Reglamento (UE) n.º 611/2013 de la Comisión, de 24 de junio de 2013, 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 [*DOUE* L 173, de 26-VI-2013]

Privacidad de las comunicaciones electrónicas

La salvaguarda de derechos como la intimidad y la confidencialidad se han convertido en una prioridad para el legislador europeo, obligado por el propio desarrollo de la tecnología. En los últimos años, la preocupación por su efectiva protección no ha pasado inadvertida en el marco comunitario, y así lo ha querido plasmar la Comisión Europea reiterando sus esfuerzos en aras de proteger los derechos fundamentales de los particulares. Reflejo de todo ello es el Reglamento 611/2013, que trata de dar una nueva dimensión a la Directiva revisada 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 que modifica entre otras la Directiva 2002/58/CE.

El Reglamento se encarga de regular cómo, cuándo y ante quién deben notificar, los proveedores de servicios de comunicaciones electrónicas, los casos de violación de datos personales, entendiendo por «violación», sin pretender adelantar el contenido que sigue, cualquier incidente de seguridad que se produzca y comprometa datos personales.

Ante una violación de datos de carácter personal, la Directiva de 2009 establece la obligación para el proveedor de notificarla a la autoridad nacional competente e informar a la persona afectada. El Reglamento 611/2013 reitera dicha obligación tratando de completar algunos aspectos no contemplados en la legislación comunitaria existente hasta la fecha.

Como apunte previo, a efectos de clarificar la pretensión y el sentido del Reglamento, conviene destacar qué se entiende por *violación de los datos personales*. Siguiendo el tenor literal de la reseñada Directiva, se entiende por tal, «la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad» (Considerando n.º 2 del Reglamento, que remite al artículo 2, letra i), de la Directiva 2002/58/CE)

Teniendo en cuenta este concepto y la gravedad que pueden entrañar los casos en los que se produzca una violación de datos personales, no es de extrañar que cada Estado haya venido tomando las medidas oportunas para tratar de paliar, en la medida de lo posible, las consecuencias negativas que desencadenan los diferentes supuestos a los que cada legislador tenga que enfrentarse. Y precisamente de tal hecho nace la necesidad de elaborar el Reglamento 611/2013, cuyo objeto es tratar de armonizar el sistema de notificación, tanto a la autoridad nacional que competa según el Estado

Ars Iuris Salmanticensis,
vol. 1, diciembre 2013, 151-226
eISSN: 2340-5155

miembro de que se trate (en España sería a la Agencia Española de Protección de Datos, AEPD), como a la persona afectada (denominada en su artículo 3 «abonado» o «particular»).

Para su exégesis resumida, se procede, a continuación, a destacar los elementos más sobresalientes de la norma comunitaria, para, seguidamente, plasmar aquellas cuestiones a nuestro entender más controvertidas.

Los puntos fundamentales que se abordan en el articulado del Reglamento son:

- No basta una mera violación de datos personales, sino que, además, ha de afectar negativamente a los datos personales o intimidad del abonado o particular (como se recoge en la Directiva del 2009).
- La notificación a realizar en caso de violación de datos personales deberá contener los extremos contemplados en los *Anexos I y II* del propio Reglamento según se dirija a la autoridad competente o al abonado (según se dispone en los artículos 2 y 3 del Reglamento). En la notificación a la autoridad competente *(Anexo I)* el contenido se dividirá en dos secciones, la primera de las cuales contendrá información relativa a la *identificación del proveedor* (nombre, identidad y datos del contacto responsable de proteger los datos y se indicará si es la primera o segunda notificación) e *información inicial sobre la violación* (fecha y hora del incidente, circunstancias del caso, naturaleza y contenido de los datos violados, medidas tanto técnicas como de organización aplicadas o pendientes de aplicarse y para los casos que proceda recurso a otros proveedores). La sección segunda reunirá la *información suplementaria sobre el caso* (resumen del incidente, número de personas afectadas, consecuencias y efectos negativos a los que se pueden enfrentar los abonados y medidas técnicas y de organización adoptadas por el proveedor para contrarrestar los efectos producidos) y, según las circunstancias particulares de cada caso, *posible notificación adicional a los abonados o particulares y posibles cuestiones de carácter transfronterizo* cuando la violación afecte a abonados de otros Estados miembros contemplando la notificación a las autoridades pertinentes que en cada caso sean competentes.

Respecto a la notificación al particular *(Anexo II)*, contendrá: el nombre del proveedor, los datos de contacto del responsable encargado de proteger los datos, fecha y resumen del incidente así como la naturaleza y contenido de los datos personales y las posibles consecuencias de la violación, debiendo informar también sobre las circunstancias en las que se ha producido la violación y las medidas adoptadas y recomendadas para subsanar y paliar respectivamente los efectos negativos derivados de la violación.

Ars Iuris Salmanticensis,
vol. 1, diciembre 2013, 151-226
eISSN: 2340-5155

– Merece especial atención la flexibilidad en cuanto a los plazos, por primera vez contemplados, de que dispone el proveedor de servicios de comunicaciones electrónicas para comunicar la violación de datos a la autoridad nacional competente. Si bien es cierto que el proveedor dispone de un primer plazo de 24 horas para poner en conocimiento de la autoridad nacional competente el hecho, la norma permite una segunda notificación dentro de los 3 días siguientes desde que se produzca la primera, a fin de que el proveedor complete la información que no tuviera en un primer momento. Sin perjuicio, añade la norma, de que se envíe una tercera notificación con la información que reste, en el *plazo más breve posible*, justificando de forma motivada la dilación (artículo 2 del Reglamento).
– Existen ciertos casos (según se desprende del artículo 4), en los que no es necesaria la notificación al afectado. La excepción a la regla viene determinada por el hecho de que el proveedor haya aplicado, a los datos afectados en cuestión, las medidas tecnológicas de protección convenientes, pues, de ser así, la notificación se convierte en potestativa.

Las medidas de protección convierten los datos en incomprensibles, a través, por ejemplo, de un cifrado específico seguro o mediante el uso del *hash value* (datos que se sustituyen por su valor resumen, calculado por una función resumen con clave criptográfica normalizada –artículo 4.2.b del Reglamento–), para evitar que personas no autorizadas accedan a ellos.

Así mismo, atribuye a la Comisión, previa consulta a determinadas autoridades, la posibilidad de publicar las medidas tecnológicas de protección (artículo 4 de la Directiva).

En segundo término, los elementos «controvertidos», de difícil aplicación práctica (por cuanto pueden llegar a ocasionar en algunos casos inseguridad jurídica por falta de concreción, imprecisión…), son los siguientes:

– Los plazos marcados respecto a cuándo se ha de producir la notificación a la autoridad competente (artículo 2.3) son de 24 horas, 3 días siguientes, para terminar señalando «el plazo más breve posible». La imprecisión es palmaria y la inseguridad jurídica es consecuencia directa.
– Señala el Reglamento que en circunstancias excepcionales, cuando la notificación al abonado o particular pueda comprometer la investigación del caso de violación de datos personales, el proveedor podrá demorar la referida comunicación (artículo 3.5). La excepcionalidad es portadora también de inseguridad jurídica, ya que, por un lado, debe haber una previa autorización de la autoridad nacional competente, y, por otro, es fundamental que la armonización del sistema sea completa y lo más garantista posible, debiendo, bajo nuestro punto de vista, ser obligatoria en todo caso la notificación de la violación al

Ars Iuris Salmanticensis,
vol. 1, diciembre 2013, 151-226
eISSN: 2340-5155

interesado (ya que la vulneración de sus derechos fundamentales se ha producido, al menos informarlo para su conocimiento y efectos oportunos).

- En el artículo 3.6 donde hace alusión a «las vías de comunicación que garanticen una pronta recepción» no se especifica cuáles son esas vías. Las imprecisiones van contra las garantías de los ciudadanos.
- Si, por un lado, resaltamos como elemento positivo el que la Comisión adopte medidas tecnológicas de protección relacionadas con la notificación (artículo 4), por otro, hay que tomar en cuenta que tal apuesta queda en mera intencionalidad por cuanto se requiere consulta previa a las autoridades nacionales y, sobre todo, porque queda en el dintel del «podrá» (vid. artículo 4.3).
- Las actividades transfronterizas que puedan desarrollar los proveedores quedan en mera enunciación (y consecuente inseguridad jurídica), por cuanto no se adoptan medidas técnicas de ejecución y porque las autoridades nacionales competentes no se ven compelidas a la cooperación en casos de violación de datos personales (con posible dimensión transfronteriza). Se produce una falta de respuesta a importantes «Considerandos» (el 4 y el 9).
- No se detallan cuáles son los soportes electrónicos seguros de que disponen los proveedores para notificar los casos de violación. En este caso no se da respuesta dispositiva al «Considerando 11».

Aun siendo lo más importante lo hasta ahora resaltado, se considera de interés dejar constancia, aunque sea de manera complementaria, de que los «Considerandos» referidos a los distintos apartados del artículo 4 de la Directiva 2002 (véanse las remisiones al artículo 4 de los considerandos 2, 3, 5, 6 y 19) se refieren a la Directiva revisada 2009/136/CE.

Todavía es pronto para aventurar si los operadores de telecomunicaciones y proveedores de servicios de Internet cumplirán con lo estipulado. No procede, aún, hacer un balance apriorístico, pues el Reglamento entró en vigor el pasado 25 de agosto. En todo caso se debe esperar al informe que, según lo preceptuado en el artículo 6 del Reglamento, presentará la Comisión en 2016, para evaluar su aplicación, sobre todo en cuanto a eficacia y repercusión. Será entonces cuando podremos evaluarlo a la luz del seguimiento del sistema hecho por los proveedores y las respuestas dadas por las autoridades competentes.

M.ª TERESA HEREDERO CAMPO
Licenciada en Derecho. Doctoranda en Derecho Civil
Universidad de Salamanca

Ars Iuris Salmanticensis,
vol. 1, diciembre 2013, 151-226
eISSN: 2340-5155