BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XII LEGISLATURA

Serie A:
PROYECTOS DE LEY **7 de marzo de 2019** **Núm. 28-2** **Pág. 1**

ENMIENDAS E ÍNDICE DE ENMIENDAS AL ARTICULADO

121/000028 Proyecto de Ley de seguridad de las redes y sistemas de información (procedente del Real Decreto-ley 12/2018, de 7 de septiembre).

En cumplimiento de lo dispuesto en el artículo 97 del Reglamento de la Cámara, se ordena la publicación en el Boletín Oficial de las Cortes Generales de las enmiendas presentadas en relación con el Proyecto de Ley de seguridad de las redes y sistemas de información (procedente del Real Decreto-ley 12/2018, de 7 de septiembre), así como del índice de enmiendas al articulado.

Palacio del Congreso de los Diputados, 27 de febrero de 2019.—P.D. El Secretario General del Congreso de los Diputados, **Carlos Gutiérrez Vicén.**

A la Mesa de la Comisión de Economía y Empresa

El Grupo Parlamentario Vasco (EAJ-PNV), al amparo de lo establecido en el artículo 110 y siguientes del Reglamento de la Cámara presenta las siguientes enmiendas al articulado al Proyecto de Ley de seguridad de las redes y sistemas de información (procedente del Real Decreto-ley 12/2018, de 7 de septiembre.

Palacio del Congreso de los Diputados, 16 octubre de 2018.—**Aitor Esteban Bravo**, Portavoz del Grupo Parlamentario Vasco (EAJ-PNV).

ENMIENDA NÚM. 1

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 2, apartado 1, letra a)

De modificación.

Debe decir:

«1. Esta Ley se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Se entenderá, a los efectos de esta Ley, que el sector identificado como "administración" en dicho anexo de la Ley 8/2011 queda referido únicamente a los organismos de las administraciones públicas que presten un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales siempre que la prestación de dicho servicio depende de las redes y sistemas de información y un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

La Directiva NIS en su exposición de motivos expresamente manifiesta que se «aplica únicamente a las administraciones públicas que hayan sido identificadas como operadores de servicios esenciales». Por ese motivo, continúa la Directiva «es responsabilidad de los Estados miembros garantizar la seguridad de las redes y sistemas de información de las administraciones públicas que no estén incluidas en el ámbito de aplicación de la presente Directiva». Se comprueba lo dicho al examinar el artículo 4 de la Directiva quienes son a tales efectos operadores de servicios esenciales (los que figura en el anexo II que reúnan los requisitos del artículo 5.2) Por el contrario el Real Decreto-ley define su ámbito por remisión a los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Y en dicho anexo se incluye como sector estratégico genérico al de la «Administración», por lo tanto ello implica extender la normativa NIS al conjunto de la actividad de las administraciones.

Lo anterior implica que la Ley se aplicaría, potencialmente, sobre todas las redes y servicios de la información autonómicos poniendo en manos del Estado la supervisión de las mismas y el régimen sancionador atribuyendo tal supervisión en última instancia al Centro Nacional de Inteligencia a través del Centro Criptológico se integra y depende del CNI.

Consideramos que el control que se pretende ejercer en teoría sobre cualquier actividad de las administraciones públicas que unilateralmente se decida atendiendo al artículo 6 del Real Decreto-ley, no es acorde con el principio de autonomía institucional de las mismas, particularmente de las Comunidades Autónomas, no se justifica en la recepción de la Directiva europea NIS (que no incluye a las administraciones públicas genéricamente en su ámbito), ni resulta necesario ni proporcionado a los efectos de salvaguardar la coordinación de las medidas de seguridad de las redes y sistemas de información entre administraciones públicas, para lo cual cabe, en su caso, arbitrar los ordinarios mecanismos de cooperación y coordinación ya contemplados en nuestro ordenamiento.

ENMIENDA NÚM. 2

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 2, apartado 3, letras a) y b)

De modificación.

Debe decir:

«3. Este Real Decreto-ley no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) A los operadores de redes y servicios de información dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos. Quedan incluidos en esta excepción, los Cuerpos policiales dependientes de las Comunidades Autónomas con competencias estatutarias reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.»

JUSTIFICACIÓN

La redacción del artículo 2.3 letra a) puede resultar confusa en su aplicación práctica y parece más razonable que se excluya expresamente del ámbito de la ley a las redes y servicios informáticos de las

cve: BOCG-12-A-28-2

fuerzas armadas y fuerzas y cuerpos de seguridad, los cuales deberán disponer de medidas de salvaguarda específicas, lo cual no choca con la Directiva NIS, que no incluye dentro de su ámbito a estos servicios y, lo que es más importante, están excluidas ya de la normativa de protección de infraestructuras críticas (PIC). Tal sería la consecuencia del juego de remisiones que establece el Real Decreto-ley a la normativa PIC aun cuando no se introdujera ninguna precisión y aunque la conclusión sea esa nos parece oportuno en aras a una mayor seguridad jurídica introducir la exclusión expresa de las redes y servicios informáticos dependientes de Defensa y de las fuerzas y cuerpos de seguridad.

ENMIENDA NÚM. 3

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 3

De modificación.

Se modifica la letra «e» del artículo 3, que debe decir:

«e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogida en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, **siempre que sea uno de los tipos que figuran en el anexo III de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.»**

JUSTIFICACIÓN

La definición de servicio digital también es más amplia de lo previsto en la Directiva. Concretamente, convendría precisar, como indica el artículo 4.5, que se refiere únicamente a los tipos de servicios que figuran en el anexo III de la Directiva.

De este modo, la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico al que se refiere el Anteproyecto de Ley, no limita el concepto de servicio de la sociedad de la información a mercado en línea, motor de búsqueda en línea y servicios de computación en la nube, como indica la Directiva en el anexo III, sino que habla de «todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

«1.º La contratación de bienes o servicios por vía electrónica. 2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales. 3.º La gestión de compras en la red por grupos de personas. 4. 9 El envío de comunicaciones comerciales. 5.º El suministro de información por vía telemática».

Esto va más allá de las facultades que la Directiva otorga a los Estados miembros en relación con los Prestadores de Servicios Digitales, rompiendo con la ambiciosa armonización en el ámbito europeo.

---

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 4

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 3, letra g)

De modificación.

Se modifica el epígrafe «g» del artículo 3.

«g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información.»

JUSTIFICACIÓN

La definición de riesgo del Real Decreto-ley español también va más allá de la definición prevista en la Directiva (art. 4.9), añadiendo que el riesgo «se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen».

La redacción usada también induce a excluir otras metodologías de análisis de riesgo de eficacia demostrada y/o aceptadas a nivel internacional como las basadas en escenarios, las basadas en la valoración de las dimensiones CID o ACIDA, u otras que en el futuro pudieran desarrollarse.

En un ámbito como el del análisis de riesgos, donde se investigan continuamente posibles metodologías de mayor efectividad que las actuales, la limitación en las metodologías viables puede lastrar significativamente a los sectores públicos y privados nacionales, al obligarles a seguir metodologías de análisis de riesgo subóptimas.

En este sentido, ni la directiva ni los marcos de referencia más reconocidos y/o extendidos a nivel internacional (ISO 27001, NIST SP800) limitan las metodologías de análisis de riesgos aplicables a una única opción.

Teniendo en cuenta que la Directiva faculta a la Comisión Europea, y al Grupo de Trabajo que bajo su amparo se crea, a dictar recomendaciones y actos de ejecución que probablemente maticen e interpreten muchos de los conceptos recogidos en la Directiva, se propone la supresión de dicho inciso en aras de cumplir con la necesaria armonización a nivel europeo, y así permitir que términos tan relevantes y que podrían incidir de manera tan significativa en la implementación de las obligaciones de la Directiva como la definición de riesgo tengan una interpretación común en todos los Estados miembros.

ENMIENDA NÚM. 5

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 3, letra h)

De modificación.

Se modifica la letra «h» del artículo 3, que debe decir:

«g) Incidente: suceso inesperado o no deseado **con efectos adversos reales** en la seguridad de las redes y sistemas de información.»

JUSTIFICACIÓN

La definición de incidente. Si bien se aplaude la introducción de la referencia a «inesperado o no deseado» a la definición que la Directiva hace sobre incidente, preocupa que se hable de «consecuencias»,

cve: BOCG-12-A-28-2

sin más matización, dado que cualquier mínimo aspecto puede tener consecuencias también mínimas, lo que no justifica su consideración como incidente.

ENMIENDA NÚM. 6

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 3, letra s)

De modificación.

Se modifica la letra «s» del artículo 3, que debe decir:

«s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir, **en su modalidad de** Infraestructura **como Servicio o "IaaS."»**

JUSTIFICACIÓN

El alcance de la directiva no afecta a todo tipo de servicios en la nube. Existen por lo menos tres modalidades:

1. SaaS o Software como servicio.
2. PaaS o Plataforma como servicio.
3. IaaS o Infraestructura como servicio.

Ya que se ha propuesto en el anteproyecto una definición amplia de «Cloud Computing», resulta necesario acotar la modalidad del servicio que es relevante para efectos de la directiva.

ENMIENDA NÚM. 7

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 7

De adición.

Se añade un nuevo párrafo, que debe decir:

«Artículo 7. Comunicación de actividad por los proveedores de servicios digitales.

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

A efectos de identificar un interlocutor principal en el organigrama del proveedor de servicios digitales para la comunicación y tratamiento de las obligaciones impuestas por la ley se recomienda la identificación y asignación de la figura organizativa de Responsable de Seguridad Corporativa (CISO).»

JUSTIFICACIÓN

La forma, punto de contacto y modelo para la comunicación a la autoridad competente del inicio de actividad resulta impreciso. Se debe evitar incumplimiento por desconocimiento.

cve: BOCG-12-A-28-2

Por los mismos motivos que la ley establece un punto de contacto único para las administraciones públicas de los Estados miembros, se debe recomendar la existencia de una figura organizativa (CISO) en los OSE y PSD, cuya misión sea la de coordinar internamente la aplicación efectiva de la ley y todas las disposiciones que de ella se deriven, así como servir de punto de interlocución principal con las Autoridades Competentes.

ENMIENDA NÚM. 8

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Nuevo artículo 9.bis

De adición.

Debe decir:

«Artículo 9.bis. Comunidades Autónomas

Las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público que dispongan de policía propia podrán desarrollar, sobre las redes y sistemas de información referidos a los sectores y ámbitos de su competencia, las facultades que se prevén en el artículo 10 respecto a su protección, siéndoles de aplicación los preceptos de la Ley referidos a las autoridades competentes y sin perjuicio de los mecanismos de coordinación que se establezcan en aplicación del artículo 14.»

JUSTIFICACIÓN

El texto del Real Decreto-ley no confiere papel alguno a las CC.AA., más allá del cumplimiento pasivo de la norma, cuando la legislación que esta transposición toma por referencia, la legislación de protección de infraestructuras críticas confiere un papel activo a las Comunidades Autónomas tanto al relacionar las atribuciones de la norma con la competencia sectorial correspondiente, como al conferir funciones de supervisión a las comunidades autónomas con responsabilidades en seguridad y orden públicos, sin que ello menoscabe la integralidad del sistema de protección de las infraestructuras críticas.

Es por ello, que en la determinación de las autoridades competentes debe atenderse a la competencia sectorial que corresponda conforme a la competencia constitucional de los sectores y servicios que figuran en los anexos al Real Decreto-ley. La Directiva NIS no excluye que cada Estado nombre una o varias autoridades. La existencia de varias autoridades competentes no impide que se designe un punto de contacto único en materia de seguridad de las redes y sistemas de información, tal como exige la Directiva.

ENMIENDA NÚM. 9

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 10, letra g)

De modificación.

cve: BOCG-12-A-28-2

Se modifica la letra g) del artículo 10, que debe decir:

«g) Cooperar, en el ámbito de aplicación de esta **ley,** con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las otras autoridades competentes conforme a lo establecido en los **artículos 9 y 9 bis,** así como con las autoridades **sectoriales** correspondientes conforme a lo establecido en los artículos 14 y 29.»

JUSTIFICACIÓN

Entre todas las autoridades con las que se cooperará no figuran explícitamente el resto de autoridades competentes ya señaladas en anteriores artículos. Esta necesidad de cooperación sí que se establece para los CSIRT en el artículo 11.2, y de forma no explícita en el artículo 14.

Las autoridades competentes deben cooperar también entre ellas. Es de esperar y la ausencia de esta obligación no resulta adecuada estéticamente.

En concreto, consideramos que es importante sostener y facilitar el ejercicio de esta cooperación siguiendo el ordenamiento territorial existente en el conjunto del Estado, incluyendo aquellas autoridades y CSIRT autonómicos que estén adecuadamente reconocidos y que tienen establecidas las relaciones de colaboración y confianza con las empresas de su ámbito geográfico, por lo que se constituyen como un órgano fundamental en la coordinación para la respuesta frente a amenazas e incidentes de seguridad.

ENMIENDA NÚM. 10

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 11, apartado 2

De modificación.

Se modifica el apartado 2, del artículo 11 que debe decir:

«2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT **autonómicos,** nacionales e internacionales **designados específicamente para la** respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.»

JUSTIFICACIÓN

Coherencia con la enmienda de adición de un nuevo artículo 11 bis.

ENMIENDA NÚM. 11

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Nuevo artículo 11 bis

De adición.

cve: BOCG-12-A-28-2

Debe decir:

«Artículo 11 bis. CSIRT autonómicos de referencia.

Las comunidades autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y el mantenimiento del orden público, que dispongan de policía propia, podrán crear, con los requisitos establecidos en el artículo 12 de esta Ley, sus propios CSRIT de referencia para prestar servicios de asesoramiento, alerta temprana y respuesta ante incidentes a entidades públicas o privadas establecidas en su territorio así como, en coordinación con los CSRIT de referencia estatal, para los operadores críticos designados conforme a la Ley 8/2011, de 28 de abril.

Los CSIRT de referencia autonómica se coordinarán con los CSRIT de referencia estatal, en función de las competencias de cada uno de ellos, a través de los instrumentos de cooperación, información y notificación establecidos en la normativa aplicable.»

JUSTIFICACIÓN

Proponemos que expresamente se diga que las Comunidades Autónomas, con competencias en materia de seguridad, podrán crear sus equipos de respuesta a incidentes de seguridad informática (CSIRT) con los requisitos establecidos en el artículo 12 de esta Ley para prestar servicios de asesoramiento, alerta temprana y respuesta ante incidentes a entidades públicas o privadas establecidas en su territorio. Y que tales CSIRT autonómicos puedan ejercer (en coordinación con el CSIRT de referencia estatal) de centros de referencia en materia de seguridad de las redes y sistemas de información, para los operadores de servicios esenciales y proveedores de servicios digitales que sean operadores esenciales y dependan de su propia Administración y sector público.

Contemplar la posibilidad de la existencia de tales centros autonómicos y su coordinación con los CSIRT estatales de referencia es un modo realista de potenciar la efectividad de los recursos ya disponibles. En tal sentido el documento «Estrategia de seguridad nacional» contempla la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre los CERT estatales y los CERT de las CC.AA. En el mismo sentido la Ley 36/2015 (arts. 6 y 11).

ENMIENDA NÚM. 12

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 14

De modificación.

Debe decir:

«Artículo 14. Cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales.

1. Las autoridades competentes, los CSIRT de referencia, **de ámbito nacional y autonómicos,** y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.

2. Consultarán así mismo, cuando proceda, con los órganos con competencias por razón de la materia en cada **una de las Comunidades Autónomas, así como en cada** uno de los sectores incluidos en el ámbito de aplicación de este Real Decreto-ley, y colaborarán con ellos en el ejercicio de sus funciones.

cve: BOCG-12-A-28-2

3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia **correspondientes** darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello.

4. Las autoridades competentes estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.»

JUSTIFICACIÓN

En coherencia con enmiendas anteriores.

ENMIENDA NÚM. 13

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 16

De modificación.

Debe decir:

«1. (igual).

2. El desarrollo reglamentario **de esta ley** preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.

3. (igual).

4. Las autoridades competentes podrán establecer mediante **disposiciones reglamentarias,** obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales, **entre ellas la exigencia de auditorías externas y la redacción de proyectos técnicos.** Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas **disposiciones reglamentarias.**

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, **los estándares internacionales y marcos de referencia de controles de seguridad generalmente aceptados,** las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, **por la que se establecen medidas para la protección de las infraestructuras críticas,** y el Real Decreto 3/2010, de 8 de enero, **por el que se regula** el Esquema Nacional de Seguridad **en el ámbito de la administración electrónica.**

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia con objeto de evitar **inconsistencias y** duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

6. (igual).»

JUSTIFICACIÓN

Entre las fuentes de referencia para el diseño de medidas de seguridad citadas en el apartado 4 no se citan estándares internacionales, marcos de referencia, cuerpos de conocimiento y otras fuentes de buenas prácticas ampliamente reconocidas y ya utilizadas y desplegadas en empresas del sector privado.

La administración debería tomar en consideración como fuente de información (incluso de manera incluso principal) las buenas prácticas ya desarrolladas internacionalmente, que son exigibles y requeridas

cve: BOCG-12-A-28-2

para otros ámbitos y que se han demostrado efectivas, en los niveles de exigencia solicitados por el mercado.

Sería desastroso para la competitividad internacional del sector privado que alguna autoridad competente (incluso sectorial) decidiera de forma autónoma la aplicación de controles de seguridad no consecuentes con los marcos de referencia habituales en el mercado, o en niveles de exigencia superiores, que obligasen a incurrir en costes elevados para el sector privado.

Esta regulación no debería influir negativamente en la competitividad del sector por sobre-regulación o sobre-exigencia […] menos aún por una exigencia inconsistente con el mercado.

En la coordinación entre autoridades sobre guías, instrucciones y similares, solo se indica la posibilidad de duplicidades. Pero no se contempla la posibilidad de inconsistencia entre estos elementos. Resulta más viable el cumplimiento de dos instrucciones duplicadas que pidan el mismo requisito, que dos instrucciones que pidan requisitos diferentes o directamente contradictorios.

ENMIENDA NÚM. 14

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo. 22, apartado 1

De modificación.

Debe decir:

«1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 19.1 en un **plazo máximo de 72 horas desde que el operador identificase el incidente.»**

JUSTIFICACIÓN

El artículo 22.1 requiere realizar una primera notificación «sin dilación indebida». Pero no se fija un plazo para notificar, aunque sea máximo.

Dado que el Reglamento General de Protección de Datos ha establecido un plazo máximo de 72 horas para la notificación, que ya es conocido por las organizaciones y ha sido ampliamente difundido, se considera muy efectivo utilizar también ese plazo. La Directiva no prohíbe ni fija plazo alguno. Este cambio es consistente con el Artículo, puesto que este artículo se refiere a las notificaciones intermedias.

ENMIENDA NÚM. 15

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 24

De modificación.

Se modifica el artículo 24.

«Artículo 24. Incidentes que afecten a servicios digitales.

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a ley, ~~así como cualquier otra parte interesada~~, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros

cve: BOCG-12-A-28-2

Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que estuviese establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o de notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.»

JUSTIFICACIÓN

El artículo 24 introduce un régimen que puede afectar de manera adversa a la armonización y seguridad jurídica pretendida por la Directiva.

En concreto, el artículo 24 prevé la posibilidad de que «los operadores de servicios esenciales y los proveedores de servicios digitales sometidos» a la ley española o «cualquier otra parte interesada» notifiquen un incidente de proveedores establecidos en otros Estados miembros, mientras que la Directiva prevé la obligación de que los propios sujetos obligados sean los que realicen la notificación. El procedimiento previsto por la Directiva es el único que puede otorgar la seguridad jurídica necesaria, ya que sólo los sujetos obligados son capaces de determinar si un determinado suceso constituye un incidente notificable.

Permitir que cualquier otra parte notifique el incidente sólo conllevaría inseguridad jurídica y el bloqueo del sistema. En primer lugar, no se entiende cómo cualquier persona distinta del propio sujeto obligado puede disponer de la información suficiente como para poder tener certeza de que efectivamente se ha producido un incidente notificable. En segundo lugar, y como consecuencia de lo anterior, es preciso tener en cuenta que la incorporación de este cambio respecto al régimen previsto por la Directiva podría implicar un colapso significativo en la labor de las autoridades, que pasarían a recibir un número muy superior de notificaciones al que recibirán otros Estados miembros también sujetos a la Directiva y que no tengan una regulación al margen de la misma.

De otro lado, este sistema implicaría un alto riesgo de proliferación de notificaciones infundadas y que sólo tendrían como objetivo atacar a los proveedores establecidos en otros Estados miembros. Ello implicaría que las autoridades y los prestadores de servicios estén más ocupados intentando gestionar el abundante número de notificaciones recibidas e identificando aquellas que realmente son verídicas y fundadas que promoviendo la correcta aplicación del sistema y trabajando en la mejora de la seguridad.

Todo ello va en contra de los propios objetivos de la Directiva y conduciría al fracaso del sistema.

ENMIENDA NÚM. 16

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 27, apartado 3

De adición

Debe decir:

«3. A la confirmación de remisión del informe anual, las autoridades competentes y los CSIRT eliminarán los datos facilitados por los operadores de servicios esenciales y los proveedores de servicios digitales durante el reporte de incidentes, para todos los incidentes desde cuya fecha de cierre hayan transcurrido más de doce meses, pudiendo conservar únicamente aquellos incidentes que aún no se hayan cerrado, o aquellos que se hayan cerrado en los últimos doce meses. Cada autoridad competente y cada CSIRT mantendrá un registro de los incidentes que se han eliminado en este proceso.»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

El Proyecto de Ley no contiene ninguna previsión relativa al tratamiento histórico de la información sobre incidentes comunicada a las autoridades competentes o a los CSIRT.

Una vez comunicado el incidente, resuelto el mismo, y obtenido la información y el aprendizaje posible de un incidente, la utilidad de la información del incidente se limita al análisis estadístico y de tendencias que cabe esperar del informe anual. Una vez agotada esa información, la disponibilidad de esa información en manos de la administración supone un costo de mantenimiento en términos de recursos de almacenamiento, de medidas de protección y en el peor de los casos un riesgo de filtración con consecuencias reputacionales para las entidades que reportaron el incidente. Por eso, parece razonable limitar estos riesgos mediante la eliminación de la información no necesaria.

ENMIENDA NÚM. 17

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 29

De modificación.

Debe decir:

«Artículo 29. Cooperación en lo relativo a los incidentes que afecten a datos personales.

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos **y con las autoridades autonómicas con competencias en materia de protección de datos personales,** para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos **y a las autoridades autonómicas con competencias en materia de protección de datos personales,** los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.»

JUSTIFICACIÓN

Las referencias que se hacen en el RD Ley a las autoridades de protección de datos, en cuanto a instaurar la necesaria cooperación cuando los incidentes afecten a datos personales, lo son únicamente a la Agencia Española de Protección de datos, ignorando a las autoridades autonómicas que tienen facultades para la protección contra la violación en materia de seguridad de datos personales. Estando en tramitación la Ley Orgánica de Protección de datos donde se materializan las competencias autonómicas en este ámbito, resulta necesario cohonestar ambas normativas.

ENMIENDA NÚM. 18

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 37

De adicion.

cve: BOCG-12-A-28-2

Se añade un nuevo apartado 3 al artículo 37, que debe decir:

«3. El órgano sancionador podrá sustituir la imposición de la sanción económica al infractor, por la exigencia de dedicación en un plazo inferior a tres meses de presupuesto adicional igual al volumen de la sanción propuesta, destinado a la mejora de la seguridad de la organización.»

JUSTIFICACIÓN

El régimen sancionador establecido se centra en sanciones meramente económicas, de efecto disuasorio en el mejor de los casos. El montante de las sanciones económicas establecidas puede inducir a que se perciban con un fin recaudatorio, más que disuasorio. ~~En particular, cuando las administraciones públicas no tienen establecida sanción económica alguna.~~

Asegurar que las sanciones económicas se destinan a la mejora de la seguridad del afectado por el incidente resultará de una mayor efectividad en la aplicación de la regulación y en un mejor servicio al usuario.

ENMIENDA NÚM. 19

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 38

De modificación.

Debe decir:

«El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) (igual)
b) (igual)
c) (igual)
d) La reincidencia, por comisión en el **término de un** ~~año~~ de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.
e) (igual)
f) (igual).
g) La utilización por el responsable de programas de **gestión de vulnerabilidades técnicas o** de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
h) (igual)
i) La disponibilidad de información previa sobre las causas que han provocado el incidente y la imposibilidad de haber tomado medidas preventivas por desconocimiento de las mismas.»

JUSTIFICACIÓN

Se cita como atenuante el establecimiento de programas de recompensa por el descubrimiento de vulnerabilidades, pero no valora como tal el establecimiento de un proceso de gestión de vulnerabilidades, mucho más extendido en la actualidad y de mucha mayor eficiencia.

Tampoco se hacen mención a otras medidas preventivas, tales como la concienciación de personal, o la imprevisibilidad del incidente, si responde a un incidente de seguridad conocido o un Zero-day.

Ninguna organización puede asegurar que sus sistemas son 100 % seguros, pero si debe exigirse haber tomado las medidas preventivas adecuadas (formación u otras). Asimismo, tampoco puede culpabilizarse a una organización de haber sido escogida como primer target por atacantes que dispongan de vulnerabilidades Zero-day. Si no se declara este eximente, la organización podría tener una triple

cve: BOCG-12-A-28-2

penalización: sufrir una incidencia, dedicación de recursos a su rápida resolución y, adicionalmente, una cuantiosa sanción ante la que no ha podido tomar ninguna acción que la evitase.

ENMIENDA NÚM. 20

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 40

Subsidiaria de supresión.

Debe suprimirse el artículo 40.

JUSTIFICACIÓN

Se propone la supresión de dicho artículo para el caso de que no se acepte nuestra enmienda al artículo 41 por las razones expuestas en la justificación a dicha enmienda.

ENMIENDA NÚM. 21

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

Al artículo 41

De modificación.

Debe decir:

«Artículo 41. Competencia sancionadora.

1. (igual)
2. (igual)
3. (igual)
4. **De conformidad con los artículos 9 bis y 10.i) se entenderá que la imposición de sanciones referidas a los sectores y ámbitos de la competencia de las Comunidades Autónomas** ~~a las que se refiere el artículo 9 bis de esta Ley~~**, corresponderá a los órganos por ellas designados.»**

JUSTIFICACIÓN

Mediante la enmienda de adición de un nuevo artículo 9 bis, se contempla como autoridades competentes en esta Ley a las CC.AA. con competencias en materia de protección de personas y bienes y para el mantenimiento del orden público que dispongan de policía propia que podrán desarrollar, sobre las redes y sistemas de información referidos a los sectores y ámbitos de su competencia, las facultades que se prevén en el artículo 10 respecto a su protección. Una de las facultades de dicho artículo, bajo la letra i), es el ejercicio de la potestad sancionadora en los casos previstos en el título VII de la Ley. Por ello debe cohonestar tal previsión con el artículo 41 que prevé los órganos que ejercerán la potestad sancionadora.

En todo caso, y de no ser así, lo previsto en el artículo 40, en relación a las infracciones cometidas por las Administraciones Públicas, ignoraría el principio de autonomía en cuanto prevé que el órgano sancionador, proponga actuaciones disciplinarias, y dicho órgano en el actual artículo 41 se refiere a

cve: BOCG-12-A-28-2

órganos del Estado (Ministro competente). Estamos ante un régimen sancionador que visualiza a las Comunidades Autónomas y a las Entidades Locales como una Unidad administrativa más dentro de la estructura de la Administración estatal.

ENMIENDA NÚM. 22

FIRMANTE:

Grupo Parlamentario Vasco (EAJ-PNV)

A la disposición adicional tercera

De modificación.

«Disposición adicional tercera. Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este Real Decreto-ley.

La plataforma común para la notificación de incidentes prevista en este Real Decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el 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, en los términos que acuerden la Agencia Española de Protección de Datos, **las autoridades autonómicas con competencias en materia de protección de datos personales** y los órganos que gestionen dicha plataforma.»

JUSTIFICACIÓN

En coherencia con la enmienda al artículo 29.

A la Mesa de la Comisión de Economía y Empresa

El Grupo Parlamentario Ciudadanos, al amparo de lo establecido en el artículo 110 y siguientes del vigente Reglamento del Congreso de los Diputados, presenta la siguiente enmienda de articulado al Proyecto de Ley de seguridad de las redes y sistemas de información, procedente del Real Decreto-ley 12/2018, de 7 de septiembre.

Palacio del Congreso de los Diputados, 21 de febrero de 2019.—**Miguel Ángel Gutiérrez Vivas,** Portavoz del Grupo Parlamentario Ciudadanos.

ENMIENDA NÚM. 23

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 2

De modificación.

Texto que se propone:

«Artículo 2. Ámbito de aplicación.

Esta ley ~~Este real decreto ley~~ se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información ~~comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se~~

cve: BOCG-12-A-28-2

~~establecen medidas para la protección de las infraestructuras críticas~~ **conforme aparecen listados en el anexo II, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, y en el anexo I, de la presente ley.**

b) Los servicios digitales, considerados conforme se determina en el artículo 3.e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.»

Texto que se sustituye:

«Artículo 2. Ámbito de aplicación.

Este Real Decreto-ley se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales, considerados conforme se determina en el artículo 3.e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.»

JUSTIFICACIÓN

En la actualidad el artículo 2.1 amplía la definición de Operador de Servicios Esenciales (OSE) en comparación con la Directiva, al incluir la definición de la Ley 8/2011. Esto no es un problema per sé, pero puede ocasionar problemas de cooperación con otros Estados miembros, al existir incoherencias que surjan de la propia definición de OSE.

En consecuencia, con el objeto de cumplir con lo previsto en la Directiva de forma armonizada en Europa, sería necesario precisar que los servicios esenciales son aquellos que aparecen listados en el anexo II, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esto se puede realizar en el artículo 2.1 o en el artículo 3 de definiciones, o en ambos, tal cual se propone.

ENMIENDA NÚM. 24

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 3 c)

De modificación.

Texto que se propone:

«Artículo 3. Definiciones.

A los efectos de **esta Ley** ~~este real decreto ley~~, se entenderá por:

[…]

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones ~~sociales~~ básicas~~, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de las redes y sistemas de información~~ **de aquellos que aparecen listados en el anexo II, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, y en el anexo I, de la presente ley.»**

cve: BOCG-12-A-28-2

Texto que se sustituye:

«Artículo 3. Definiciones.

A los efectos de este Real Decreto-ley, se entenderá por:

[…]

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de las redes y sistemas de información.»

JUSTIFICACIÓN

La definición de servicio esencial es mucho más amplia de lo previsto en la Directiva. Tal y como está formulada, sería muy difícil discernir entre un servicio esencial y otro que no lo es, especialmente cuando el texto del real proyecto de Ley refiere a «… mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de las redes y sistemas de información».

En consecuencia, con el objeto de cumplir con lo previsto en la Directiva de forma armonizada en Europa, sería necesario precisar que los servicios esenciales son aquellos que aparecen listados en el anexo II, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

ENMIENDA NÚM. 25

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 3 e)

De modificación.

Texto que se propone:

«Artículo 3. Definiciones.

A los efectos de **esta Ley** ~~este real decreto ley~~, se entenderá por:

[…]

e) Servicio digital: servicio de la sociedad de la información ~~entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico,~~ **conforme figura en el anexo III de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, y en el anexo II, de la presente ley.**

[…]»

Texto que se sustituye:

«Artículo 3. Definiciones.

A los efectos de este Real Decreto-ley, se entenderá por:

[…]

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[…]»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

La definición de servicio digital es más amplia de lo previsto en la Directiva. Concretamente, convendría precisar, como indica el artículo 4.5, que se refiere únicamente a los tipos de servicios que figuran en el anexo III de la Directiva.

De este modo, la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico al que se refiere el proyecto de Ley, no limita el concepto de servicio de la sociedad de la información a mercado en línea, motor de búsqueda en línea y servicios de computación en la nube, como indica la Directiva en el anexo III, sino que habla de todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.
2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3.º La gestión de compras en la red por grupos de personas.
4.º El envío de comunicaciones comerciales.
5.º El suministro de información por vía telemática.

Esto va más allá de las facultades que la Directiva otorga a los Estados miembros en relación con los prestadores de servicios digitales, rompiendo con la ambiciosa armonización en el ámbito europeo. Por ello, se propone la modificación de este apartado.

ENMIENDA NÚM. 26

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 3 g)

De supresión.

Texto que se suprime:

«Artículo 3. Definiciones.

A los efectos de **esta Ley** ~~este real decreto ley~~, se entenderá por:

[…]

~~g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza.~~»

JUSTIFICACIÓN

La definición de riesgo del Proyecto de Ley español va más allá de la definición prevista en la Directiva (artículo 4.9), añadiendo que el riesgo «se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen».

La redacción usada induce a excluir otras metodologías de análisis de riesgo de eficacia demostrada y/o aceptadas a nivel internacional como las basadas en escenarios, las basadas en la valoración de las dimensiones CID o ACIDA, u otras que en el futuro pudieran desarrollarse.

---

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 27

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 6.1

De modificación.

Texto que se propone:

«Artículo 6. Identificación de servicios esenciales y de operadores de servicios esenciales.

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Se identificará a un operador como operador de servicios esenciales bajo los siguientes criterios: ~~si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:~~

a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;

b) la prestación de dicho servicio depende de las redes y sistemas de información, y

c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.»

Texto que se sustituye:

«Artículo 6. Identificación de servicios esenciales y de operadores de servicios esenciales.

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Se identificará a un operador como operador de servicios esenciales si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:

a) En relación con la importancia del servicio prestado:

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial.

2.º La valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública.

b) En relación con los clientes de la entidad evaluada:

1.º El número de usuarios que confían en los servicios prestados por ella.

2.º Su cuota de mercado.

cve: BOCG-12-A-28-2

Reglamentariamente podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.»

JUSTIFICACIÓN

El artículo 6.1 del RDL reformula los criterios del artículo 5.2 de la Directiva, cosa que no hacía falta, al ser la Directiva clara y coherente. El RDL no aporta nada, salvo una clasificación en categorías y una diferente organización que sólo redunda en complicar más la norma. No hacía falta extender la Directiva en esta dirección, pues esta era clara. Se propone reformular 6.1 para hacerlo coincidir con el articulado 5.2 de la Directiva.

ENMIENDA NÚM. 28

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 7

De modificación.

Texto que se propone:

«Artículo 7. Comunicación de actividad por los proveedores de servicios digitales.

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a ~~la autoridad competente~~ **la Secretaría de Estado encomendada con la gestión principal del presupuesto para la innovación tecnológica de las telecomunicaciones,** en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

A efectos de identificar un interlocutor principal en el organigrama del proveedor de servicios digitales para la comunicación y tratamiento de las obligaciones impuestas por la Ley, se recomienda la identificación y asignación de la figura organizativa de Responsable de Seguridad Corporativa (RSC).

Los protocolos concretos de comunicación se desarrollarán reglamentariamente por parte de la Secretaría de Estado.»

Texto que se sustituye:

«Artículo 7. Comunicación de actividad por los proveedores de servicios digitales.

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.»

JUSTIFICACIÓN

La forma, punto de contacto y modelo para la comunicación a la autoridad competente del inicio de actividad resulta impreciso. Se debe evitar incumplimiento por desconocimiento. Se sugiera que este punto de contacto sea la Secretaría de Estado.

Se propone señalar explícitamente que se desarrollará reglamentariamente la forma de esta comunicación.

Por los mismos motivos que la Ley establece un punto de contacto único para las Administraciones Públicas de los Estados miembros, se debe recomendar la existencia de una figura organizativa (RSC) en los Operadores de Servicios Electrónicos (OSE) y Proveedores de Servicios Digitales (PSD), cuya misión sea la de coordinar internamente la aplicación efectiva de la ley y todas las disposiciones que de ella se deriven, así como servir de punto de interlocución principal con las autoridades competentes.

---

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 29

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 9, punto 1 y 3 (nuevo)

De adición.

Texto que se propone:

«1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) […]
b) […]
c) […]

En el caso de que un mismo proveedor de servicio a varios sectores, deberá comunicarlo a todas las autoridades competentes para que estas determinen, de acuerdo al criterio fijado por el Consejo de Seguridad Nacional, el interlocutor único de dicho proveedor.

[…]

3. El Consejo de Seguridad Nacional será asimismo el encargado de fijar la estrategia nacional de seguridad de las redes y sistemas de información, estableciendo los objetivos estratégicos y las medidas normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. La estrategia nacional de seguridad de las redes y sistemas de información se revisará bianualmente o de manera excepcional ante nuevas amenazas de seguridad. Esta estrategia abordará objetivos, prioridades, funciones y responsabilidades de las distintas instituciones implicadas, programas de educación, concienciación e investigación, plan de evaluación de riesgos y listado de los agentes que participan en la ejecución de la estrategia de seguridad de las redes y sistemas de información.»

Texto que se sustituye:

«1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) […]
b) […]
c) […].»

JUSTIFICACIÓN

Tenemos aquí un modelo complejo en exceso porque opera en función de tres opciones que, a su vez, dependen de la categoría de los sujetos. Es incluso difícil de escribir. El CNPIC es autoridad competente para OSE que sean operadores críticos conforme a otra ley. La autoridad sectorial correspondiente (que no se sabe qué es) lo será para los OSE que no sean críticos. La Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa, para los proveedores de servicios digitales (PSD), el Centro Criptológico Nacional para PSD y OSE que sean operadores críticos y se encuentren bajo el régimen jurídico de la Administración del Estado… y todo ello supuestamente coordinador por el Consejo de Seguridad Nacional. Todo esto supone varios problemas de concepto básicos, como que un mismo proveedor de servicios puede dar servicio a varios sectores y por tanto tener varios organismos competentes. Resulta, por tanto, una fuente de problemas, más allá de que esta estructura genera mucha burocracia infructuosa.

Por otra parte, el artículo 7 de la directiva marca la necesidad de definir un marco de seguridad de las redes de los servicios sensibles. Se supone que la normativa española debería dejar claro cuál es ese marco de seguridad, incluyendo objetivos, estrategia, medidas concretas y procedimiento de seguimiento. España

cve: BOCG-12-A-28-2

cuenta con una estrategia de ciberseguridad nacional desde 2013, que se supone obsoleta para lo rápido que se actualizan las amenazas. Aunque en el artículo 9 del RDL se comentan las autoridades competentes, se debería aclarar el papel del Consejo de Seguridad Nacional, y podría haberse concretado la periodicidad de sus actualizaciones o el modo en que dichos cambios serán transpuestos a las empresas que ofrecen servicios sensibles. El nuevo punto que se propone como adición solventa esta duda y especifica la entidad responsable de fijar la estrategia nacional y la periodicidad mínima de sus actualizaciones.

ENMIENDA NÚM. 30

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 16, puntos 2 y 4

De modificación.

Texto que se propone:

«Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

[…]

2. El desarrollo reglamentario de ~~este real decreto~~ **esta Ley** preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.

3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella,

Sus funciones específicas serán las previstas reglamentariamente.

4. Las autoridades competentes ~~podrán establecer~~ **establecerán** mediante orden ministerial, obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales, **entre ellas la exigencia de auditorías externas y la redacción de proyectos técnicos**. Así mismo, ~~podrán dictar~~ **dictarán** instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, **los estándares internacional y marcos de referencia de controles de seguridad generalmente aceptados,** las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

Así mismo, las redes y sistemas de información empleados por los operadores de servicios esenciales podrán verse sometidas a auditorías de seguridad realizadas por la autoridad competente, de manera que se compruebe la idoneidad de las medidas de seguridad aplicadas.

[…]»

Texto que se sustituye:

«Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

[…]

2. El desarrollo reglamentario de este real-decreto preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.

cve: BOCG-12-A-28-2

3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.

Sus funciones específicas serán las previstas reglamentariamente.

4. Las autoridades competentes podrán establecer mediante orden ministerial, obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

[…]»

JUSTIFICACIÓN

Entre las fuentes de referencia para el diseño de medidas de seguridad citadas en el segundo párrafo de este artículo 16.4 no se citan estándares internacionales, marcos de referencia, cuerpos de conocimiento y otras fuentes de buenas prácticas ampliamente reconocidas y ya utilizadas y desplegadas en empresas del sector privado.

La Administración debería tomar en consideración como fuente de información (incluso de manera principal) las buenas prácticas ya desarrolladas internacionalmente, que son exigibles y requeridas para otros ámbitos y que se han demostrado efectivas, en los niveles de exigencia solicitados por el mercado.

Sería desastroso para la competitividad internacional del sector privado que alguna autoridad competente (incluso sectorial) decidiera, de forma autónoma, la aplicación de controles de seguridad no consecuentes con los marcos de referencia habituales en el mercado, o en niveles de exigencia superiores, que obligasen a incurrir en costes elevados para el sector privado.

Esta regulación no debería influir negativamente en la competitividad del sector por sobre-regulación o sobre-exigencia, menos aún por una exigencia inconsistente con el mercado.

En el artículo 16.4 se comenta que las autoridades podrán dar guías y recomendaciones, pero esto no debería ser una opción, sino que estas acciones mínimas deben estar establecidas en el marco europeo y ser de obligado cumplimiento.

Asimismo, las redes deberían exponerse a controles de seguridad, de manera que los CSIRTs hagan ataques preventivos a dichas infraestructuras comprobando su resistencia e identificando fallos de seguridad. Aunque este punto se desarrolla levemente en el artículo 32 del RD, debe incluirse en las obligaciones de los OSE.

ENMIENDA NÚM. 31

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 16, punto 5

De modificación.

Texto que se propone:

«Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

[…]

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia en lo relativo al contenido y a la aplicación de

cve: BOCG-12-A-28-2

las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia con objeto de evitar **inconsistencias o** duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

[…]»

Texto que se sustituye:

«Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

[…]

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

[…]»

JUSTIFICACIÓN

En la coordinación entre autoridades sobre guías, instrucciones y similares, sólo se indica la posibilidad de duplicidades. Pero no se contempla la posibilidad de inconsistencia entre estos elementos. Resulta más viable el cumplimiento de dos instrucciones duplicadas que pidan el mismo requisito, que dos instrucciones que pidan requisitos diferentes o directamente contradictorios.

ENMIENDA NÚM. 32

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 19.1

De modificación.

Texto que se propone:

«Artículo 19. Obligación de notificar.

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios.

Las notificaciones podrán referirse también a los sucesos o incidencias que **tengan** ~~puedan afectar~~ las redes y sistemas de información empleados para la prestación de los servicios, pero que aún no hayan tenido un efecto adverso real sobre aquellos.

[…]»

Texto que se sustituye:

«Artículo 19. Obligación de notificar.

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios.

Las notificaciones podrán referirse también a los sucesos o incidencias que puedan afectar las redes y sistemas de información empleados para la prestación de los servicios, pero que aún no hayan tenido un efecto adverso real sobre aquellos.

[…].»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

Resulta necesario ajustar los tiempos verbales para establecer claramente la obligación de notificación solo en los casos en aquellas situaciones en los que los efectos sean significativos. De utilizarse la expresión «puedan tener» se estaría dando cabida a toda una variedad de situaciones, de consecuencias todavía inciertas, que motivarían la dispersión de los recursos de seguridad.

Adicionalmente, y sin perjuicio de la obligación de informar al CSIRT nacional de referencia, sería conveniente compartir esta información tan pronto como sea posible con aquellos CSIRT de referencia en el ámbito autonómico de forma que la gestión de la misma pueda realizarse de la forma óptima utilizando todas las estructuras del Estado y las Autonomías.

ENMIENDA NÚM. 33

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 20.1

De modificación.

Texto que se propone:

«Artículo 20. Protección del notificante.

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes **relativos a la seguridad de redes y sistemas de información,** no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación**, incluyendo las denuncias falsas**.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

3. En todo caso, se pondrá en conocimiento del operador de servicios esenciales o del proveedor de servicios digitales prestadores de los servicios a los que se refiere, el incidente notificado.»

Texto que se sustituye:

«Artículo 20. Protección del notificante.

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

La norma debería establecer el régimen de responsabilidad aplicable a los operadores que notifiquen obligatoriamente incidentes. La norma crea un desequilibrio legal evidente entre el régimen sancionador, previsto en su título VII de forma detallada, y la indefinición de la redacción actual del artículo 20.1.

Por otra parte, el artículo 20.2 pretende establecer un principio similar al de «whistleblowing» aplicado a posibles incidentes que se produzcan en los operadores.

— En este sentido, creemos que el objetivo del legislador es incentivar la mejora de los canales internos de denuncia, no de los externos. En este sentido, consideramos que la redacción propuesta es desafortunada, porque protege la notificación anónima de incidentes al no exigir que las denuncias se realicen ante el operador de servicios esenciales o el proveedor de servicios digitales sujeto a la norma. En consecuencia, el operador denunciado podría no conocer la existencia de una notificación en su contra y estaría indefenso ante falsas denuncias o fuentes que divulguen falsas noticias que afecten al operador, a otras empresas o al país, ya que no podría verificarlas. Consideramos fundamental que los operadores y proveedores puedan acceder al contenido de dichas notificaciones oportunamente para evitar un posible daño reputacional irreparable.

— Tampoco se establece qué tipo de incidentes estarían amparados por este artículo.

— Por último, el artículo menciona la posibilidad de que se acredite la mala fe del empleado o personal que recurra a esta posibilidad, sin establecer los criterios para poder apreciarla.

ENMIENDA NÚM. 34

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 21.1

De modificación.

Texto que se propone:

«Artículo 21. Factores para determinar la importancia de los efectos de un incidente.

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

Para los operadores de servicios esenciales:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.
c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
~~f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.~~
~~g) El daño reputacional.~~»

Texto que se sustituye:

«Artículo 21. Factores para determinar la importancia de los efectos de un incidente.

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.

cve: BOCG-12-A-28-2

c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.
g) El daño reputacional.»

JUSTIFICACIÓN

La redacción original no se ajusta a lo establecido en los artículos 14.4 y 16.4 de la Directiva, los factores y criterios para determinar la importancia de un incidente son diferentes para los proveedores que para los prestadores.

A diferencia del resto de criterios (letras a-e) que son mensurables, cuantificables y, por tanto, objetivos, los factores a los que hacen alusión las letras f) y g) son totalmente subjetivos, agregando elementos al reporte de incidentes que consideramos se exceden del campo de la directiva.

Estos criterios generarían inseguridad jurídica, muy especialmente «el daño reputacional» que es un intangible difícil de cuantificar y muy subjetivo, por lo que se sugiere su eliminación.

Por otro lado, el reporte de incidentes quedará finalmente definido en los actos de implementación.

ENMIENDA NÚM. 35

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 24

De modificación.

Texto que se propone:

«Artículo 24. Incidentes que afecten a servicios digitales.

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este Real Decreto-ley, ~~así como cualquier otra parte interesada,~~ que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que está establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.»

Texto que se sustituye:

«Artículo 24. Incidentes que afecten a servicios digitales.

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este Real Decreto-ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que está establecido el citado proveedor.

cve: BOCG-12-A-28-2

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.»

JUSTIFICACIÓN

Permitir que cualquier otra parte notifique el incidente sólo conllevaría inseguridad jurídica y el bloqueo del sistema. En primer lugar, es un abuso de un concepto jurídico indeterminado. Es difícil pensar cómo otra persona distinta del propio sujeto obligado puede disponer de la información suficiente como para poder tener certeza de que efectivamente se ha producido un incidente notificable. En segundo lugar, y como consecuencia de lo anterior, es preciso tener en cuenta que la incorporación de este cambio respecto al régimen previsto por la Directiva podría implicar un colapso significativo en la labor de las autoridades, que pasarían a recibir un número muy superior de notificaciones al que recibirán otros Estados miembros también sujetos a la Directiva y que no tengan una regulación al margen de la misma.

De otro lado, este sistema implicaría un alto riesgo de proliferación de notificaciones infundadas y que sólo tendrían como objetivo atacar a los proveedores establecidos en otros Estados miembros. Ello implicaría que las autoridades y los prestadores de servicios estén más ocupados intentando gestionar el abundante número de notificaciones recibidas e identificando aquellas que realmente son verídicas y fundadas que promoviendo la correcta aplicación del sistema y trabajando en la mejora de la seguridad.

ENMIENDA NÚM. 36

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 26.2

De modificación.

Texto que se propone:

«Artículo 26. Información al público.

[…]

2. La autoridad competente también podrá ~~decidir~~ informar de modo directo al público o a terceros sobre el incidente**, respetando en todo caso la confidencialidad que entrañe dicha información**.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.»

Texto que se sustituye:

«Artículo 26. Información al público.

[…]

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.»

JUSTIFICACIÓN

En el apartado 1 no se concreta qué se entiende por interés público y qué situaciones estarían amparadas por este apartado. Proponemos añadir el siguiente texto en el apartado 2 con el fin de

cve: BOCG-12-A-28-2

salvaguardar la confidencialidad de la información que los operadores suministran a las autoridades, que en esos casos no podría hacerse pública.

Si bien se recoge en el articulado la necesidad de consultar y coordinar de la autoridad competente antes de informar al público, vemos imprescindible matizarlo. De modo contrario, un dato descontextualizado o una mala interpretación del mercado comprometerían seriamente a la entidad.

ENMIENDA NÚM. 37

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 27 bis

De adición.

Texto que se propone:

«Artículo 27 bis. Periodo de retención de la información sobre incidentes.

Tras la publicación del informe anual, las autoridades competentes y los CSIRT eliminarán los datos facilitados por los operadores de servicios esenciales y los proveedores de servicios digitales durante el reporte de incidentes, para todos los incidentes desde cuya fecha de cierre hayan transcurrido más de treinta y seis meses, pudiendo conservar únicamente aquellos incidentes que aún no se hayan cerrado, o aquellos que se hayan cerrado en los últimos treinta y seis meses. Cada autoridad competente y cada CSIRT mantendrá un registro de los incidentes que se han eliminado en este proceso.»

JUSTIFICACIÓN

El Proyecto de Ley no contiene ninguna previsión relativa al tratamiento histórico de la información sobre incidentes comunicada a las autoridades competentes o a los CSIRT.

Una vez comunicado el incidente, resuelto el mismo, y obtenido la información y el aprendizaje posible de un incidente, la utilidad de la información del incidente se limita al análisis estadístico y de tendencias que cabe esperar del informe anual. Una vez agotada esa información, la disponibilidad de esa información en manos de la Administración supone un costo de mantenimiento en términos de recursos de almacenamiento, de medidas de protección y en el peor de los casos un riesgo de filtración con consecuencias reputacionales para las entidades que reportaron el incidente. Por eso, parece razonable limitar estos riesgos mediante la eliminación de la información no necesaria.

ENMIENDA NÚM. 38

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 30

De modificación.

Texto que se propone:

«Artículo 30. Autorización para la cesión de datos personales.

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y

cve: BOCG-12-A-28-2

limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso. Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los operadores de servicios esenciales y los proveedores de servicios digitales respecto a las incidencias detectadas en la prestación de servicios que se presten.

~~b)~~ **c)** Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

~~c)~~ **d)** Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

~~d)~~ **e)** Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

~~e)~~ **f)** Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.»

Texto que se sustituye:

«Artículo 30. Autorización para la cesión de datos personales.

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso. Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.»

JUSTIFICACIÓN

Es necesario introducir otros supuestos para el tratamiento legítimo de datos personales en materia de ciberseguridad para estar en condiciones de asegurar la prevención, protección y resiliencia de las infraestructuras.

En esta propuesta de enmienda ya se tiene en cuenta la existencia de otros CSIRT nacionales, entre los que se encuentran los CSIRT autonómicos, que pueden ser relevantes en la gestión de incidentes con datos personales.

ENMIENDA NÚM. 39

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 32

De modificación.

Texto que se propone:

«Artículo 32. Supervisión de los operadores de servicios esenciales.

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar **el cumplimiento de los requisitos necesarios para garantizar** la seguridad de las redes y sistemas de información, ~~incluida la~~

cve: BOCG-12-A-28-2

~~documentación sobre políticas de seguridad~~ **junto con la garantía y el secreto de las comunicaciones. Las autoridades competentes podrán inspeccionar los operadores sujetos a esta Ley para garantizar su cumplimiento.**

Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. El operador de servicios esenciales podrá sustituir la realización de auditorías por la aportación de la información recopilada en los últimos doce meses mediante su programa de auditoría ejecutado de acuerdo con el artículo 16.6.d, siempre que dicha información cubra los requerimientos de la auditoría solicitada.

3. A la vista de la información recabada, la autoridad competente podrá ordenar al operador que subsane los incumplimientos detectados e indicarle cómo debe hacerlo.»

Texto que se sustituye:

«Artículo 32. Supervisión de los operadores de servicios esenciales.

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá ordenar al operador que subsane los incumplimientos detectados e indicarle cómo debe hacerlo.»

JUSTIFICACIÓN

Se considera que la información requerida por las autoridades se debe referir al ámbito de este Proyecto de Ley, no a la política general de la empresa, que pertenece al ámbito de la libertad de empresa.

Por ello, se propone ajustar el artículo 32.1.

El regulador no contempla el reúso de la información derivada del programa de auditorías que el operador o prestador ya estarán ejecutando en cumplimiento de 16.6.d.

La habilitación del ejercicio del derecho de auditoría por parte de las autoridades competentes es necesario para el buen desempeño de sus funciones. No obstante, el ejercicio de este derecho supone un sobrecoste para los operadores, por lo que la limitación de los derechos de auditoría por el regulador aporta seguridad a los operadores y prestadores de servicio. Por esta razón, se propone modificar el epígrafe 32.2, sobre reúso de información de auditoría.

ENMIENDA NÚM. 40

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 33, puntos 1, 2 y 3 (nuevo)

De modificación.

Texto que se propone:

«Artículo 33. Supervisión de los operadores de servicios esenciales.

[…]

1. La autoridad competente para la supervisión de los servicios digitales ~~sólo~~ inspeccionará el cumplimiento de las obligaciones derivadas de este Real Decreto-ley cuando tenga noticia de algún

cve: BOCG-12-A-28-2

incumplimiento, incluyendo por petición razonada de otros órganos o denuncia**, o por procedimiento rutinario de inspección**.

En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

2. **El proveedor de servicios digitales podrá sustituir la realización de auditorías por la aportación de la información recopilada en los últimos doce meses durante su programa de auditoría ejecutado de acuerdo con el artículo 16.6.d, siempre que dicha información cubra los requerimientos de la auditoría solicitada.**

Cuando la autoridad competente tenga noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medias de supervisión pertinentes.

A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

3. Las autoridades competentes ejercitarán este derecho de inspección y supervisión sobre operadores de servicios esencial como máximo con frecuencia anual, salvo que exista motivo fundado o alerta conocida que motive la realización de una inspección extraordinaria.»

Texto que se sustituye:

«Artículo 33. Supervisión de los operadores de servicios esenciales.

[…]

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de este Real Decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia.

En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

2. Cuando la autoridad competente tenga noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medias de supervisión pertinentes.

A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.»

JUSTIFICACIÓN

El regulador se atribuye un derecho ilimitado de auditoría sobre operadores, tanto en número de auditorías exigibles como en profundidad de las mismas. Sobre los prestadores de servicios digitales, el derecho es ilimitado en profundidad, dado que debe ser iniciado por denuncia. Consideramos que también para los proveedores de servicios digitales, debe ser posible la inspección rutinaria.

Por otra parte, el regulador no contempla el reúso de la información derivada del programa de auditorías que operador o prestador ya estarán ejecutando en cumplimiento de 16.6.d.

La habilitación del ejercicio del derecho de auditoría por parte de las autoridades competentes es necesario para el buen desempeño de sus funciones. No obstante, el ejercicio de este derecho supone un sobrecoste para los operadores, por lo que la limitación de los derechos de auditoría por el regulador aporta seguridad a los operadores y prestadores de servicio. Por ello se propone agregar el epígrafe 33.3, para dar una consistencia.

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 41

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 38

De modificación.

Texto que se propone:

«Artículo 38. Graduación de la cuantía de las sanciones.

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora.
c) La naturaleza y cuantía de los perjuicios causados.
d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.
e) El número de usuarios afectados.
f) El volumen de facturación del responsable.
g) La utilización por el responsable de programas **de gestión de vulnerabilidades técnicas o** de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.
i) La disponibilidad de información previa sobre las causas que han provocado el incidente y la imposibilidad de haber tomado 'medidas preventivas por desconocimiento de las mismas.»

Texto que se sustituye:

«Artículo 38. Graduación de la cuantía de las sanciones.

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora.
c) La naturaleza y cuantía de los perjuicios causados.
d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.
e) El número de usuarios afectados.
f) El volumen de facturación del responsable.
g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.»

JUSTIFICACIÓN

Se cita como atenuante el establecimiento de programas de recompensa por el descubrimiento de vulnerabilidades, pero no valora como tal el establecimiento de un proceso de gestión de vulnerabilidades, mucho más extendido en la actualidad y de mucha mayor eficiencia.

Tampoco se hacen mención de otras medidas preventivas, tales como la concienciación de personal, o la imprevisibilidad del incidente, si responde a un incidente de seguridad conocido o un Zero-day.

Ninguna organización puede asegurar que sus sistemas son 100 % seguros, pero si debe exigirse haber tomado las medidas preventivas adecuadas (formación u otras). Asimismo, tampoco puede culpabilizarse a una organización de haber sido escogida como primer target por atacantes que dispongan

cve: BOCG-12-A-28-2

de vulnerabilidades Zero-day. Si no se declara este eximente, la organización podría tener una triple penalización: sufrir una incidencia, dedicación de recursos a su rápida resolución y, adicionalmente, una cuantiosa sanción ante la que no ha podido tomar ninguna acción que la evitase.

ENMIENDA NÚM. 42

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 39.4 (nuevo)

De adición.

Texto que se propone:

«Artículo 39. Proporcionalidad de sanciones.

[…]

4. El órgano sancionador podrá sustituir la imposición de la sanción económica al infractor, por la exigencia de dedicación en un plazo inferior a tres meses de presupuesto adicional igual al volumen de la sanción propuesta, destinado a la mejora de la seguridad de la organización.»

JUSTIFICACIÓN

El régimen sancionador establecido se centra en sanciones meramente económicas, de efecto disuasorio en el mejor de los casos. El montante de las sanciones económicas establecidas puede inducir a que se perciban con un fin recaudatorio, más que disuasorio. En particular, cuando las Administraciones Públicas no tienen establecida sanción económica alguna.

Asegurar que las sanciones económicas se destinan a la mejora de la seguridad del afectado por el incidente resultará en una mayor efectividad en la aplicación de la regulación y en un mejor servicio al ciudadano.

Se propone añadir un nuevo epígrafe 39.4.

ENMIENDA NÚM. 43

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al artículo 41.4 (nuevo)

De adición.

Texto que se propone:

«Artículo 41. Competencia sancionadora.

[…]

4. Todas las sanciones muy graves y graves deberán ser aprobadas por el punto único de contacto designado por el artículo 13 o por el organismo sobre el que este delegue. El punto único de contacto tendrá potestad de variar la sanción impuesta para homogeneizarla con otras sanciones similares que hubiesen sido impuestas anteriormente.»

cve: BOCG-12-A-28-2

JUSTIFICACIÓN

Existen varios órganos sancionadores, de acuerdo con las distintas autoridades competentes descritas en el artículo 9.

Añadir un mecanismo de supervisión y consistencia en las sanciones impuestas, haciendo que deban ser validadas por el punto único de contacto del artículo 13, dará consistencia al régimen sancionador.

ENMIENDA NÚM. 44

FIRMANTE:

Grupo Parlamentario Ciudadanos

A la disposición final cuarta, punto 2 (nuevo)

De modificación.

Texto que se propone:

«Disposición final cuarta. Entrada en vigor.

1. ~~El presente Real Decreto-ley~~ **La presente Ley** entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

2. No obstante lo dispuesto en el párrafo anterior, cuando el cumplimiento de una obligación recogida en la presente ley dependa de desarrollos reglamentarios posteriores, serán de aplicación desde la fecha de entrada en vigor de los mismos.»

Texto que se sustituye:

«Disposición final cuarta. Entrada en vigor.

El presente Real Decreto-ley entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".»

JUSTIFICACIÓN

El Proyecto de Ley remite a desarrollo reglamentario posterior muchos aspectos fundamentales necesarios, lo que genera incertidumbre e inseguridad jurídica sobre su aplicación. Por ello consideramos necesario que se recoja en el Proyecto de Ley que aquellas obligaciones cuya ejecución y cumplimiento esté supeditado a cualquier desarrollo reglamentario posterior, su aplicación estará condicionada a la entrada en vigor de dichos desarrollos. De lo contrario se desconocería las medidas a llevar a cabo para su cumplimiento. Consideramos fundamental que la norma contemple un régimen transitorio que permita continuar aplicando los criterios actualmente existentes ¡mientras no se aprueben las normas de desarrollo de esta ley.

Por tanto, se precisaría acompasar la normativa, así como se contemplen plazos suficientes para llevar a cabo las adaptaciones tecnológicas necesarias.

ENMIENDA NÚM. 45

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al anexo I (nuevo)

De adición.

cve: BOCG-12-A-28-2

Texto que se propone:

Se añade un anexo al Proyecto de Ley, con la siguiente redacción:

«ANEXO I

Tipos de entidades a efectos del artículo 2

Sector	Subsector	Tipo de entidad
1. Energía.	a) Electricidad.	— Empresas eléctricas.
		— Gestores de la red de distribución.
		— Gestores de la red de transporte.
	b) Crudo.	— Operadores de oleoductos de transporte de crudo.
		— Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte.
	c) Gas.	— Empresas suministradoras.
		— Gestores de la red de distribución.
		— Gestores de la red de transporte.
		— Gestores de almacenamiento.
		— Gestores de la red de GNL.
		— Compañías de gas natural.
		— Gestores de las instalaciones de refinado y tratamiento de gas natural.
2. Transporte.	a) Transporte aéreo.	— Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.° 300/2008 del Parlamento Europeo y del Consejo.
		— Entidades gestoras de los aeropuertos.
		— Operadores de control de la gestión del tráfico que prestan el servicio de control del tránsito aéreo, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.° 549/2004 del Parlamento Europeo y del Consejo.
	b) Transporte por ferrocarril.	— Administradores de infraestructuras.
		— Empresas ferroviarias.
	c) Transporte marítimo y fluvial.	— Empresas de transporte marítimo.
		— Organismos gestores de los puertos.
		— Operadores de servicios de tráfico de buques.
	d) Transporte por carretera.	— Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión, responsables del control de la gestión del tráfico.
		— Operadores de los sistemas de transporte inteligentes.
3. Banca.		Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.° 575/2013 del Parlamento Europeo y del Consejo.

cve: BOCG-12-A-28-2

Sector	Subsector	Tipo de entidad
4. Infraestructuras de los mercados financieros.		**— Gestores de centros de negociación.**
		— Entidades de contrapartida central (CCP), tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.° 648/2012 del Parlamento Europeo y del Consejo.
5. Sector sanitario.	**Entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas).**	**Prestadores de asistencia sanitaria.**
6. Suministro y distribución de agua potable.		**Suministradores y distribuidores de aguas destinadas al consumo humano.**
7. Infraestructura digital.		**— IXP.**
		— Proveedores de servicios del DNS.
		— Registros de nombres de dominio de primer nivel.»

ENMIENDA NÚM. 46

FIRMANTE:

Grupo Parlamentario Ciudadanos

Al anexo II (nuevo)

De adición.

Texto que se propone:

Se añade un anexo al proyecto de ley, con la siguiente redacción:

«ANEXO II

Tipos de servicios digitales a efectos del artículo 3

1. **Mercado en línea.**
2. **Motor de búsqueda en línea.**
3. **Servicios de computación en nube.»**

A la Mesa de la Comisión de Economía y Empresa

Al amparo de lo establecido en el Reglamento de la Cámara, el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea presenta las siguientes enmiendas parciales al Proyecto de Ley de seguridad de las redes y sistemas de información (procedente del Real Decreto-ley 12/2018, de 7 de septiembre).

Palacio del Congreso de los Diputados, 26 de febrero de 2019.—**Eva García Sempere,** Diputada.—**Alberto Garzón Espinosa,** Portavoz del Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea.

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 47

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al conjunto del articulado

De modificación.

Se modificarán todas las referencias que en el articulado se realiza al concepto de «Real Decreto-ley» que deben ser modificadas por la palabra «Ley».

MOTIVACIÓN

Mejora técnica.

ENMIENDA NÚM. 48

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 9

De supresión.

Se suprime el apartado 2.º de la letra a) del apartado primero del artículo 9, quedando el texto del artículo de la siguiente manera:

«Artículo 9. Autoridades competentes.

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).»

MOTIVACIÓN

El artículo 2.3, letra a), establece que no se aplicará la presente ley a los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos. No parece congruente por tanto que el apartado segundo del artículo 9.1.a) señale una autoridad competente en materia de seguridad de las redes para operadores no críticos cuando se supone que los mismos están excluidos de la aplicación de la presente ley.

---

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 49

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 17

De modificación.

Se modifica el artículo 17, quedando el texto del artículo de la siguiente forma:

«Artículo 17. Normas técnicas.

Las autoridades competentes promoverán, **sin imponer ni favorecer el uso de un tipo específico de tecnología,** la utilización de regulaciones, normas o especificaciones técnicas en materia de seguridad de las redes y sistemas de información elaboradas en el marco del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea. En ausencia de dichas normas o especificaciones, promoverán la aplicación de las normas o recomendaciones internacionales aprobadas por los organismos internacionales de normalización, y, en su caso, de las normas y especificaciones técnicas aceptadas a nivel europeo o internacional que sean pertinentes en esta materia.»

MOTIVACIÓN

La presente enmienda tiene como finalidad asegurar la no imposición por parte de las autoridades españolas de ningún tipo de obligación de uso de un sistema específico de tecnología, todo ello acorde con lo ya indicado en el artículo 19 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, Directiva que es objeto de transposición mediante el presente Proyecto de Ley.

ENMIENDA NÚM. 50

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 20

De modificación y adición.

Se modifica el apartado 2 adicionando un concepto y se adiciona un nuevo apartado 3 al artículo 20, quedando el texto del artículo de la siguiente forma:

«Artículo 20. Protección del notificante.

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que Informen sobre incidentes no podrán sufrir consecuencias adversas o **represalias** de ningún tipo en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

cve: BOCG-12-A-28-2

3. Las empresas de servicios digitales o cualquier otra entidad, no podrán emprender, ni directa ni indirectamente, ningún tipo de acción que pueda provocar consecuencias adversas o represalias a usuarios de los servicios esenciales o digitales que informen sobre incidentes, salvo en los supuestos en que se acredite mala fe en su actuación.»

MOTIVACIÓN

La presente enmienda viene a ampliar el marco de protección también a los usuarios esenciales o digitales que informen sobre incidentes. No parece lógico que solo se establezca normativamente la protección de aquellos que trabajen o presten servicios para una empresa o entidad mientras los ciudadanos que por cualquier circunstancia, y actuando de buena fe, notificasen incidencias en los servicios digitales no cuenten con la adecuada protección por parte de los poderes públicos frente a actuaciones de hostigamiento o represalia por parte de empresas o entidades responsables de los fallos o incidencias, por lo que quedarán prohibidas cualquier tipo de acción contra los usuarios, salvo mala fe.

Igualmente, en el apartado 2 se adiciona el concepto de «represalia» al de «consecuencias adversas», como también se hace en el apartado 3, por ser más garantista y comprensivo.

ENMIENDA NÚM. 51

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 21.1

De supresión.

Se modifica el artículo 21.1, suprimiéndose la letra g), quedando el texto del artículo de la siguiente forma:

«Artículo 21. Factores para determinar la importancia de los efectos de un incidente.

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.
c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.»

MOTIVACIÓN

Se considera inadecuado la inclusión entre el elenco de incidencias a las que refiere el artículo 19.1, primer párrafo, la conducta supuestamente atinente al «daño reputacional», toda vez que su carácter evidentemente subjetivo puede llevar a que se generen notificaciones con un evidente ánimo censor o con

---

cve: BOCG-12-A-28-2

ENMIENDA NÚM. 52

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 26

De modificación y adición.

Se modifica el artículo 26, quedando el texto del artículo de la siguiente forma:

«Artículo 26. Información al público.

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente**, respetando en todo caso la confidencialidad de los datos que pudieran afectar a terceros de buena fe**.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.»

MOTIVACIÓN

Proponemos añadir el siguiente texto en el apartado 2 con el fin de salvaguardar la confidencialidad de los datos que pudieran afectar a terceros de buena fe.

ENMIENDA NÚM. 53

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 30

De modificación y adición.

Se modifica el artículo, quedando el texto del artículo de la siguiente forma:

«Artículo 30. Autorización para la cesión de datos personales.

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso**, debiendo en todo caso contar con las garantías suficientes para su correcto tratamiento en conformidad con la legislación de protección de datos**.

Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

cve: BOCG-12-A-28-2

e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.»

MOTIVACIÓN

Se propone mejorar el texto original para dotar al artículo de una cláusula que prescriba la obligación de contar con las debidas garantías para el tratamiento de datos a los que se refiere el artículo enmendado.

ENMIENDA NÚM. 54

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

Al artículo 37.1

De modificación.

Se modifica el apartado 1 del artículo 37, quedando el texto del artículo de la siguiente forma:

«Artículo 37. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.
b) Por la comisión de infracciones graves, multa **de 50.001 hasta** 500.000 euros.
c) Por la comisión de infracciones leves, amonestación o multa hasta **50.000 euros.»**

MOTIVACIÓN

La presente enmienda viene a modificar la cuantía máxima se la sanción leve, así como la mínima de la sanción grave, toda vez que este Grupo entiende que las cuantías propuestas en el texto original resultan desproporcionadas, estableciéndose un marco sancionador excesivamente amplio que iba desde la mera amonestación sin repercusión económica hasta los cien mil euros, estimando este Grupo más acorde establecer un marco más comprensible y proporcionado que vaya desde la mera amonestación a una sanción económica con la regia mínima de la amonestación, toda vez que dota de mayor seguridad jurídica I sistema de sanciones.

ENMIENDA NÚM. 55

FIRMANTE:

Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea

De adición.

Se añade una nueva disposición adicional quinta con la siguiente redacción:

«Disposición adicional quinta. **Se modifica el artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General,** que queda redactado como sigue:

"Artículo 58 bis. Utilización de medios tecnológicos y datos personales en los actividades electorales.

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará

cve: BOCG-12-A-28-2

amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas y exclusivamente bajo el consentimiento de las personas afectadas, prestado de manera separada, específica e inequívoca para este fin, de conformidad con el artículo 6.1 de la Ley Orgánica de Protección de Datos.

Asimismo, en la recopilación de datos personales se respetará el cumplimiento del deber de información básica, que especificará en todo caso la posibilidad de retirar el consentimiento a través del ejercicio del derecho de supresión.

2. Los partidos políticos, coaliciones y agrupaciones electorales solo podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el período electoral previo el consentimiento de la persona afectada en concordancia con lo previsto en el apartado anterior.

Las plataformas digitales no podrán condicionar el acceso a los contenidos web a la prestación del consentimiento por la persona afectada. En la realización de actividades políticas, se informará a la persona usuaria de los medios para el ejercicio de sus derechos, destacando en cada comunicación la posibilidad de retirar el consentimiento a través del ejercicio del derecho de supresión.

3. Queda prohibida la compraventa de datos de naturaleza política o ideológica para cualquier tipo de finalidad, incluidos aquellas actuaciones de índole electoral.

Igualmente queda prohibida la creación de perfiles ideológicos o políticos, así como la personalización de envíos de propaganda electoral derivados del tratamiento de datos o de los datos personales obtenidos en páginas web y otras fuentes de acceso público.

4. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

El envío de propaganda electoral por medios electrónicos o sistemas de mensajería estará en todo caso sometido a las condiciones de los envíos postales recogidas en el artículo 59 de la presente ley, estableciéndose un máximo de un envío por elector en cada convocatoria electoral.

Quedarán excluidos de cualquier tipo de envío de propaganda electoral por medios electrónicos o sistemas de mensajería aquellos electores que hayan manifestado su oposición al traslado de copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral.

5. Las actividades electorales anteriormente referidas identificarán de modo destacado su naturaleza electoral así como la posibilidad de realizar de forma sencilla y gratuita el ejercicio del derecho de acceso, rectificación, cancelación y oposición.”»

MOTIVACIÓN

La nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos, introdujo un nuevo artículo 58 bis en la legislación electoral, LOREG, lo que ha generado una manifiesta inseguridad jurídica sobre el uso que los partidos políticos pueden hacer de los datos de los usuarios que en Internet, y especialmente en las redes sociales, se encuentran alojados. Al objeto de garantizar la seguridad de estos datos y de asegurar un proceso electoral limpio y democrático, en el que queden proscritas las prácticas de compraventa de datos ideológicos o políticos o la elaboración de perfiles de carácter ideológico, se presenta esta enmienda de modificación.

cve: BOCG-12-A-28-2

ÍNDICE DE ENMIENDAS AL ARTICULADO

cve: BOCG-12-A-28-2

Artículo 10

— Enmienda núm. 9, del G.P. Vasco (EAJ-PNV), letra g).

Artículo 11

— Enmienda núm. 10, del G.P. Vasco (EAJ-PNV), apartado 2.

Artículo 12

— Sin enmiendas.

Artículo 13

— Sin enmiendas.

Artículo 14

— Enmienda núm. 12, del G.P. Vasco (EAJ-PNV), apartados 1, 2, 3 y apartado nuevo.

Artículo 15

— Sin enmiendas.

Artículos nuevos

— Enmienda núm. 8, del G.P. Vasco (EAJ-PNV).
— Enmienda núm. 11, del G.P. Vasco (EAJ-PNV).

Título IV

Artículo 16

— Enmienda núm. 13, del G.P. Vasco (EAJ-PNV), apartados 2, 4 y 5.
— Enmienda núm. 30, del G.P. Ciudadanos, apartados 2 y 4.
— Enmienda núm. 31, del G.P. Ciudadanos, apartado 5.

Artículo 17

— Enmienda núm. 49, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea.

Artículo 18

— Sin enmiendas.

Título V

Artículo 19

— Enmienda núm. 32, del G.P. Ciudadanos, apartado 1.

Artículo 20

— Enmienda núm. 33, del G.P. Ciudadanos, apartado 2 y nuevo.
— Enmienda núm. 50, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea, apartado 2 y nuevo.

Artículo 21

— Enmienda núm. 51, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea, apartado 1, letra g).
— Enmienda núm. 34, del G.P. Ciudadanos, apartado 1, letras f) y g).

cve: BOCG-12-A-28-2

Artículo 22

— Enmienda núm. 14, del G.P. Vasco (EAJ-PNV), apartado 1.

Artículo 23

— Sin enmiendas.

Artículo 24

— Enmienda núm. 15, del G.P. Vasco (EAJ-PNV).
— Enmienda núm. 35, del G.P. Ciudadanos.

Artículo 25

— Sin enmiendas.

Artículo 26

— Enmienda núm. 36, del G.P. Ciudadanos, apartado 2.
— Enmienda núm. 52, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea, apartado 2.

Artículo 27

— Enmienda núm. 16, del G.P. Vasco (EAJ-PNV), apartado nuevo.

Artículo 28

— Sin enmiendas.

Artículo 29

— Enmienda núm. 17, del G.P. Vasco (EAJ-PNV).

Artículo 30

— Enmienda núm. 38, del G.P. Ciudadanos, letra b).
— Enmienda núm. 53, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea.

Artículo 31

— Sin enmiendas.

Artículos nuevos

— Enmienda núm. 37, del G.P. Ciudadanos.

Título VI

Artículo 32

— Enmienda núm. 39, del G.P. Ciudadanos, apartado 1 y nuevo.

Artículo 33

— Enmienda núm. 40, del G.P. Ciudadanos, apartados 1, 2 y nuevo

Artículo 34

— Sin enmiendas.

cve: BOCG-12-A-28-2

Título VII

Artículo 35

— Sin enmiendas.

Artículo 36

— Sin enmiendas.

Artículo 37

— Enmienda núm. 54, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea, apartado 1, letras b) y c).

— Enmienda núm. 18, del G.P. Vasco (EAJ-PNV), apartado nuevo.

Artículo 38

— Enmienda núm. 19, del G.P. Vasco (EAJ-PNV), letras d) y g) y nueva.
— Enmienda núm. 41, del G.P. Ciudadanos, letra g) y nueva.

Artículo 39

— Enmienda núm. 42, del G.P. Ciudadanos, apartado nuevo.

Artículo 40

— Enmienda núm. 20, del G.P. Vasco (EAJ-PNV).

Artículo 41

— Enmienda núm. 21, del G.P. Vasco (EAJ-PNV), apartado nuevo.
— Enmienda núm. 43, del G.P. Ciudadanos, apartado nuevo.

Artículo 42

— Sin enmiendas.

Disposición adicional primera

— Sin enmiendas.

Disposición adicional segunda

— Sin enmiendas.

Disposición adicional tercera

— Enmienda núm. 22, del G.P. Vasco (EAJ-PNV).

Disposición adicional cuarta

— Sin enmiendas.

Disposiciones adicionales nuevas

— Enmienda núm. 55, del G.P. Confederal de Unidos Podemos-En Comú Podem-En Marea.

Disposición final primera

— Sin enmiendas.

cve: BOCG-12-A-28-2

Disposición final segunda

— Sin enmiendas.

Disposición final tercera

— Sin enmiendas.

Disposición final cuarta

— Enmienda núm. 44, del G.P. Ciudadanos, apartado nuevo.

Anexos nuevos

— Enmienda núm. 45, del G.P. Ciudadanos.
— Enmienda núm. 46, del G.P. Ciudadanos.

cve: BOCG-12-A-28-2