BREXIT

# Perspectivas en materia de Protección de Datos

La opción tomada por los ciudadanos británicos en el referéndum del pasado 23 de junio de 2016 tiene múltiples consecuencias, muchas de ellas jurídicas. Algunas han sido ya abordadas, pero se ha relegado a un segundo plano lo que el denominado Brexit puede significar para un derecho de los ciudadanos europeos como es la privacidad y la protección de datos.

El marco regulatorio de protección de datos en la Unión Europea confería una total libertad de circulación a los datos dentro de las fronteras de los 28 países miembros. Así, la salida del Reino Unido de la Unión, y por tanto, de ese entorno legislativo, va a provocar que se considere a los radicados en las islas como establecidos en un tercer país, lidiando con controversias como las actualmente existentes con Estados Unidos. En resumidas cuentas, enviar datos de cualquier país de la Unión a Reino Unido constituirá una transferencia internacional de datos, con los efectos legales que ello conlleva.

Es evidente que, dada la importancia que tiene el tratamiento masivo de datos para una empresa de cualquier tipo de industria, Reino Unido no va a mantenerse distante respecto de sus antiguos compañeros, pues no interactuar en este campo con la Unión le dejaría en fuera de juego en un campo de vital importancia para la economía.

Ante esta situación se abre una clara incertidumbre, que habrá de ser resuelta por el gobierno británico en los próximos meses, en torno a la decisión que se adoptará en materia de protección de datos desde el Estado insular.

Antes de nada, hay que comprender la situación legislativa del Reino Unido en esta materia. En la actualidad, la norma aplicable a la protección de datos a nivel nacional es la UK Data Protection Act de 1998, producto de la transposición de la directiva europea de protección de datos de 1995, por lo que implanta los conceptos y principios fundamentales que se utilizan en las normativas europeas de protección de datos en toda Europa. También es relevante la UK Electronic Communications Act, que regula cuestiones de firma electrónica provenientes de la directiva de 1999, transacciones y comunicaciones electrónicas, apoyada en los textos que transpusieron la directiva de comercio electrónico del año 2000. Como puede verse, el marco legislativo actual no dista mucho del que existe en los otros 27 países gracias a la transposición de varias directivas.

A primera vista, la reacción previsible es que se considere al Reino Unido un país con un nivel de protección seguro en protección de datos, no habiendo demasiados problemas para mantener la situación actual, puesto que su normativa está actualmente adaptada a la Europea, siendo muy próxima a la de los otros 27. Claro que esto depende de varios factores: en primer lugar, el gobierno británico cambia, por lo que no conocemos las intenciones de próximos ocupantes del número 10 de Downing Street, así que es factible pensar en un cambio de política legislativa en cuanto a la protección de datos, rompiendo así de manera más drástica los lazos les unían con la Unión. Otra variable a considerar es que la declaración como país con nivel de protección suficiente depende de la aprobación de la Comisión Europea, teniendo que llevarse a cabo por un procedimiento regulado, habiendo de estudiarse numerosos elementos como el funcionamiento de una autoridad de control, la jurisprudencia acerca del tema, los compromisos internacionales del país; además de que ha de revisarse el acuerdo cada cuatro años.

Suponiendo que la segunda opción, más realista y conservadora, sea la que se dé de manera efectiva, la coyuntura no estaría exenta de problemas. La necesidad de la declaración de la Comisión a la que se hacía referencia puede provocar que, en el intervalo de tiempo que exista entre la salida efectiva de la Unión y la aprobación del acuerdo, Reino Unido sea un tercer país y los movimientos al mismo sean transferencias internacionales de datos. Aquí se abriría un intervalo de tiempo indeterminado en el que las empresas de ambas partes tendrían que regularizar sus operaciones para cumplir con una normativa de transición con fecha de caducidad indeterminada. En resumen, demasiados cambios y obligaciones para un espacio de tiempo relativamente corto. A esto hay que sumarle que la normativa y las prácticas del Estado británico en materia de protección de datos serán vigiladas de forma detallada por los reguladores de la Unión, sometiéndose a un escrutinio minucioso.

No cabe olvidar que esta pugna tiene dos bandos, así que la reacción de la Unión Europea ha de ser valorada. Puesto que, si se produce la salida efectiva, será la Comisión la que deberá valorar un acuerdo que declare a Reino Unido como una especie de "puerto seguro", la institución europea puede exigir unos estándares tremendamente exigentes con su excompañero. Así, el lado europeo tiene la capacidad de someter la normativa británica a un análisis pormenorizado que les degrade en la negociación, teniendo que aceptar un férreo control desde Bruselas con tal de no terminar en un limbo normativo.

Esta declaración de país con un nivel de protección suficiente sería necesaria solamente si Reino Unido, al abandonar la Unión Europea, no decide entrar en el Espacio

Económico Europeo. Este es el modelo que sigue Suiza, que no es parte del EEE. El país helvético tiene un acuerdo desde el año 2000 por el que se establece que, al igual que otros territorios como la Isla de Man, Uruguay o Nueva Zelanda, se asegura un nivel adecuado para el tratamiento de datos personales en ese Estado. En el caso de que los británicos opten por adherirse al EEE, la legislación europea en materia de protección de datos se les aplicaría, así que no habría una transferencia internacional de datos al enviar datos a las islas.

Viendo que la opción digamos, tranquila, conservadora o cercana a la Unión, entraña muchos más problemas de los que parece, hay que tener en mente que no puede descartarse un movimiento mucho más drástico por parte del gobierno entrante, reformando la legislación existente en protección de datos para alejarse de la europea, de la cual manifestaron sus discrepancias durante el proceso de aprobación, adoptando así una posición más acorde con los principios menos proteccionistas del mundo anglosajón. Puesto que se asemeja contraproducente que se aíslen de tal forma, esta opción parece menos probable, aunque siempre puede razonarse que si la Unión ha llegado a alcanzar un acuerdo con Estados Unidos, podría alcanzarse con Gran Bretaña en tal caso.

A este respecto, el Information Commissioner's Office, a través de Christopher Graham, ha manifestado que "es crucial tanto para empresas y organizaciones como para consumidores y ciudadanos que haya consistencia internacional en torno a las leyes y derechos de protección de datos", así como que "hablaremos con el gobierno para presentar nuestra visión de que es necesaria una reforma en la legislación británica". Por tanto, desde instituciones del país relevantes en el tema abogan, parece por mantener una unidad en la normativa entre Europa y el Reino Unido.

Sea cual sea la opción seguida, las consecuencias son, como mínimo, complejas. La salida se basa en el artículo 50 del Tratado de la Unión Europea, según el cual, el Estado saliente y la Unión habrán de negociar un pacto de salida, fijando una fecha para el cese de la aplicación de los tratados que, de no fijarse, se produciría al cumplirse los dos años de la celebración de ese acuerdo, pudiendo prorrogarse este lapso de tiempo. Este periodo tiene una importancia vital, puesto que el Reglamento Europeo de Protección de Datos comenzará a tener efectos el 25 de Mayo de 2018, con lo que es más que probable que llegue a ser aplicable a Reino Unido durante un tiempo, puesto que todavía no se ha llegado al acuerdo de salida. Así, la situación en esta materia se tornaría esperpéntica: durante el periodo de negociación del acuerdo de salida y durante el plazo para la misma se seguiría aplicando la ley de 1998, proveniente de una directiva europea; hasta Mayo de 2018, momento en el que la salida, casi con total seguridad, no será efectiva todavía, por lo que empezará a aplicarse el reglamento europeo de protección de datos hasta la fecha en la que se fije el fin de la aplicación de los tratados. Cabe añadir que, una vez entre en vigor el reglamento, cualquier empresa u organización estará obligada a cumplir con su articulado si trata datos de ciudadanos de la UE, independientemente de dónde esté radicada la misma, así que cuando llegue el momento en que eviten la aplicación del reglamento, gran parte de las corporaciones británicas tendrán que sujetarse en buena parte de su actividad a dicho texto.

Podemos prever, sin miedo a equivocarnos, que la legislación británica seguirá acorde a la europea durante un plazo considerable, lo cual torna la bifurcación anteriormente comentada en una decisión a medio plazo. La aplicación del reglamento en Reino Unido será una realidad, así que durante un periodo prudencial habrá calma en cuanto a la protección de datos en el continente. De hecho, Reino Unido, al igual que el resto de países de la Unión, tendrá que transponer a su derecho interno la directiva de reciente aprobación (mayo) por el Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión; es decir, su legislación seguirá avanzando al ritmo del resto de la Unión, de momento.

El mare magnum de dudas suscitadas por el referéndum deja a todos los actores en una situación de desconcierto en el que no cabe más que esperar al desarrollo de los acontecimientos para hablar a ciencia cierta. Mientras tanto solamente se pueden hacer pronósticos y conjeturar.

*Por favor, no duden en escribir a su contacto habitual en ELZABURU o al correo brexit@elzaburu.es en el caso de que necesiten más aclaraciones sobre estos aspectos o cualquier otro relacionado con el Brexit.*



Calle Miguel Ángel, 21
28010 Madrid, España

+34 917 009 400
brexit@elzaburu.es

www.elzaburu.es/brexit