G A _ P

Gómez-Acebo & Pombo

Nuevas obligaciones en materia de ciberseguridad: el Real Decreto Ley 12/2018, de 7 de septiembre

Ana Santamaría Dacal

Consejo Asesor de GA_P

El Real Decreto Ley 12/2018 ha transpuesto la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, identificando las obligaciones de adaptación y notificación a las que van a estar sometidos determinados proveedores de servicios, así como sus regímenes de supervisión y sancionador.

Mediante el Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, el Gobierno ha procedido a la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión *(Network and Information Security Directive)*, cuyo plazo de transposición ya había vencido el pasado 9 de mayo. El carácter transversal e interconectado de las tecnologías de la información y de la comunicación limita la eficacia de las medidas que se emplean para contrarrestar los riesgos de seguridad de las redes y de los sistemas de información cuando se toman de modo aislado, de ahí la utilidad de los requisitos mínimos comunes en materia de ciberseguridad que impone la directiva a nivel europeo y que el Real Decreto Ley 12/2018 incorpora en nuestro ordenamiento insertándolos en la Estrategia de Ciberseguridad Nacional.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

1. Los operadores afectados

El real decreto ley se aplica a dos tipos de operadores: los de servicios esenciales (con un ámbito sectorial más amplio del previsto en la directiva al extenderse a todos los servicios comprendidos en los sectores estratégicos del anexo de la Ley 8/2011, de 28 de abril) y los proveedores de servicios digitales (mercados en línea, motores de búsqueda en línea y servicios de computación en nube; estarán por tanto excluidos, por ejemplo, las llamadas redes sociales —salvo que desarrollen actividades propias de un motor de búsqueda— o los servicios de radiodifusión de vídeos a la carta).

2. Las obligaciones que impone el real decreto ley

Lo más reseñable del real decreto ley son las obligaciones que impone a los dos tipos de operadores señalados. Son principalmente tres:

1) En primer lugar, cada operador tiene la *obligación de adoptar medidas técnicas y de organización para gestionar los riesgos* que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios correspondientes. Ello conlleva una actividad previa de identificación de esos riesgos susceptibles de amenazar la ciberseguridad, lo que normalmente exigirá realizar tests de intrusión, monitorizaciones continuas o auditorías especializadas semejantes a los ya extendidos con arreglo a los códigos de buenas prácticas. Por lo demás, esta obligación de adopción de medidas de gestión de riesgos no difiere mucho de la que impone el nuevo Reglamento Europeo de Protección de Datos de Carácter Personal a los responsables y encargados del tratamiento.

2) En segundo lugar, los operadores tienen la *obligación de notificar los incidentes*. Esta obligación tiene distinto alcance en función del tipo de operador:

   a) Los operadores de servicios esenciales deben notificar los incidentes que *puedan tener* efectos perturbadores significativos de dichos servicios. Se trata, por tanto, de una notificación de carácter preventivo, pues basta con que el incidente se produzca para que surja la obligación de notificación, aunque el efecto adverso aún no sea real y actual. Además, los operadores de servicios esenciales no sólo deben notificar la producción del incidente —«sin dilación indebida»— (primera notificación), sino también su resolución (notificación final) y cualquier otra información que afecte a su evolución mientras no esté resuelto (notificaciones intermedias).

   b) Los operadores de servicios digitales, por el contrario, sólo están obligados a notificar los incidentes *que tengan* efectos perturbadores significativos en dichos servicios cuando el proveedor tenga acceso a la información necesaria para valorar el impacto de un incidente.

En ambos casos, la notificación es obligatoria tanto si se trata de redes y servicios propios como si lo son de proveedores externos, incluso si éstos están sometidos por sí mismos al real decreto ley.

Las notificaciones se practicarán a la autoridad administrativa competente en cada caso, a través del CSIRT (equipo de respuesta a incidentes) de referencia, que será, como regla general, el INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, salvo para las entidades del sector público, en las que el equipo de respuesta será el CCN-CERT, del Centro Criptológico Nacional, y los operadores de servicios esenciales que tengan incidencia en la defensa nacional, en las que el ESPDEF-CERT, del Ministerio de Defensa, cooperará con el CCN-CERT y el INCIBE-CERT. El real decreto ley prevé que las autoridades competentes y los CSIRT de referencia utilicen una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes. Por otra parte, en la medida en que el nuevo Reglamento de Protección de Datos impone igualmente una notificación a la Agencia de Protección de Datos de toda violación de la seguridad de los datos personales y que con frecuencia estos robos de datos serán consecuencia de uno de los ciberincidentes regulados en el real decreto ley, resulta particularmente importante la previsión de colaboración de todas las autoridades afectadas para hacer frente a este tipo de incidentes. En particular, sería fundamental que la colaboración permitiera reducir la carga para el operador de llevar a cabo dos notificaciones distintas a autoridades con exigencias eventualmente muy diferentes.

En fin, el real decreto ley prevé expresamente que los empleados y el personal que informen sobre ciberincidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los casos en que se acredite mala fe en su actuación.

3) En tercer lugar, los operadores de servicios esenciales y los proveedores de servicios digitales están *obligados a resolver los incidentes* de seguridad que les afecten *y a solicitar ayuda especializada*, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes. Igualmente, deben suministrar al CSIRT de referencia y a la autoridad competente toda la información que éstos les requieran para el desempeño de sus funciones.

3. Supervisión y sanciones

La supervisión del cumplimiento de las obligaciones derivadas del real decreto ley es también más intensa en el caso de los operadores de servicios esenciales, a los que las autoridades competentes pueden, con carácter preventivo, solicitar toda la información que consideren necesaria para evaluar la seguridad de las redes y sistemas, así como exigir que sometan éstas a una auditoría por una entidad externa y, en todo caso, requerirle que subsane las deficiencias detectadas. En el caso de los proveedores de servicios digitales, por el contrario, las

inspecciones sólo podrán llevarse a cabo cuando la autoridad tenga noticia de algún incumplimiento. La constatación de tales incumplimientos podrá sancionarse —de acuerdo con la gravedad de la infracción y de factores como el grado de culpabilidad, la cuantía de los perjuicios causados, el número de usuarios afectados, la continuidad o persistencia de la conducta infractora, etcétera — con multas de hasta un millón de euros o, en el caso de las infracciones menos graves, con una simple amonestación.

El futuro desarrollo reglamentario del real decreto ley está llamado a desempeñar un papel importante, no obstante, en la precisión del contenido de estas obligaciones y del procedimiento para cumplirlas.