten datos de los ciudadanos de la UE tendrán que cumplir el RGPD incluso tras el periodo de transición.

- Las comunicaciones comerciales. En la DPA, si una entidad remite comunicaciones comerciales directamente a sus clientes o potenciales clientes, lo único que se requiere es ofrecer la posibilidad de que el receptor manifieste su negativa al tratamiento. En el RGPD, las empresas deben asegurarse de que sus destinatarios las consienten previamente, garantizando que, en el momento de solicitar el consentimiento para recabar datos, tal solicitud debe estar expresada en un lenguaje sencillo y explicando claramente cómo se utilizarán los datos.

- Las solicitudes. En la DPA, los individuos tienen derecho a obtener una copia de la información que las organizaciones tienen sobre ellos. El ejercicio de este derecho permite que las organizaciones británicas puedan cobrar una tarifa de entre 2 y 50 libras dependiendo del tipo de solicitud. En el RGPD también existe este derecho, aunque no contiene tasas prefijadas, sino una compensación por costes en determinados casos, señalando expresamente la obligación de satisfacer las pretensiones dentro del mes siguiente a la solicitud.

- Notificación de violaciones de datos. En la DPA británica, la notificación de una violación de datos es obligatoria solo si también estaba comprendida en el Reglamento de Privacidad y Comunicaciones Electrónicas (Privacy and Electronic Communications Regulations) de 2003, que se refería a cualquier brecha de seguridad de datos en los proveedores de telecomunicaciones o los proveedores de servicios de Internet. En el RGPD, la notificación es obligatoria si la violación de datos entraña un riesgo para los derechos y libertades de la persona, debiendo comunicar tal violación a la autoridad de control tan pronto como sea posible y dentro de las 72 horas siguientes a su descubrimiento. Además, si es probable que la violación de los datos suponga un “alto riesgo” para las personas, también debe notificarse directamente a los interesados.

- Sanciones. La DPA prevé sanciones de hasta 500.000 libras por infracciones graves. En el RGPD, las sanciones tienen un límite superior de 20 millones de euros o el 4% del volumen de negocios anual mundial (lo que sea mayor).

De todo ello cabe deducir que, puesto que el RGPD es superior en exigencias a la DPA británica, muchas de las organizaciones del Reino Unido que gestionan datos podrían estar ya satisfaciendo ambas regulaciones. En lo tocante a las transferencias internacionales de datos, aunque el Reino Unido haya sido reclasificado como “tercer

país", esta realidad no debería suponer ninguna diferencia significativa para esas mismas organizaciones mientras se mantenga el período de transición. Efectivamente, en virtud de lo dispuesto en el RGPD, la transferencia de datos personales desde el Espacio Económico Europeo (EEE) a terceros países y organizaciones internacionales solo está permitida en determinadas circunstancias, a saber:

- Si la Comisión Europea ha emitido una decisión de adecuación que declare que existe un nivel adecuado de protección de datos.
- Si se han establecido las salvaguardas oportunas, como las normas corporativas vinculantes (*Binding Corporate Rules*, BCR) o las cláusulas contractuales estándar (*Standard Contractual Clauses*, SCC).
- Si la transferencia está basada en códigos de conducta aprobados, como el Escudo de Privacidad (Privacy Shield) UE-EE. UU.[9]

Por otro lado, la mayoría de las organizaciones que proporcionan bienes o servicios a los residentes en la UE o que monitorizan su comportamiento también tendrán que nombrar un representante de la UE de conformidad con el artículo 27 del RGPD. Por tanto, es de esperar que, habiendo incorporado el Reino Unido a su ordenamiento jurídico las exigencias del RGPD –al menos en sus aspectos más significativos–, la Comisión adopte una decisión de adecuación en tal sentido, como ya ha hecho con otros países y territorios[10], situación que ambas partes esperan alcanzar antes de concluir el periodo de transición. Sin embargo, si pese a todo no se llega a una decisión de adecuación, el 31 de diciembre de 2020 aquellas organizaciones del Reino Unido que traten datos personales de residentes en la UE tendrán que recurrir a otras salvaguardas, como las normas corporativas vinculantes o las cláusulas contractuales estándar.

Desde el punto de vista administrativo, tras el periodo de transición, la autoridad británica ICO (Information Commissioner's Office) dejará de ser autoridad de supervisión en el marco del RGPD, lo que significa que no podrá aprobar las normas corporativas vinculantes (BCR) para las transferencias de datos personales del EEE al Reino Unido, que tendrá que aprobar una autoridad de supervisión de los 27 Estados restantes. Puesto que las sanciones por incumplimiento del RGPD en materia de transferencias de datos a terceros países u organizaciones internacionales son de elevada cuantía (hasta 20 millones de euros o el 4% del volumen de negocios mundial anual; lo que sea mayor), en caso de no aprobarse una decisión de adecuación, las organizaciones que traten datos personales de residentes en la UE deberán adoptar medidas para garantizar el cumplimiento legal más allá del 31 de diciembre de 2020.

No podemos concluir este apartado sin mencionar el Reglamento de Comunicaciones Electrónicas (Electronic Communications [Amendment etc.] EU Exit) de 2019, un instrumento legal que introduce modificaciones técnicas en la normativa relativa a la

[9] En el momento de redactar estos párrafos no se ha suscrito un acuerdo equivalente para las transferencias del EEE al Reino Unido.

[10] Andorra, Argentina, Canadá, las islas Feroe, Guernsey, Israel, Japón, Jersey, la isla de Man, Nueva Zelanda, Suiza, Uruguay y Estados Unidos (para empresas adheridas al Privacy Shield). Las conversaciones con Corea del Sur están en curso.

notificación de las violaciones de los datos personales por parte de los proveedores de servicios de comunicaciones electrónicas y que revoca la legislación directa de la UE redundante o inapropiada para mantenerse en la legislación del Reino Unido tras el Brexit.

La ciberseguridad de las redes y los sistemas de información

En 2018 el Reino Unido hizo pública una propuesta en relación con la aplicación del Reglamento NIS (Information Systems Regulations) de 2018 dirigida a aquellos proveedores de servicios digitales (PSD) no británicos al objeto de que tales entidades, establecidas dentro y fuera del Reino Unido y una vez consumada la salida de la UE, conocieran las implicaciones de tal salida en materia de ciberseguridad.

El Reglamento NIS británico de 2018 traspone a su ordenamiento jurídico la denominada Directiva NIS de la UE, que tenía por objeto la creación de normas comunes en la UE relativas a garantizar la seguridad de las redes y los sistemas de información de los actores más significativos para el normal desenvolvimiento de los Estados. Pretendía encarar los riesgos que suponen los ciberincidentes para la sociedad europea mediante el desarrollo de capacidades nacionales de ciberseguridad y aumentando las obligaciones de cooperación y notificación de incidentes de las entidades de su ámbito de aplicación, entre otras[11].

Esta norma británica –coincidente en su ámbito de aplicación con la Directiva NIS– iba dirigida a dos grupos de entidades: “operadores de servicios esenciales” (como las organizaciones que operan en los sectores de la energía, el transporte, la salud, el agua y las tecnologías digitales) y los “proveedores de servicios digitales” (como los mercados *online*, los motores de búsqueda y los servicios de computación en la nube). No ha resultado una sorpresa que el Gobierno del Reino Unido haya confirmado que el Reglamento NIS de 2018 seguirá aplicándose de forma práctica en el Reino Unido tras el Brexit, lo que significa que, al menos y hasta que esta norma sea derogada, los requisitos esenciales de la Directiva NIS seguirán siendo de plena aplicación en Reino Unido.

Como es sabido, la Directiva NIS exige que los PSD no establecidos en la UE pero que ofrezcan sus servicios a la UE deben designar un representante en un Estado miembro de la UE en el que el proveedor ofrezca sus servicios (art. 18.2). Así pues, una vez designado un representante en la UE, el PSD deberá cumplir con la legislación nacional que traspone la Directiva NIS en el Estado miembro de la UE en el que esté establecido dicho representante. Éste deberá actuar en nombre del PSD y ser el punto de contacto con las autoridades pertinentes en el país donde ofrezca sus servicios. En la práctica, esta circunstancia puede provocar que algunos PSD establecidos en el Reino Unido deban cumplir localmente los preceptos del Reglamento NIS británico de 2018 y, simultáneamente, la legislación nacional que traspone la Directiva NIS en un Estado miembro concreto, lo que podría comportar significativos inconvenientes –entre ellos, el

[11] La Directiva NIS fue transpuesta al ordenamiento jurídico español mediante Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

aumento de los costes de cumplimiento–, especialmente si los regímenes de la UE y del Reino Unido evolucionan en el tiempo de manera diferente[12].

Por su parte, en relación con los PSD no establecidos en el Reino Unido tras el Brexit, el Gobierno británico –que, a tales efectos, deberá aplicar la legislación que modifica el Reglamento NIS de 2018– ha manifestado su intención de exigir que tales proveedores, cuando ofrezcan sus servicios en el Reino Unido, designen a un representante. Puede serlo cualquier persona física o jurídica establecida en el Reino Unido. Debe ponerse a disposición de los departamentos de información (Information Commissioner's Office, ICO), responsables de regular los PSD, y de comunicaciones (Government Communications Headquarters, GCHQ), responsables de garantizar el cumplimiento del Reglamento NIS de 2018. El representante se designará sin perjuicio de cualquier acción legal que pueda iniciarse contra el PSD que lo haya nombrado y debe designarse en los tres meses siguientes tras la entrada en vigor de la enmienda futura al Reglamento NIS de 2018 o dentro de los tres primeros meses en que la organización de la que se trate se convierta en un PSD de su ámbito de aplicación.

Conclusiones

En lo tocante a la protección de datos, lo que suceda tras el periodo de transición dependerá del resultado de las negociaciones entre la UE y el Reino Unido. La posición por defecto es que el RGPD se incorporará a la legislación del Reino Unido a través del denominado "UK-GDPR", aunque podría haber novedades en relación con la forma en la que se tratan cuestiones específicas tales como las transferencias de datos entre el Reino Unido y la UE, por ejemplo.

En relación con la legislación derivada de la Directiva NIS, los PSD, establecidos o no en el Reino Unido, que presten servicios a la UE deben designar un representante en la UE del post-Brexit. Análogamente, los PSD establecidos fuera del Reino Unido que ofrezcan servicios allí tras el Brexit deberán designar un representante dentro del Reino Unido.

Los PSD que estén sujetos tanto al Reglamento NIS británico de 2018 como a la transposición nacional de la Directiva NIS en un Estado miembro deberán considerar la posibilidad de establecer procedimientos que garanticen la monitorización y el cumplimiento efectivo de cada cuerpo normativo, so pena de significativas sanciones.

En todo caso, durante el período de transición derivado del Acuerdo de Retirada se deberán cerrar los acuerdos correspondientes para mantener o mejorar el que ha venido siendo en los últimos años el *statu quo* jurídico en materia de ciberseguridad y protección de datos en Europa. Así lo esperamos, en beneficio de todos.

[12] Por ejemplo, un PSD con sede en el Reino Unido que se vea afectado por un incidente de ciberseguridad puede tener que notificar y establecer un enlace con múltiples reguladores del Reino Unido y la UE, cada uno con sus propios requisitos y expectativas de notificación.