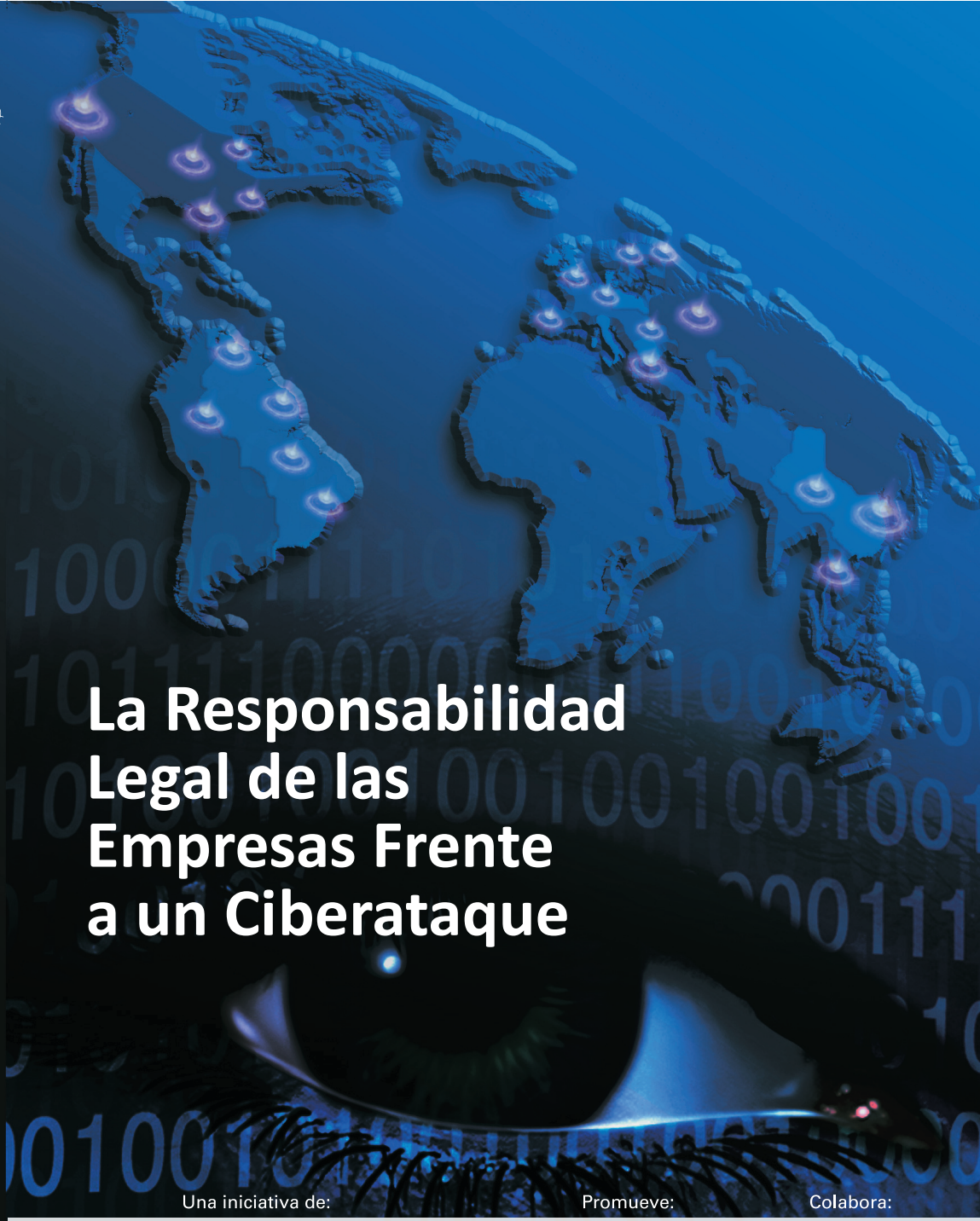


La Responsabilidad Legal de las Empresas Frente a un Ciberataque

Una iniciativa de:

enaTIC ABOGACIA DIGITAL

ISMS Forum Spain

Promueve:

Abogacía Española CONSEJO GENERAL

Colabora:

INTECO Instituto Nacional de Tecnologías de la Comunicación

ÍNDICE

En este Estudio han colaborado:

Adolfo Hernández

Andreu Van Den Eynde

Ángel Díez Bajo

Blanca Escribano

Cristina Sirera

David Echarri

Fernando Benítez

Ignacio San Macario

Javier Carbayo

Javier González

Ofelia Tejerina

Marcos García-Gasco

María José Santos

Noemí Brito

Sofía Fontanals

Víctor Salgado

Revisores

Eloy Velasco

Lucas Blanque

Tomás González

Coordinadores

Carlos Alberto Saiz

Francisco Pérez Bes

Prólogo del Consejo General de la Abogacía Española

El Informe de ISMS-Forum y ENATIC, al que estas breves palabras sirven de prólogo, es una muestra de cómo la evolución de las tecnologías de la información suponen al tiempo un horizonte, cuando no una realidad tangible, de oportunidades, retos y riesgos.

El avance de Internet ha generado un aumento históricamente incuestionable de la rapidez de las comunicaciones, de la amplitud de la información disponible y de las posibilidades de acceder a ella. Y ha supuesto también una mayor exposición de las instituciones públicas y de las entidades privadas, y aún de los propios ciudadanos, al ojo público, con las consiguientes demandas de transparencia y de rendición de cuentas, siempre deseables, pero también a las amenazas derivadas del empleo y, en su caso, del abuso de las tecnologías de la información y de la comunicación para la consecución de fines ilícitos.

Es sabido que hace tiempo que la ley llega tarde, que el legislador trata de resolver con largas e intrincadas normas los retos que plantean las mencionadas tecnologías, lo que demuestra que, en ocasiones, parece olvidar que las exigencias que plantean para el Derecho dichas tecnologías son, en muchos casos, atendibles con las clásicas categorías jurídicas. Tal podría ser el caso del instituto de la responsabilidad. Pero no es menos cierto, en cualquier caso,

que determinadas cuestiones sí merecen un nuevo enfoque que revista de caracteres específicos aquellos aspectos que merecen un tratamiento particularizado por razones derivadas de su especial significación para la comunidad, para el Estado en su conjunto.

Buen ejemplo de este segundo enfoque lo representa el régimen de las infraestructuras críticas. Si bien su arranque puede situarse en el año 2004, el hito relevante lo constituyen la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección, y la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. En esta segunda puede observarse cómo las denominadas infraestructuras críticas no son sólo las integradas en la esfera pública, sino también las de titularidad privada, en cuanto reúnan los requisitos fijados en la norma, que pivotan sobre la protección de los sectores estratégicos y los servicios esenciales.

De este modo, los Estados miembros, y en España en particular, se han dotado de un régimen jurídico que comprende disposiciones organizativas y operativas encaminadas a lograr la correcta planificación de los eventuales ataques y, en su caso, a articular la reacción del Sistema de Protección de Infraestructuras Críticas para garantizar el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.

La Ley 8/2011 es clara cuando determina que su objeto es el establecimiento de las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello, precisa la Ley, se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

Entre esas amenazas, como ilustra el informe que el Consejo General de la Abogacía Española ha tenido el honor de patrocinar, se encuentran los denominados ciberataques, que plantean retos de calado por sus especiales características. Entre esos retos se encuentra el de la adecuada y proporcionada respuesta en Derecho.

Por ello es de justicia terminar estas líneas felicitando a los autores del informe por el acierto de este excelente trabajo y porque va a ser una utilísima herramienta para las empresas en un mundo tan complejo como es el de los ciberataques.

Carlos Carnicer
Presidente del Consejo General de la Abogacía Española

Prólogo del Instituto Nacional de Tecnologías de la Comunicación

Desde entidades como INTECO y el Ministerio de Industria del que depende, como también desde la abogacía digital, se es consciente del reto que supone, en cuanto a necesidades legislativas y regulatorias, esta nueva sociedad conectada en la que vivimos, que demanda un marco jurídico sólido y coherente que ofrezca seguridad jurídica a los ciudadanos y a los operadores de la economía digital, pero que a su vez permita luchar de manera eficaz contra las amenazas que suponen, para el bienestar económico y social, los ciberataques y la industria del cibercrimen.

En este sentido, debe destacarse la iniciativa conjunta de ENATIC e ISMS Forum a la hora de abordar, en el informe que ahora nos ocupa, un aspecto tan importante como es el del impacto jurídico en un caso de ciberataque dirigido a una empresa situada en España. Conviene señalar que se trata de un estudio que, además de la novedad doctrinal que supone un trabajo de estas características, los autores apuestan por realizar un análisis global de una situación (imaginaria pero posible) identificando y analizando aquellas obligaciones, tanto legales como regulatorias, de las que se pueden desprender eventuales responsabilidades civiles, penales o administrativas para la empresa atacada.

Lo acertado de esta publicación es, también, el momento histórico en el que se produce. En efecto, sólo en el plano empresarial venimos siendo testigos de unas -cada vez más habituales y graves- situaciones de ciberataques y fugas de información, que no sólo causan grandes daños económicos y de reputación a las entidades que los sufren, sino también de confianza en los ciudadanos, hecho éste que pone en serio peligro los usos innovadores de nuevas tecnologías y el normal desarrollo de la economía digital.

Además, este informe ve la luz en un momento de gran actividad legislativa en lo que a la ciberseguridad concierne. Así, por ejemplo, hemos sido testigos de la aprobación, en el mes de febrero de 2014, del Plan de Confianza en el ámbito Digital para los años 2013-2015, que hace suyos los compromisos de la Agenda Digital para España; de la Estrategia Europea de Ciberseguridad y de la Estrategia de Ciberseguridad Nacional en los ámbitos de la confianza digital y el mercado digital interior (ciudadanía, empresas, industria y profesionales), proponiendo un conjunto de medidas que contribuyan a darles cumplimiento y alcanzar los objetivos conjuntos en colaboración con todos los agentes implicados.

En este momento, en el que la ciberseguridad es ya un elemento esencial en nuestra vida diaria, no queda más que desear que la información y conclusiones recogidas en este trabajo sirvan de concienciación para cualquier organización. Y que, dentro de esta importante labor de difusión que supone esta iniciativa, esta

publicación sea la primera de muchas otras en las que se sigan analizando los aspectos legales derivados de ciberataques, con las particularidades que tienen las distintas legislaciones y normativas sectoriales que podemos encontrar en el escenario jurídico español.

Francisco Pérez Bes
Secretario General del Instituto Nacional de Tecnologías de la Comunicación

Supuesto de hecho

El estudio realizado en el presente documento parte de un supuesto de hecho ficticio, pero representativo, de escenario de infraestructura empresarial que puede verse afectado en caso de un ciberataque. En particular, la naturaleza de los servicios esenciales que podrían verse afectados, las organizaciones encargadas de su prestación, la tecnología empleada hoy día, así como de la actuación de un ciberatacante sobre una infraestructura crítica.

Se describe a continuación este supuesto de hecho:

1) Energías Estatales de España (EEES) es una sociedad anónima cuya actividad se enmarca en la prestación de servicios de suministros energéticos y distribución a empresas y consumidor final a nivel nacional e internacional, con presencia en diferentes países de Europa y América del Sur. Esta organización está establecida en España.

2) En la prestación de tales servicios, EEES está sujeta al cumplimiento de todas las obligaciones que exige la legislación vigente española.

3) No obstante, en el caso particular de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de

las infraestructuras críticas, manifiesta no haber recibido instrucción alguna del CNPIC ni de otros organismos de las AA.PP. españolas, sobre la necesidad de cumplimiento o controles a cumplir.

4) Para la prestación de sus servicios, EEES cuenta con diversas centrales repartidas por el territorio nacional. Dichas centrales llevan años en funcionamiento, contando con el equipamiento y tecnología propios del sector.

5) La prestación de servicios que ofrece EEES sigue distintos procesos, algunos de los cuales están externalizados a otras empresas.

6) Los procesos de marketing, atención al cliente, contratación, cancelación de servicios, y facturación, son realizados para EEES por GESCLIENTE S.A., según se recoge en su correspondiente contrato. GESCLIENTE S.A., a su vez, utiliza los servicios SaaS (Software as a Service) que provee Cloud ACME, empresa internacional con sede en Bélgica que ofrece herramientas CRM (Customer Relationship Management) y otros servicios a sus clientes mediante el uso del denominado cloud computing, así como garantías de su seguridad mediante diversas certificaciones profesionales como ISO 27001, a cuyo mantenimiento se compromete por contrato.

7) La gestión operativa de los sistemas esenciales para la operación de las centrales, o sistemas SCADA (Supervisory Control And Data Acquisition) está externalizada en ICS Exemplary S.L., empresa de ingeniería especializada en sistemas de control industrial, mediante un contrato entre ambas partes. El personal de las centrales está contratado por ICS Exemplary, y la gestión de las mismas se realiza mediante las normas y procedimientos propios de esta empresa, de acuerdo a las condiciones establecidas en dicho contrato.

8) ICS Exemplary, además, dispone de un departamento informático propio y se ocupa de la gestión de los sistemas informáticos de la planta y de EEES, entre los que se encuentran los PCs de usuarios, servidores, infraestructura de red, e incluso el sitio web de EEES en Internet. Esto es debido a que parte del personal de EEES trabaja en las propias centrales, de manera que tiene contacto estrecho con la gestión de las mismas, donde recibe incluso visitas de otros proveedores como puede ser GESCLIENTE.

9) EEES dispone, además de otros servicios, de un seguro contratado con una importante aseguradora española para cubrir posibles pérdidas derivadas de incidentes en la prestación de sus servicios.

10) El 13 de Septiembre de 2013 (Viernes), a las 09:00 horas, el personal encargado de la central energética que presta servicios a la Comunidad de Madrid, percibió un comportamiento anómalo en los sistemas de la planta, que recibían la orden de apagarse desde el centro de control. Alertado dicho centro de la situación, se verificó que esta no era debida a un error humano, y se inició el protocolo de reencendido de los sistemas de generación de energía eléctrica, si bien este no pudo ser ejecutado correctamente por anomalías en los sistemas del centro de control, que continuaban emitiendo dicha orden de apagado.

11) El servicio no pudo ser restablecido hasta varias horas después, dejando sin suministro a buena parte de la capital en el intervalo de tiempo transcurrido. Como consecuencia, numerosos servicios esenciales para la economía y la salud ciudadana se vieron perjudicados, tales como hospitales, gestión del tráfico, comunicaciones telemáticas, etc.

12) Los medios de comunicación se hicieron eco no solo de la caída de servicio de la central, sino de la modificación no autorizada del portal web de EEES, gestionado por ICS Exemplary, y que mostró en su portada un mensaje de un grupo reclamando la autoría del ataque, en el que se indicaba además el robo de información (datos personales,

consumos, datos bancarios, etc.) de un número importante de los clientes de EEES.

13) ICS Exemplary, alarmado ante la gravedad de la situación y de acuerdo con EEES, decide en primer lugar buscar por sí mismo las causas del problema y atajarlo. La revisión de los logs del servidor web que aloja al portal de EEES revela que la modificación de la web procede de uno de los PCs de usuario ubicados en la planta energética atacada, responsabilidad de un técnico de la planta reconocido en las redes sociales, y cuyo puesto de trabajo puede ser conocido a través de Internet. La revisión de este PC, realizada por el personal técnico informático de la central, no da indicios de haber sido utilizado de manera no autorizada o infectado con malware conocido, sin embargo, los registros del proxy de salida a Internet indican que este PC estaba realizando conexiones hacia diversas direcciones IP de origen ruso.

14) Este técnico tenía además acceso a los sistemas del centro de control, a los que en ocasiones accedía de manera remota desde su PC ubicado en el área de oficinas, por pura cuestión práctica, ya que eso evita desplazamientos para tareas puntuales. Los registros del sistema SCADA no revelan haber recibido órdenes legítimas procedentes del PC del técnico en el momento del ataque, ni de otros PCs de usuarios

similares. El equipo técnico de la central, buscando posibles explicaciones, encuentra en un conocido sitio de Internet (scadahacker.com) vulnerabilidades publicadas con exploits conocidos que podrían afectar a sus sistemas, de acuerdo a las versiones del software instaladas en la central, por lo que creen que su sistema pudo haber sido atacado y que ello motivaría el comportamiento anómalo mostrado.

15) EEES, sabiendo que esta información es la gestionada por GESCLIENTE S.A., se pone en contacto con esta empresa. El personal de GESCLIENTE S.A. accede al sistema CRM con su usuario y contraseña habitual, el cual presenta al entrar un registro de los últimos accesos realizados. Este registro confirma un acceso reciente desde una dirección IP de origen ruso, utilizando el mismo usuario y contraseña.

16) En este punto, EEES decide contactar con las fuerzas de seguridad del Estado.

Estudio legal de responsabilidades

I. Análisis de la responsabilidad del atacante:

A. Tipo de responsabilidad legal

Los hechos descritos parecen encajar en una pluralidad de acciones típicas: desde la incardinación del resultado final en el tipo de desórdenes públicos del art. 560.3 del Código Penal (o incluso en el delito de estragos del art. 346 si entendemos el medio empleado como de gran potencia, en un sentido amplio en la interpretación del tipo), o los diversos delitos cometidos como medio para conseguir el resultado final, delitos estos dentro del ámbito de la ciberdelincuencia, como el acceso no consentido a equipos informáticos y el descubrimiento de datos reservados de los artículos 197.2 y 3 de nuestro Código Penal; o los daños en sistemas informáticos de los tipos del artículo 264.1,2 y 3.

Una vez determinada la responsabilidad penal del atacante, nace, necesariamente, en virtud del artículo 109 y los que le siguen en el Código Penal, la responsabilidad civil derivada del delito, si bien ésta tiene una consideración autónoma, pudiéndose exigir ante la jurisdicción civil en cualquier momento posterior a la producción del

daño o la causa de los perjuicios, o bien conjuntamente con la acción penal.

La responsabilidad civil surge de la obligación legal de reparar el daño y los perjuicios causados, por tanto abarcaría tanto los sufridos por la empresa atacada, las empresas con las que se han subcontratado determinados servicios y productos, pero también los daños sufridos y los perjuicios causados a los usuarios finales del servicio de la empresa EEES.

Cuestión diferente es la posibilidad real de persecución efectiva dentro del ámbito penal de los responsables del delito; y, dentro del ámbito civil, la casi total imposibilidad de que a los atacantes, en el difícil caso de que pudieran ser atraídos a la jurisdicción española, pudieran responder por la responsabilidad civil.

Desde el punto de vista estrictamente penal, la posibilidad de perseguir delitos cometidos en el Estado español fuera de sus límites territoriales y jurisdiccionales pasa necesariamente por la suscripción de instrumentos internacionales, tales como convenios de colaboración judicial y policial que, si bien, dentro de la Unión Europea están muy avanzados, con países fuera de nuestro ámbito político resulta prácticamente imposible ante la falta de herramientas de colaboración judicial y policial que, suponiendo una merma de la soberanía, faciliten la "entrega del nacional".

B. Ley aplicable

A los efectos que ahora interesan, las conductas con relevancia jurídico-penal son diversas:

- La intromisión no autorizada en el sistema informático de EEES.
- La modificación o alteración de datos que causa un mal funcionamiento de la infraestructura, dando lugar a la imposibilidad de suministrar energía a los clientes.
- La sustracción de datos almacenados en el sistema informático de EEES.
- La modificación (por desfiguración) de la página de inicio de la web corporativa de EEES.

Debe reseñarse que la mera intrusión no autorizada a través del aprovechamiento de vulnerabilidades del sistema informático de un tercero, constituye una infracción penal desde la incriminación, en el año 2010, del delito de intromisión ilegítima en equipos o sistemas informáticos (conductas que podríamos denominar de *hacking*) del artículo 197.3 del Código Penal (en adelante CP).

> *[…] 3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas*

informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33[1]*.*

Sin embargo, dicha infracción (como sucede en la mayoría de casos reales) no será sancionada de forma independiente al tratarse de la primera fase de la comisión de delitos posteriores que, en definitiva, son la culminación del propósito criminal de los autores. Por lo tanto, la intrusión, aun siendo ilegal, es sólo el primer eslabón de un plan criminal más ambicioso y por tanto no será sancionada aparte, sino como integrante del delito finalmente cometido, en ocasiones agravando la pena de dicho delito final del que la intromisión es sólo un medio.

El ataque supone la comisión de dos delitos independientes, todos ellos sancionables conforme al CP actual con penas de prisión: un

[1] Número 3 del artículo 197 introducido en su actual redacción por el apartado quincuagésimo tercero del artículo único de la L.O. 5/2010, de 22 de junio, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 23 junio)

delito continuado de daños informáticos agravado, y un delito de descubrimiento y revelación de secretos.

Sea cual fuese la técnica utilizada por los atacantes, se produce una intrusión para obstaculizar o interrumpir el funcionamiento del sistema informático que controla los procesos industriales de la infraestructura. Dicha modalidad de sabotaje está expresamente prevista en el artículo 264.2 CP como modalidad de daños informáticos por interrupción de sistemas.

> *[…] 2**.** El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años*[2]*.*

Existe actualmente cierta problemática para calificar de daños informáticos algunos "ciberataques" pues el CP exige demostrar que las conductas de sabotaje han sido graves, siendo la "gravedad" un término de evidente vaguedad y de difícil concreción a los efectos de garantizar la seguridad jurídica. No obstante, no parece el supuesto

[2] *Artículo 264 redactado por el apartado sexagésimo séptimo del artículo único de la L.O. 5/2010, de 22 de junio, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 23 junio)*

de hecho analizado un caso de difícil encaje penal debido a la específica naturaleza de la industria afectada. Así, al tratarse EEES de una empresa que gestiona una infraestructura crítica, el ataque supone una afectación a los intereses generales de notoria gravedad. Es de aplicación incluso la modalidad agravada del delito de daños informáticos del artículo 264.3 CP por ese especial resultado dañoso producido.

> *[…] 3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:*
>
> *1º Se hubiese cometido en el marco de una organización criminal.*
>
> *2º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.*

Sería posible incluso vincular el ataque con la intención de poner en peligro la integridad o vida de personas (puesto que la dependencia de servicios básicos de salud, por ejemplo, del suministro eléctrico boicoteado es conocida por los atacantes) dándose un supuesto de daños específicos agravados por el peligro creado a la salud o vida, del artículo 266.2 CP.

> *[…] 2. Será castigado con la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses el que cometiere los daños previstos en el artículo 264, en cualquiera de las circunstancias mencionadas en el apartado anterior.*

Concurre otro supuesto de daño o sabotaje informático, en este caso en su modalidad simple del artículo 264.1 CP (es decir, no agravado), por la alteración intencional de la página web corporativa a través de la publicación de un mensaje reivindicativo de los autores, conducta técnicamente llamada de desfiguración o *defacement*.

> *[…] 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.*

Al existir dos conductas de daño, ello daría lugar a la aplicación de un único delito continuado de daños informáticos (74.2 CP).

> *[…] 2. Si se tratare de infracciones contra el patrimonio, se impondrá la pena teniendo en cuenta el perjuicio total causado. En estas infracciones el Juez o Tribunal impondrá, motivadamente, la pena superior en uno o dos grados, en la extensión que estime conveniente, si el hecho revistiere*

notoria gravedad y hubiere perjudicado a una generalidad de personas.

Finalmente los atacantes habrían –presuntamente- accedido a bases de datos (datos personales, consumos, datos bancarios) alojadas en el sistema informático, haciéndose con dichos datos –evidentemente- sin autorización de sus titulares y en perjuicio tanto de éstos como de la propia empresa EEES. Tal conducta integraría un delito de descubrimiento y revelación de secretos del artículo 197.2 CP que protege la integridad de los datos informáticos y castiga modalidades de espionaje.

[…] 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

En los delitos de descubrimiento y revelación de secretos habitualmente el perjudicado puede disponer del proceso penal, decidiendo si quiere incoarlo mediante denuncia o incluso si quiere desistir de él una vez iniciado, pero dicha regla general no sería de aplicación al supuesto analizado al tratarse de una conducta

delictiva que afecta a los intereses generales y que, por tanto, trasciende del ámbito de la propio empresa atacada.

C. Jurisdicción competente

Al efectuarse el ataque cibernético desde fuera de España acudimos a lo previsto en la Ley Orgánica del Poder Judicial (LOPJ) y la Ley de Enjuiciamiento Criminal (LECr), donde el artículo 14 de la LECr señala: "*Será competente para la instrucción de las causas, el Juez de Instrucción del partido en que el delito se hubiere cometido (forum delicti comissi)*". Cuando estamos hablando de accesos remotos a través de Internet la Sala Segunda del Tribunal Supremo, a partir del 3 de febrero de 2005 acordó aplicar el principio de ubicuidad basado en el siguiente pronunciamiento: "*El delito se comete en todas las jurisdicciones en que se haya realizado algún elemento del tipo. En consecuencia el Juez de cualquiera de ellas que primero haya realizado las actuaciones procesales, será en principio competente para la instrucción de la causa*". Por tanto entendemos que la jurisdicción española resulta competente para conocer de un supuesto como el descrito.

Por otro lado, como en este supuesto el delito afecte a una pluralidad de personas situadas en lugares diferentes, es decir en el territorio de más de una Audiencia Provincial, la LOPJ establece que será competente para su instrucción y juicio la Audiencia Nacional

(sus Juzgados Centrales de Instrucción, y luego, para la vista oral los Centrales de lo Penal).

Habida cuenta que estos delitos tienen un alcance que va más allá de nuestras fronteras, para ayudar a los Estados miembros de la UE a cooperar en la lucha contra la delincuencia internacional organizada se han creado 2 agencias que serían necesarias para combatir este ataque: Eurojust y la Oficina Europea de Policía (Europol). La Comisión Europea decidió crear un Centro Europeo Ciberdelincuencia (EC3) en Europol, que será el punto central de la lucha de la UE contra la delincuencia informática. EC3 inició oficialmente sus actividades el 1 de enero de 2013, con el objetivo de abordar las siguientes áreas de la delincuencia informática:

a. Delitos como el fraude "online" a través de Internet cometido por grupos organizados para conseguir grandes ganancias ilegales.

b. Delitos que causen daños graves a las víctimas como la explotación sexual infantil a través de Internet.

c. Delitos que afecten a los sistemas de infraestructuras críticas en la Unión Europea.

Eurojust es una agencia de la Unión Europea (UE) con sede en La Haya. Fue creada en 2002. La función de este órgano europeo es facilitar la cooperación judicial penal entre las autoridades de los Estados miembros. Prioritariamente va dirigido a luchar contra el

crimen organizado en sus distintas vertientes: narcotráfico, fraude, trata de seres humanos, terrorismo, corrupción, delito informático, blanqueo de capitales y otras actividades ilegales relacionadas con la presencia de grupos delictivos organizados en la actividad económica.

II. Identificación y análisis de la responsabilidad de la empresa atacada:

A. Responsabilidad civil frente a los clientes y usuarios.

Responsabilidad Contractual

Se plantea si la interrupción del suministro de electricidad, provocado por un ataque de terceros a los sistemas informáticos de una empresa, cuya actividad se desenvuelve en el marco de las obligaciones de prestación de un servicio de suministro que debe ser entendido como un "producto" (art. 136 TRLGDCYU), y que debe ser entregado con la debida calidad y sin interrupciones (art. 48 de la Ley 54/1997)[3], generaría para sus clientes consumidores finales[4] del

[3] SAP de Granada, de 22 de septiembre de 2006: "el citado Real Decreto regulador del Suministro de Energía eléctrica, al regular las consecuencias del incumplimiento de la calidad de servicio individual en su art. 105 y los descuentos que ello supone para los consumidores", dejan establecido en su apartado 7 que "sin perjuicio de las consecuencias definidas en los párrafos anteriores, el consumidor afectado por el incumplimiento de la calidad de servicio individual, podrá reclamar, en vía civil, la indemnización de daños y perjuicios que dicho incumplimiento le haya causado", con lo que se evidencia que dicha normativa no altera los principios generales de la responsabilidad contractual o

sector privado, el derecho a obtener una indemnización por daños y perjuicios, bajo la premisa de un incumplimiento contractual, y bajo qué condiciones.

En este contexto va a ser determinante analizar los elementos de la carga de la prueba sobre dos aspectos esenciales. Por una parte debe tenerse en cuenta que, para poder reclamar responsabilidades indemnizatorias, los clientes afectados deben acreditar que el fallo del suministro de la energía contratada es lo que ha provocado los daños que se reclama sean resarcidos (relación de causalidad)[5]. Por otra parte, y para evitar hacerse cargo de dichos costes, la empresa suministradora del servicio debe poder demostrar que se encuentra bajo alguno de los supuestos de exoneración de responsabilidad (art. 1105 C.C.)[6], y acreditar incuestionablemente que actuó con la

extracontractual del código civil, que pueden exigirse a dichas entidades en cualquiera de dichas vías, dado el concepto unitario de la culpa civil (sentencia del Tribunal Supremo de 6 de abril de 1998) con la posibilidad de aplicar las normas de concurso de ambas responsabilidades que más se acomoden al caso, siempre en favor de la víctima, y para el logro de su resarcimiento del daño lo más completo posible (Sentencia del Tribunal Supremo de 15 de febrero de 1993)".

[4] SAP de León, de 11 de marzo de 2010: "La demandante no tiene la condición de consumidora por su condición de empresaria: persona física o jurídica que actúe en el marco de su actividad empresarial o profesional (art. 4 del Real Decreto Legislativo 1/2007, de 16 de noviembre (LA LEY 11922/2007), por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias). Y como dispone el art. 3 del citado Real Decreto Legislativo, sólo son consumidores o usuarios las personas físicas o jurídicas que actúan en un ámbito ajeno a una actividad empresarial o profesional. Estos preceptos se citan para descartar las normas de protección de consumidores y usuarios y la doctrina de los Tribunales que las aplican, y alguna de las cuales son citadas en el recurso interpuesto."

[5] Art. 129.1 TRLGDCYU. "El régimen de responsabilidad previsto en este libro comprende los daños personales, incluida la muerte, y los daños materiales, siempre que éstos afecten a bienes o servicios objetivamente destinados al uso o consumo privados y en tal concepto hayan sido utilizados principalmente por el perjudicado".

[6] Además, el art. 105 del RD 1955/2000, por el que se aprueba el Reglamento de Transporte, Distribución, Comercialización, Suministro y Procedimientos de Autorización de Instalaciones de Energía Eléctrica; y en el art. 8 de la Orden del Ministerio de Economía 797/2002, de 22 de marzo, por la que se aprueba el procedimiento de medida y control de la continuidad del suministro eléctrico.

debida diligencia en el mantenimiento de las medidas de seguridad de sus sistemas técnicos[7] (arts. 1.101 C.C y 147 TRLGDCYU). Si EEES lograse probar ambas circunstancias, podría acogerse a lo dispuesto por el art. 14.3 del RD 223/2008, de 15 de febrero[8], y verse libre de cualquier tipo de responsabilidad civil[9], pero en no pocas ocasiones se ha considerado que la suya es "una actividad de riesgo, de ahí que se le pueda exigir una responsabilidad cuasi objetiva, pues su deber era poner todos los medios para detectar cualquier irregularidad, por difícil que fuese, y estaba obligada a ello

[7] SAP de Madrid, de 24 de marzo de 2010, tras estudiar los tres regímenes de responsabilidad antes mencionados, afirma: "el debate se ha de centrar en acreditar la existencia de la alteración en el suministro que se alega en la demanda, y acreditado tal extremo, así como el nexo de causalidad entre el mismo y el daño, procederá declarar la responsabilidad de la entidad demandada y su obligación de reparar el daño causado, sin necesidad de indagar acerca de las causas que hubieran determinado la indicada alteración porque no afectarían a la referida responsabilidad". En similar sentido, la SAP de Las Islas Baleares, de 15 de abril de 2010: "... la conclusión lógica y coherente con los hechos probados es que la causa de los daños fueron las alteraciones habidas en el suministro eléctrico, no habiéndose acreditado por la entidad suministradora, como le incumbía, que o bien esas alteraciones no existieron o que, resultando existentes, se debieron a una causa ajena a su ámbito de responsabilidad o que, en su caso, adoptó todas las medidas a su alcance para evitar este tipo de incidencias a sus clientes, pues no debe olvidarse que la demandada como garante legal del suministro constante de energía eléctrica y con determinada calidad, que debe asegurar, le corresponde demostrar el cumplimiento correcto de tal obligación cuando un usuario acredita haber sufrido perjuicios derivados de la interrupción del suministro o su deficiente aporte".

[8] RD 223/2008, de 15 de febrero, por el que se aprueban el Reglamento sobre condiciones técnicas y garantías de seguridad en líneas eléctricas de alta tensión y sus instrucciones técnicas complementarias ITC-LAT 01 a 09.

[9] SAP de León, de marzo de 2010: "solo un hecho externo y violento puede justificar la rotura, tal y como se explica en la sentencia recurrida, y de hechos ajenos a la propia suministradora no puede responder ésta, como ya hemos expuesto. El sistema de conducción de energía eléctrica debe de estar dotado de elementos y materiales resistentes, pero la resistencia de los elementos y materiales tiene límites que, cuando se sobrepasan, dan lugar a la rotura. En este caso, como se ha indicado, el número de elementos dañados y su simultánea interacción revela la intervención de un agente externo lo suficientemente intensa como para provocar la rotura de materiales cuya idoneidad no ha sido cuestionada ni puesta en duda por el único perito que ha emitido informe".

por imperativo legal (art. 41.1 y 99 y ss. Decreto 1955/2000)"[10]. Por tanto, en el caso de que EEES no pudiera acreditar debidamente que cumplió con las garantías necesarias para proteger la prestación del servicio con calidad y sin interrupciones, entrarían en juego todas las normas de defensa de los consumidores y podría exigirse responsabilidades económicas al prestador del servicio, como si de un "producto defectuoso" se tratase.

Responsabilidad Extracontractual

En caso de existir afectados por el corte de suministro que no fuesen parte contratante directa del servicio (art. 1902 C.C.), podrían éstos exigir la imputación de responsabilidad objetiva a EEES, por la simple obligación genérica que tiene "de no causar daño a otro" y, como se ha dicho, por suponer por si misma esta concreta actividad una situación de peligro o riesgo.

Por esta posibilidad de responsabilidad extracontractual añadida a la anterior, por las responsabilidades en cascada que pueden derivarse de un supuesto de hecho como el que nos ocupa, y por las dificultades de acreditar la debida diligencia en el cuidado de las instalaciones o la intervención directa de un tercero en los fallos del suministro, es habitual que las empresas de servicios energéticos cuenten con la cobertura de un seguro de responsabilidad civil (art. 43 de la Ley 50/1980 de C.S.). En todo caso, el juego de la carga de

[10] P.ej. las SAP de Castellón, de 4 de febrero de 2010 y de Málaga, de 11 de marzo de 2010, sobre la necesidad de una suficiente acreditación de que los daños provienen de la intervención de tercero.

la prueba es igualmente esencial en estos casos, y será lo que defina la imposición a EEES de responsabilidades de carácter civil.

En cuanto a las vías de actuación, según el 1.089 del C.C. "*las obligaciones nacen de la ley, de los contratos y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia*", y como se ha expuesto, parece que la empresa EEES podría estar exenta de responsabilidad civil por tratarse de un ataque ejecutado por terceros a sus sistemas informáticos (siendo éstos los verdaderos responsables).

Sin embargo, si suponemos que no se pudiera acreditar que dicho ataque se produce por terceros ajenos a la empresa, EEES tendría que asumir las indemnizaciones por daños y perjuicios causados a los consumidores finales según lo dispuesto por la legislación relativa a la defensa de los consumidores y usuarios, tanto a nivel estatal (*RD Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias)*, como a nivel autonómico (*Ley 11/1998, de 9 de julio, de Protección de los Consumidores de la Comunidad de Madrid*. Por otra parte, y respecto a normativa específica del sector eléctrico, se tendrán en cuenta la *Ley 54/1997, de 27 de noviembre, del Sector Eléctrico*; el *Decreto 19/2008, de 13 de marzo, del Consejo de Gobierno, por el que se desarrolla la Ley 2/2007, de 27 de marzo, por la que se regula la garantía del suministro eléctrico de la Comunidad de*

Madrid; y la *Ley 2/2007, de 27 de marzo, por la que se regula la garantía del suministro eléctrico en la Comunidad de Madrid* (modificada por la Ley 4/2007, de 13 de diciembre, por la que se regula la garantía del suministro eléctrico en la Comunidad de Madrid, adaptándola a la Ley 17/2007, de 4 de julio).

Por último, y en caso de que nos encontrásemos ante afectados personas jurídicas, que actúan en el tráfico mercantil como intermediarios (mediando actividad comercial), señalar que entrarían en juego las reglas del Código de Comercio sobre responsabilidades en caso de incumplimientos contractuales, y la posibilidad de repercutir las eventuales reclamaciones de los clientes finales de dichas personas jurídicas.

B. Responsabilidad administrativa frente a los reguladores.

1. Desde el punto de vista de la normativa española relativa al sector eléctrico español.

1.1) Garantía de suministro y medidas asociadas: La reciente Ley 24/2013, de 26 de diciembre, del Sector Eléctrico (en lo que sigue, Ley 24/2013), regula en los arts.6 y siguientes, la denominada garantía de suministro de forma que el Gobierno podría adoptar, para un plazo determinado, las medidas necesarias para garantizar el suministro de energía eléctrica cuando concurran ciertos supuestos, por ejemplo, situaciones de desabastecimiento energético, o de las que se pueda derivar amenaza grave para la

integridad física o la seguridad de las personas, de aparatos o instalaciones o para la integridad de la red de transporte o distribución de energía eléctrica. Entre otras medidas, se encuentran, incluso, las de operación directa de las instalaciones de generación, transporte y distribución. Cuando las medidas adoptadas afecten únicamente a una comunidad autónoma, como podría ocurrir en el supuesto de hecho de referencia, la decisión se adoptará en colaboración con ésta[11].

1.2) Otras obligaciones relacionadas con las empresas comercializadoras de energía eléctrica y las consecuencias jurídico-administrativas derivadas de su incumplimiento:

Entre otras obligaciones destacan las de:

a) Garantizar las condiciones técnicas y de seguridad de las instalaciones y del equipo asociado a las que se sujeta la propia autorización de las actividades de distribución de energía eléctrica (art.53.4 a) de la Ley 24/2013). De forma

[11] Sin perjuicio de lo anterior, en el caso de que en los territorios no peninsulares, se produjeran situaciones de riesgo cierto para la prestación del suministro de energía eléctrica o situaciones de las que se pueda derivar amenaza para la integridad física o la seguridad de las personas, de aparatos o instalaciones o para la integridad de la red de transporte o distribución de energía eléctrica, las medidas allí previstas podrán ser también adoptadas por las comunidades o ciudades autónomas afectadas, siempre que se restrinjan a su respectivo ámbito territorial. En dicho supuesto, tales medidas no tendrán repercusiones económicas en el sistema eléctrico, salvo que existiera acuerdo previo del Ministerio de Industria, Energía y Turismo que así lo autorice (art.7.5 de la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico).

que, el incumplimiento de estas condiciones y requisitos pueden dar lugar a la revocación de la autorización correspondiente (art.53.10 de la Ley 24/2013). Esto se entiende sin perjuicio de la aplicación del específico régimen sancionador dispuesto en el título X de esta Ley.

b) Preservar el carácter confidencial de la información de la que tenga conocimiento en el desempeño de su actividad, sin perjuicio de la obligación de información a las Administraciones Públicas (art.47. 1 K) de la Ley 24/2013), pudiendo ser la empresa comercializadora requerida por la Administración Pública competente, así como la Comisión Nacional de los Mercados y la Competencia, para acreditar el cumplimiento de estas obligaciones. En caso de incumplimiento por un comercializador de cualquiera de las obligaciones que le son exigibles en el ejercicio de su actividad, incluyendo la señalada, el mismo será sancionado de acuerdo con lo establecido en los arts. 61 y siguientes de la Ley 24/2013. La comisión de una infracción muy grave podrá llevar aparejada la extinción de la habilitación para actuar como comercializador.

c) Obligaciones relativas a la calidad del servicio (continuidad, número y duración de las interrupciones, así como a la calidad del producto): que se determinen reglamentariamente por la Administración competente. De esta forma, si como consecuencia de ataques o incidentes

similares a los que alude el supuesto por ejemplo, bajara la calidad de la distribución de una zona de forma continua, o pudieran producirse consecuencias graves para los usuarios, o concurrieran circunstancias especiales que pudieran poner en peligro la seguridad en el servicio eléctrico, por un lado, la Administración competente podría requerir a la empresa que, a través de los planes de inversiones correspondientes, promoviera nuevas actuaciones de impulso de la calidad de servicio en dichas zonas. Por otro lado, también podrían aplicarse reducciones en la facturación a abonar por los usuarios. Luego, el ataque a las instalaciones que implique una disminución en la calidad del servicio puede implicar, además de una merma reputacional a la empresa, consecuencias económicas indirectas relacionadas con las nuevas inversiones a acometer y la reducción de los ingresos derivados de la facturación a los usuarios. En todo caso, lo anterior se entiende sin perjuicio de la aplicación del específico régimen sancionador dispuesto en el título X de esta Ley.

1.3) Régimen jurídico sancionador en este ámbito: Según la gravedad del caso, la situación a la que alude el supuesto de hecho de base de este Informe podría acarrear la existencia de una infracción muy grave por posible aplicación del art.64 apartados 13, 16,17, 30 ó 31, lo que podría conllevar multa por importe no inferior

a 6.000.001 euros ni superior a 60.000.000 de euros[12]. También aquélla podría resultar sancionada como grave por aplicación de lo previsto en el art.65 apartados 8, 9 y 17, lo que supondría una posible multa importe no inferior a 600.001 euros ni superior a 6.000.000 euros. Asimismo, en ambos casos, podrían aplicarse sanciones accesorias como la suspensión, revocación o no renovación de las autorizaciones durante un período no superior a tres años en su caso (art.68 de la Ley 24/2013), y aplicarse otras medidas complementarias como la restitución de las cosas o su reposición al estado natural anterior al inicio de la actuación infractora, y si concurrieran daños, y dicha reposición no fuera posible, se exigiría una indemnización por daños y perjuicios irrogados (art.69 de la Ley 24/2013).

1.4) Consideraciones de interés derivadas de la legislación territorial aplicable al caso (Ley 2/2007, de 27 de marzo, por la que se regula la garantía del suministro eléctrico en la Comunidad de Madrid): Con pleno respeto a lo indicado con anterioridad respecto a la legislación estatal, es importante destacar la siguiente obligación adicional de interés, a saber:

[12] En cualquier caso la cuantía de la sanción no podrá superar el 10 por ciento del importe neto anual de la cifra de negocios del sujeto infractor, o el 10 por ciento del importe neto anual de la cifra de negocios consolidada de la sociedad matriz del grupo al que pertenezca dicha empresa, según los casos (art.67.2 de la Ley 24/2013).

Comunicación de incidencias en el suministro (art.15): Las empresas distribuidoras tendrán que comunicar, a la mayor brevedad posible y, en todo caso, en plazo no superior a seis horas desde que tengan lugar, al órgano competente en materia de energía de la Comunidad de Madrid, las incidencias que reglamentariamente se determinen en función del número de suministros afectados y de los tiempos de interrupción. No se determina en el caso si dicha comunicación se ha producido o no en dicho tiempo, pero su incumplimiento puede calificarse como grave lo que supone una multa de 600.000,01 hasta 6.000.000 de euros (art.21.2.2 b) por relación con el art.22 de esta Ley autonómica).

Con carácter adicional, -lo que es relevante respecto a este caso-, debe considerarse que si la empresa distribuidora y transportista acredita que la incidencia en la continuidad del suministro se debe a actuaciones de terceros, podrá procederse a la incoación del procedimiento sancionador contra el tercero causante del incidente (art.16).

2. Desde la perspectiva de la normativa española relativa a la protección de las infraestructuras críticas.

En base al indicado principio de responsabilidad compartida, y considerando que: a) EEES ha sido designado como operador crítico (lo que no se deduce de forma expresa en el supuesto de hecho base de este Informe); b) No se han dirigido de instrucciones específicas por parte del CNPIC o de otros organismos vinculados a

AA.PP. españolas competentes en este ámbito, respecto a la necesidad de cumplimiento de la LPIC y su normativa de desarrollo, se destaca que:

*EEES en tanto operador crítico debía contar, como mínimo, con los oportunos Planes de Seguridad y los Planes de Protección Específicos, los que parecen inexistentes, y actuar conforme a los mismos en este tipo de incidentes, así como colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas que gestiona.

*Las autoridades y organismos de carácter administrativo competentes que formen parte del Sistema, deberán ejercitar las funciones y facultades que a nivel normativo se determinen respecto a la protección de las infraestructuras críticas existentes en su demarcación territorial, para la protección de personas y bienes y para el mantenimiento del orden público, sin perjuicio de los mecanismos de coordinación que se establezcan. A estos efectos, se destaca la importancia del desarrollo e implementación de los citados Planes de Apoyo Operativo, sobre todo, en lo relativo a la relación con las Fuerzas y Cuerpos de Seguridad con competencia en la demarcación territorial de que se trate, así como su posible actuación en relación a la protección de tales infraestructuras.

Si no se ha actuado, adoptando las oportunas obligaciones y medidas de seguridad y protección indicadas en la LPIC y su Reglamento de desarrollo, se incumplen estas normas, aumentando

el grado de inseguridad y desprotección de las instalaciones y equipos vinculados a la prestación de un servicio esencial, incrementando la vulnerabilidad de aquellos. Esto puede, además, implicar, en paralelo, el incumplimiento de otras tantas leyes, como así ocurre: legislación protectora de los datos personales o, en el caso concreto, la propia normativa del sector eléctrico, como se comprueba.

Por otra parte, si en el caso objeto de estudio, EEES no hubiera, ni tan siquiera, sido designado como operador crítico en coherencia con los procedimientos dispuestos al efecto (art.13 LPIC y art.14 de su Reglamento de desarrollo, aprobado por el Real Decreto 704/2011, de 20 de mayo), también deberían adoptarse las oportunas medidas correctoras en este ámbito por la Administración Pública competente que, en caso contrario, se sujetaría a la responsabilidad derivada de la falta de actuación debida, incluyendo, la de tipo patrimonial, si así se apreciara.

3. Frente al Ministerio de Industria (competente en el sector eléctrico), de conformidad con la Ley de Infraestructuras Críticas.

Teniendo en cuenta que el sector de la energía forma parte de un sector estratégico, será de aplicación a este supuesto práctico la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas[13] ("Ley PIC"). Esta norma incorpora al Derecho español la Directiva 2008/114/CE, de 8 de

[13] http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

diciembre, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección[14], y se desarrolla reglamentariamente por el Real Decreto 704/2011, de 20 de mayo[15] (el "Reglamento").

No obstante, la estructura final del marco normativo para la protección de las infraestructuras críticas no ha llegado a completarse. En la actualidad el Ministerio del Interior está trabajando en el desarrollo de los planes estratégicos concretos para los diferentes sectores definidos por la Ley PIC[16]. En el caso del sector de la energía, en junio de 2013 comenzaron los trabajos para identificar las infraestructuras críticas en todo el territorio español. La duración de estos trabajos será de aproximadamente seis meses, por lo que se espera que en breve se empiecen a designar oficialmente los operadores críticos de acuerdo con el procedimiento establecido en la Ley PIC. Este hecho justifica que, en nuestro supuesto de hecho, la empresa atacada no haya recibido instrucción alguna del Centro Nacional para la Protección de las Infraestructuras Críticas ("CNPIC"), órgano que, de acuerdo con la Ley PIC, se encarga del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF
[15] http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf
[16] La Ley PIC define los **sectores estratégicos** como cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de la Ley PIC y abarca los siguientes sectores: administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua**, energía**, salud, tecnologías de la información y las comunicaciones (TIC), transporte, alimentación y sistema tributario y financiero.

Seguridad del Ministerio del Interior en relación con la protección de infraestructuras críticas en el territorio nacional.

Sin perjuicio de la mencionada instrucción y tras un acuerdo con el Ministerio de Industria, el Instituto Nacional de Tecnologías de la Comunicación ("INTECO") se ha convertido en un instrumento de apoyo para el CNPIC en la gestión de incidentes de ciberseguridad. Los operadores responsables de una infraestructura crítica pueden acudir a un CERT (*Computer Emergency Response Team*) que, como equipo de respuesta ante emergencias informáticas, se encarga de gestionar incidentes relacionados con la seguridad tecnológica de las infraestructuras críticas nacionales. El sitio oficial del CNPIC[17] recoge una pequeña guía para dar respuesta a incidentes en infraestructuras críticas.

Desde el punto de vista de la responsabilidad, habría que analizar cómo fue la actuación de EEES con anterioridad al ataque. Siguiendo el tenor literal de la Ley PIC, los operadores considerados críticos (tanto públicos como privados) deben colaborar con las autoridades competentes con el fin de optimizar la protección de las infraestructuras críticas. De acuerdo con este principio, el Reglamento despliega varias obligaciones para aquellos operadores que, como bien pudiera ocurrir en el caso que ahora nos ocupa, fueran considerados por el Ministerio del Interior como operadores críticos. En particular deberán (i) prestar colaboración técnica a la

[17] www.cnpic-es.es/

Secretaría de Estado de Seguridad, a través del CNPIC; (ii) colaborar en la elaboración de los Planes Estratégicos Sectoriales; (iii) elaborar el Plan de Seguridad del Operador, así como el Plan de Protección Específico para cada una de las infraestructuras críticas; (iv) designar a un Responsable de Seguridad y Enlace; (v) designar un Delegado de Seguridad por cada infraestructura crítica; y (vi) facilitar las inspecciones que las autoridades competentes lleven a cabo.

En caso de incumplimiento de las obligaciones mencionadas, ni la Ley PIC ni el Reglamento prevén un régimen sancionador específico de cara a eventuales incumplimientos ante la administración competente; en este sentido, será necesario atender a la legislación sectorial en materia energética[18]. Cabe destacar que el propio CNPIC ha acuñado un concepto de responsabilidad compartida, entendiendo este principio como "*una asociación público-privada, sustentada sobre la base de la cooperación y el entendimiento mutuos*, donde todas las partes implicadas (públicas y privadas) deben aceptar su parte de responsabilidad bajo los principios de colaboración, confianza mutua e intercambio de información". En este sentido, resulta necesario esperar a la aprobación de los distintos planes estratégicos sectoriales para completar el esquema

[18] Sin perjuicio de este marco legislativo principal, no debemos olvidar la aplicación de multitud de normativa conexa a las ya citadas anteriormente, tanto desde la perspectiva de su aplicación general a todos los sectores estratégicos (v.gr.: legislación relativa a protección civil, intervención militar de emergencia, etc.), como en el caso particular del sector energético (normativa aplicable a los subsectores de la electrificad, el gas o los hidrocarburos).

de responsabilidad respecto de las medidas para la protección de las infraestructuras críticas.

4. Frente a los órganos administrativos competentes en virtud de la normativa de telecomunicaciones y sociedad de la información.

En nuestro supuesto de hecho, la empresa atacada tiene externalizada la gestión de determinados servicios como la gestión de su web y el suministro de conectividad Internet y demás servicios de telecomunicaciones. Así, la gestión de los sistemas IT y de telecomunicaciones se realiza por dos empresas: Cloud ACME, que provee servicios de cloud computing o *SaaS (subcontratada a su vez por GESCLIENTE S.A.)* e ICS Exemplary, que a su vez actúa como cliente o intermediario con los proveedores de sistemas informáticos, de telecomunicaciones e incluso el sitio web de EEES en Internet.

Los hechos han de ser analizados a la luz de la Directiva 2002/21/CE (implementada en España por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones), que establece que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público deberán adoptar las medidas adecuadas para salvaguardar su integridad y seguridad e introduce requisitos de notificación de las violaciones de la seguridad y las pérdidas de integridad[19]. Por su

[19] Artículo 13bis de la Directiva, implementado en derecho español por el artículo 36 bis de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones: Artículo 36 bis. Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.

parte, la Directiva 2002/58/CE (Directiva de Privacidad y comunicaciones electrónicas) exige que los proveedores de servicios de comunicaciones electrónicas accesibles para el público tomen las medias técnicas y de organización necesarias para velar por la seguridad de sus servicios.

Con el fin de facilitar la implementación a nivel de los distintos estados miembros de la Unión, se promulgó el Reglamento (UE) nº 611/2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas. Este Reglamento, que tiene efecto directo inmediato desde su entrada en vigor el 25 de agosto de 2013, armoniza la operativa práctica en la notificación de la violación de datos personales, clarificando la obligación contenida en la Directiva de Privacidad desde su reforma en 2009[20].

La Directiva de Privacidad (implementada en España de la Ley 32/2003 y normativa de desarrollo) impone la obligación de notificar violaciones de datos únicamente a los proveedores de servicios de comunicaciones electrónicas (operadores de telecomunicaciones y proveedores de servicios de Internet). Como resumen de su impacto, puede decirse que los operadores destinatarios de esta norma han de implantar internamente las medidas protección necesarias para que, en casos de violaciones de datos, la

[20] Directiva 2002/58/CE modificada por la Directiva 2009/136/CE.

información sea canalizada en la empresa de la manera más rápida posible para notificarlo en veinticuatro horas.

La notificación ha de dirigirse a tres tipos de destinatarios (i) la autoridad nacional competente (normalmente de protección de datos o el regulador sectorial de telecomunicaciones, en materia de seguridad, el Ministerio de Industria), (ii) el usuario o titular de los datos - salvo que los datos se hayan encriptado y sean ininteligibles para cualquiera que haya accedido de forma no autorizada (la Comisión va a publicar una lista de las medidas de encriptación apropiadas en un futuro próximo)- y, por último, (iii) si el proveedor no tienen un vínculo contractual directo con el titular afectado, la notificación se realizará en su lugar al proveedor que tenga dicho vínculo, en nuestro supuesto de hecho, ICS Exemplary/EEES.

La notificación debe incluir la información que se detalla en el Anexo del Reglamento, que distingue entre las especificaciones de las notificaciones dirigidas a autoridades y a abonados o particulares. Hay información coincidente como, por ejemplo, (i) la identidad del proveedor y sus datos de contacto; (ii) el momento y circunstancias de la violación; (iii) la naturaleza y el contenido de los datos, (iv) las soluciones contempladas; (v) las consecuencias que puede tener la violación y (vi) medidas técnicas y organizativas para paliar la violación. Para las autoridades nacionales, se requiere información adicional, como, por ejemplo, el número de particulares o abonados afectados, el número de notificaciones realizadas y las violaciones y

notificaciones acaecidas en otros Estados miembros. Los particulares deben ser informados de las medidas que han de tomar para paliar los efectos negativos.

Como se apuntaba anteriormente, el plazo de la notificación a la autoridad competente es de veinticuatro horas desde la detección de la violación. La notificación de cierta información puede ser retrasada hasta tres días desde la notificación inicial si no está inmediatamente disponible. En los casos en los que no sea posible recolectar toda la información requerida en ese plazo, el proveedor debe acreditar una justificación razonada de dicho incumplimiento.

Respecto a la notificación a un particular, únicamente las violaciones que puedan tener un efecto negativo en la privacidad o datos personales del abonado deben ser notificadas. Los factores a tener en cuenta para esta valoración incluyen (i) el tipo o naturaleza y contenido de los datos en cuestión (en particular, si se trata de datos financieros, de categorías especiales); (ii) las posibles consecuencias que la violación puede tener para el abonado o particular afectado (concretamente, cuando la violación pueda entrañar fraude o usurpación de la identidad, daños físicos, sufrimiento psicológico, humillación o perjuicio para la reputación); y (iii) las circunstancias en las que se ha producido la violación de datos (teniendo en cuenta el lugar del robo de los datos o el momento en el que el proveedor haya tenido conocimiento de que los datos se hayan en poder de un tercero no autorizado). En cualquier caso, la notificación no ha de realizarse si el proveedor

prueba que ha aplicado las medidas tecnológicas de protección convenientes de forma que los datos se han convertido en incomprensibles para toda persona que no esté autorizada para acceder a ellos (i.e. cifrado con algoritmo normalizado o sustitución por valor resumen (*hash value*) u otras medidas publicadas por la Comisión y tras consulta al Grupo del Artículo 29, ENISA y SEPD).

La notificación a un abonado o particular ha de realizarse sin dilación tras la detección, pero al contrario de lo que ocurre respecto a la notificación a autoridades, no existe un plazo límite. En circunstancias extraordinarias, donde la notificación a un abonado o particular arriesga la investigación de la violación, el proveedor puede retrasar la notificación con permiso y hasta que la autoridad nacional considere.

En cuanto a la forma de la notificación, esta ha de ser *online* y siguiendo un formulario en el caso de las autoridades y de forma clara, pronta, segura y desagregada respecto a informaciones de otros asuntos.

En casos de *outsourcing* o contratación mayorista de algún input, el proveedor que no tiene relación contractual directa con el abonado ha de informar inmediatamente al proveedor contratante de la violación de los datos personales.

En definitiva, los proveedores de servicios de telecomunicaciones y de acceso a Internet, habrían tenido que notificar a ICS

Exemplary/EEES la violación de los datos con el fin de que éste, si es necesario, lo notifique al abonado o particular.

Es importante señalar que debido a que, como se apuntaba anteriormente, esta normativa es específica para redes y servicios de comunicaciones electrónicas, los reguladores de la UE han decidido ampliar el ámbito de las obligaciones de seguridad en las redes a otros agentes dentro de la cadena de valor de la prestación de servicios de sociedad de la información, mediante la Propuesta de Directiva relativa a medidas para garantizar un elevado nivel común de seguridad de las redes de la información en la Unión Europea[21] (en adelante "Directiva SRI"). La Directiva propone la aplicación de medidas de protección a todas las redes y a todos los sistemas de información[22].

Así, sin perjuicio de la normativa sobre ciberdelincuencia, de la normativa sobre infraestructuras críticas y de la relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, la propuesta Directiva SRI establece obligaciones y mecanismos de cooperación que han de cumplir los estados de la Unión, así como obligaciones y medidas de seguridad en las redes que han de imponerse, no sólo al sector de las comunicaciones electrónicas, sino a los principales proveedores de servicios de la sociedad de la

[21] Bruselas, 7.2.2013 COM(2013) 48 FINAL 2013/0027(COD)

[22] Al estar sometidas a su normativa específica, se excluyen de esta norma tanto los proveedores de servicios de confianza como las redes y servicios de comunicaciones electrónicas, que se someten a su regulación específica de la Directiva 2002/21/CE (Directiva Marco).

información y a los que sirven de apoyo a los servicios de la sociedad de la información derivados o actividades en línea, como son: las plataformas de comercio electrónico, las pasarelas de pago por Internet, las redes sociales, los motores de búsqueda, los servicios de computación en la nube o las tiendas de aplicaciones. La interrupción de estos servicios de apoyo a la sociedad de la información impide la prestación de otros servicios de la sociedad de la información que dependen de ellos.

La Directiva propone establecer medidas para garantizar un elevado nivel común de seguridad, imponiendo a los Estados que exijan a los operadores que (i) proporcionen la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre las políticas de seguridad; y que (ii) se sometan a una auditoría de seguridad practicada por un organismo independiente o una autoridad nacional cualificada y pongan los resultados en conocimiento de la autoridad competente. Cualquier incumplimiento será sancionado y se propone que las sanciones sean eficaces, proporcionadas y disuasorias.

Desde el punto de vista de la normativa española relativa la protección de los datos personales.

5. Frente al regulador en materia de protección de datos

El ataque a los sistemas de información de la empresa afectada ha consistido, además de en la interrupción del suministro energético y la modificación de su sitio web, en la sustracción de datos de

carácter personal de un considerable número de clientes de la compañía.

No obstante, tal empresa no quedaría exonerada de responsabilidad de forma automática por el hecho de haber sufrido una intrusión ilícita en sus sistemas en el marco de un ciberataque.

Sin perjuicio de las responsabilidades imputables a los ciberdelincuentes derivadas de la intromisión ilegítima en los sistemas y el acceso no autorizado a datos personales, la propia empresa que ha sufrido el ataque podría incurrir en responsabilidad administrativa si se constatase que el mismo ha sido posible debido a una infracción de sus obligaciones en materia de protección de datos; concretamente, de su deber de garantizar la seguridad de los datos de los clientes en su calidad de responsable del tratamiento[23].

En este sentido, la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de protección de datos de carácter personal ("LOPD") consagra el principio de seguridad de los datos, obligando al responsable del fichero o tratamiento a adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no

[23] El responsable del fichero o tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que, solo o conjuntamente con otros, decide sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente [Artículo 3.d) LOPD y Artículo 5.1.q) del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre ("RLOPD")]. De conformidad con esta definición, EEES se configuraría como responsable de tratamiento respecto de los datos personales de sus clientes.

autorizado[24]. Esta obligación debe ponderarse de acuerdo con varios factores: el estado de la tecnología, la naturaleza de los datos y los riesgos a los que éstos se encuentren expuestos. Por tanto, las medidas deben ser proporcionadas y adecuadas al caso concreto.

Se prohíbe, en consecuencia, incluir datos personales en ficheros que no reúnan unas mínimas condiciones de integridad y seguridad que se regulan de forma pormenorizada en el RLOPD[25] y se clasifican, de conformidad con la naturaleza y sensibilidad de los datos tratados, como de nivel bajo, medio y alto.

Sobre esta base, el mantenimiento de ficheros, locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad se tipifica como una infracción grave, sancionable con multa de entre 40.001 y 300.000 euros cuando la infractora es una entidad privada[26].

Resulta de especial interés señalar que, de acuerdo con el criterio mantenido por la Agencia Española de Protección de Datos

[24] Artículo 9 LOPD (que transpone el Artículo 17.1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa 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 Artículos 79 y ss. RLOPD. Es importante señalar que esta obligación también recae, en su caso, sobre los encargados de tratamiento, a los que nos referiremos más adelante.

[25] Las medidas de seguridad se regulan en el Título VIII RLOPD. Estas medidas son de naturaleza técnica y organizativa si bien en otras secciones del RLOPD se recogen otro tipo de medidas dirigidas, asimismo, a garantizar un adecuado tratamiento de los datos personales (e.g. principio de calidad de los datos, deber de secreto, garantía del ejercicio de derechos ARCO -acceso, rectificación, cancelación y oposición- por parte del titular de los datos).

[26] Artículos 44.3.h) y 45.2 LOPD.

("AEPD")[27] y la doctrina de la Audiencia Nacional[28], la obligación impuesta en virtud del principio de seguridad de los datos no es una obligación de medios, sino de resultado. No basta, por tanto, con la mera implantación o aplicación formal de las medidas de seguridad (obligación de medios), sino que las medidas adoptadas han de ser eficaces en la práctica, impidiendo de forma efectiva la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales por parte de terceros (obligación de resultado).

Así, la entidad responsable del tratamiento es *"por disposición legal una deudora de seguridad en materia de datos"* a la que se exige un especial deber de diligencia en la custodia de la información personal y debe garantizar que las medidas de seguridad implantadas *"se cumplan y se ejecuten con rigor[29]"*.

En sentido contrario, de acuerdo con este criterio, si no se implementasen las medidas de seguridad previstas en el RLOPD

[27] Resolución AEPD de 21 de junio de 2013 (Resolución R/01477/2013); Resolución AEPD de 5 de junio de 2012 (Resolución R/01093/2012); Resolución AEPD de 28 de febrero de 2011 (Resolución R/00434/2011);Resolución AEPD de 8 de septiembre de 2009 (Resolución 02021/2009); Resolución AEPD de 14 de septiembre de 2009 (Resolución 02019/2009); Resolución AEPD de 20 de octubre de 2008 (Resolución R/01404/2008); Resolución AEPD de 11 de diciembre de 2008 (Exp. E/00795/2006)

[28] Sentencia AN de 11 de diciembre de 2008 (recurso nº 36/2008; JUR 2009/3136); Sentencia AN de 28 de junio de 2006 (recurso nº 290/2004; JUR 2006\204327); Sentencia AN de 23 marzo de 2006 (recurso nº 478/2004; JUR 2006\130610); Sentencia AN de 7 de febrero de 2003 (recurso nº 1182/2001; JUR 2006\275713); Sentencia AN de 13 de junio de 2002 (recurso nº 1161/2001).

[29] Entre otras, la ya referida Sentencia AN de 28 de junio de 2006 (recurso nº 290/2004; JUR 2006\204327).

pero no se constatase una alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal, no habría sanción[30].

No obstante, tal y como ha mantenido la AEPD en línea con los pronunciamientos de la Audiencia Nacional[31], pese a tratarse de una obligación de resultado, no se trata de una obligación absoluta. Así, no cabría imputar los hechos al responsable del fichero cuando, habiendo éste adoptado las medidas técnicas y organizativas necesarias y adecuadas para garantizar la seguridad de los datos personales, la intrusión se debe a una actividad ilegal por parte de terceros con elevados conocimientos informáticos.

De acuerdo con lo expuesto, en el supuesto objeto de análisis, para determinar si la empresa ciberatacada incurriría en responsabilidad por vulneración del principio de seguridad de los datos, habría que verificar si existe un nexo causal entre la falta de medidas de seguridad o la defectuosa implementación de las mismas y el acceso no autorizado a sus sistemas informáticos. En otras palabras, si la ausencia, insuficiencia o ineficacia de las medidas ha posibilitado la

[30] En el supuesto analizado por la AEPD en su Resolución de fecha 1 de abril de 2008 (Resolución R/00351/2008), el responsable del tratamiento no cumplía con las medidas de seguridad exigidas (e.g. los soportes que contenían datos personales no habían sido objeto de cifrado, las copias de respaldo se realizaba con carácter mensual, no se había designado un responsable de seguridad, no se había realizado informe alguno en relación con el análisis del registro de accesos ni las auditorías exigidas por la normativa). Sin embargo, pese a las deficiencias detectadas, la AEPD acordó no iniciar la actividad sancionadora y archivar las actuaciones pues, de la inspección llevada a cabo, no se había concluido que se hubiese producido una alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal.

[31] Resolución AEPD de 15 de abril de 2011 (Resolución R/01585/2010); Sentencia AN de 25 de febrero de 2010 (recurso nº 226/2009; JUR 2010/82723).

intrusión ilícita y la sustracción de los datos personales de los clientes de la compañía.

En todo caso, es importante mencionar que la LOPD también obliga a implementar las medidas de seguridad correspondientes a los encargados del tratamiento, debiendo tales medidas constar en el contrato que éstos deben suscribir con el responsable del fichero[32]. Asimismo, la LOPD establece que el encargado será considerado responsable del tratamiento y responderá de las infracciones en que haya incurrido personalmente cuando, entre otros supuestos, utilice los datos personales incumpliendo las estipulaciones del contrato suscrito con el responsable.

Por consiguiente, si el incumplimiento del deber de seguridad de los datos fuera imputable a un encargado del tratamiento con el que la compañía afectada hubiese contratado una prestación de servicios, sería dicho encargado quien respondería de la infracción y de la sanción correspondiente[33].

Por último, no debe obviarse la posibilidad de la apreciación del apercibimiento, en los términos y condiciones descritos en el art.45.6 de la LOPD, como ya ha hecho por la Agencia Española de

[32] Artículos 9 y 12 LOPD.

[33] Resolución AEPD de 27 de febrero de 2009 (Resolución R/00409/2009). Este procedimiento tuvo su origen en la denuncia de un particular contra el responsable de un fichero por una vulneración del principio de seguridad de los datos. No obstante, la AEPD sancionó al encargado de tratamiento al haber sido éste quien había incumplido su obligación de adoptar, de forma efectiva, las medidas necesarias para impedir el acceso no autorizado por parte de terceros a los datos de carácter personal.

Protección de Datos (AEPD) en algunos casos enjuiciados derivados de la existencia de brechas de seguridad[34].

Merece, por último, una mención especial al borrador de futuro Reglamento Europeo de Protección de Datos, que se encuentra actualmente en tramitación y cuya posible entrada en vigor traerá consigo modificaciones significativas en el ámbito de la protección de datos personales, y en concreto en aspectos del fenómeno del Data Breach Notification.

C. Responsabilidad penal

Escudriñados y analizados los posibles delitos que pudieran encajar en el supuesto de hecho objeto de estudio, vamos a analizar si cabe la posibilidad de atribuir responsabilidad penal a EEES, la empresa atacada, únicamente por los delitos de los art. 197 y 264, que de los relatados son los únicos de los que la persona jurídica puede ser responsable.

Para ello debemos atender al artículo 31 bis de nuestro Código Penal, que nos describe los criterios objetivos y subjetivos de atribución de responsabilidad criminal a la persona jurídica.

[34] Remítase, por ejemplo, a la Resolución nº R/01093/2012: http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2012/common/pdfs/A-00368-2011_Resolucion-de-fecha-05-06-2012_Art-ii-culo-9-LOPD.pdf

En primer lugar, el art. 31 bis, 1), nos informa de que la atribución de responsabilidad penal a la persona jurídica vendrá determinada por la comisión de delitos en nombre, o por cuenta, de la empresa, y en su provecho, requisitos estos que deben contarse de forma acumulativa, no excluyente.

Desde este primer análisis ya puede descartarse la posibilidad de participación criminal de la empresa ante la ausencia total de concurrencia de los requisitos esenciales del art. 31 bis: actuar en nombre o por cuenta de la empresa, y hacerlo en su provecho.

En este caso la empresa EEES es claramente perjudicada y los autores no actúan ni en nombre ni en provecho de la empresa, sino con un propósito y energía criminal únicamente atribuibles a ellos.

Igualmente sucede con la ausencia del elemento subjetivo: ni los representantes legales o administradores de hecho o de derecho, así como tampoco trabajador alguno, sometido a la autoridad laboral de los primeros, han tenido participación alguna, ni directa ni indirectamente, en el hecho criminal.

Podría darse el caso en el que la persona jurídica tuviera la doble condición de perjudicada y responsable penal por los mismos hechos, pero por los motivos expuestos, no es el caso.

El hecho de que las medidas de seguridad y los controles sobre las mismas hayan resultado ineficaces, a la vista del resultado del ataque estudiado y sus consecuencias, no determina, en absoluto, y

por sí misma, responsabilidad criminal, sino que más bien puede haber generado otro tipo de responsabilidades, como ya se ha comentado.

Por tanto, se debe excluir del análisis de la responsabilidad de la empresa EEES la correspondiente al ámbito penal.

III. Estudio de la eventual responsabilidad de la Administración Pública por no impedir el ataque.

Según se prevé por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas[35] (en adelante, LPIC), los Estados modernos y sus empresas se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo.

Asimismo, reza el Preámbulo de la citada Ley, *"[…] En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden (…) ocasionar fallos*

[35] Normativa descargable desde la siguiente URL: http://noticias.juridicas.com/base_datos/Admin/l8-2011.t3.html#t3

inesperados y cada vez más graves en los servicios básicos para la población (…)". Y continúa diciendo, "(…) la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques (…). Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las Comunidades Autónomas (…)".

Así las cosas, cualquier interrupción no deseada como consecuencia de incidencias[36] en el suministro de servicios básicos a la ciudadanía, por ejemplo, en el suministro de energía eléctrica, –como parece concurrir en el supuesto de hecho al que se refiere este Informe-, podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales[37] asociados, con carácter básico, a sectores

[36] Por ejemplo, por denegación de servicio; infección por malware; compromiso del sistema; hacking; violación de políticas, entre otras posibles.

[37] El 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 (art.2 a) de la Ley 18/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas).

estratégicos[38], pudiendo generar también, como también indica dicha Ley, perturbaciones y disfunciones graves en materia de seguridad.

Por todo ello, la LPIC tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. También regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas.

En desarrollo de tal objeto, por un lado, se ha elaborado un Catálogo Nacional de Infraestructuras Estratégicas y, por otro lado, se ha definido un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la LPIC crea el Centro Nacional para la Protección de las

[38]La Energía se cataloga como sector estratégico conforme el Anexo a la LPIC. Como subsector en relación a éste se incluye la electricidad (infraestructuras e instalaciones de generación y transporte de electricidad, en relación con el suministro de electricidad), tal y como, prevé la propia Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF.

Infraestructuras Críticas (en lo que sigue, CNPIC) como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del Sistema de Protección de Infraestructuras Críticas en nuestro país (en adelante, el Sistema)[39].

Igualmente, como ya se adelantaba, la citada Ley regula también las especiales obligaciones que deben asumir tanto las Administraciones Públicas, como los operadores[40] de

[39] Según el art.5 de la LPIC, el Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. Resultan agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes:
a) La Secretaría de Estado de Seguridad del Ministerio del Interior.
b) El Centro Nacional para la Protección de las Infraestructuras Críticas.
c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.
d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.
g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.
h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
i) Los operadores críticos del sector público y privado.
Todo este entramado se desarrolla por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, y que concreta las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema), los diferentes instrumentos de planificación del mismo y las obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas.

[40] Conforme dispone el art.13 de la LPIC, los operadores críticos deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:
a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.
b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.
c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente.

infraestructuras críticas[41] ubicadas en territorio nacional[42], con el fin de proteger debidamente a éstas contra ataques deliberados de todo tipo (tanto de carácter físico cuanto cibernético).

---

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo.
Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas. Se deberá estar a lo dispuesto reglamentariamente al efecto en los arts.22 y siguientes del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Existe una "GUÍA PARA LA ELABORACIÓN DE PLANES DE SEGURIDAD DEL OPERADOR Y PLANES DE PROTECCIÓN ESPECÍFICA" editada por AEISEguridad que puede resultar de interés: http://www.aeiseguridad.es/index.php/Una_guia_ayudara_a_los_proveedores_de_seguridad_en_infraestructuras_criticas_a_elaborar_Planes_de_Seguridad_y_Proteccion
e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.
f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.
g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.
Es requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva. La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan. Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

[41] Las Infraestructuras críticas aluden a las infraestructuras estratégicas (las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Asimismo, en lo que respecta a la designación de los operadores críticos, el art.14 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas[43] dispone que bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, en aplicación de los criterios previstos en el artículo 2, apartado h) de la LPIC[44]. En tal caso, el CNPIC, elaborará una propuesta de resolución al respecto y la notificará al titular o administrador de aquéllas. El interesado dispondrá de un plazo de quince días a contar desde el día siguiente a la recepción de la notificación para remitir al CNPIC las alegaciones que considere procedentes, transcurrido el cual la Comisión, a propuesta del Grupo de Trabajo, dictará la resolución en la que se designará, en su caso, a dicho operador, como crítico. Esta resolución podrá ser recurrida en alzada ante el Secretario de Estado de Seguridad, y, eventualmente, con posterioridad, ante la jurisdicción contencioso-administrativa, en los términos generales previstos en la legislación

[42] Se exceptúan de su aplicación las infraestructuras 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 (art.3.2 de la LPIC).

[43] Puede accederse al este texto normativa desde la siguiente URL: http://noticias.juridicas.com/base_datos/Admin/rd704-2011.html

[44] Art.2 h) LPIC relativo a los Criterios horizontales de criticidad: *" Los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:*

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.(…)"

vigente en materia de procedimiento administrativo y del orden jurisdiccional contencioso-administrativo.

Al margen de las funciones y deberes asociados a los operadores críticos, e indicadas con anterioridad, se destaca la especial obligación en torno a la seguridad de las comunicaciones de forma que los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado (art.15 de la LPIC).

En otro orden de cosas, debe reseñarse, sin perjuicio de lo anterior, la existencia de Planes de Apoyo Operativo específicamente desarrollados en el art.30 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Se refieren a los documentos operativos, cuyo contenido mínimo establece el CNPIC, donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas. Así, por cada una de las infraestructuras críticas e infraestructuras críticas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o,

en su caso, el órgano competente de la Comunidad Autónoma[45], supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura.

Así, sobre la base de sus correspondientes Planes de Protección Específicos, los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

[45] En coherencia con lo dispuesto por el art.10 de la LPIC, las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

Los Planes de Apoyo Operativo serán validados y aprobados por la Secretaría de Estado de Seguridad, a través del CNPIC, y las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de cada Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean validados, todos los Planes de Apoyo Operativo de las infraestructuras críticas e infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado.

Los Planes de Apoyo Operativo deberán ser revisados cada dos años por el cuerpo policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, requiriendo la aprobación expresa del CNPIC.

En lo relativo a la identificación y reporte de incidentes de seguridad para operadores estratégicos, INTECO ha elaborado una Guía básica de protección de Infraestructuras Críticas:

http://www.inteco.es/guias/Puesto_Operador_Proteccion_Infraestructuras_Criticas.

En todo caso, tal y como se prevé en la Resolución del Parlamento Europeo, de 12 de junio de 2012, sobre la protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global (2011/2284(INI)), *"[…] la próxima «Estrategia de Seguridad en Internet» de la Comisión debería tomar como centro de referencia la labor en materia de CIIP y adoptar un enfoque global y sistemático de la ciberseguridad que incluya tanto medidas proactivas, por ejemplo, la introducción de pautas mínimas para las medidas de seguridad o la formación de los usuarios particulares, las empresas y las institucione*s públicas, como reactivas, por ejemplo, sanciones penales, civiles y administrativas (…)".[46]

En este ámbito, recientemente, se ha aprobado en España la denominada Estrategia de Ciberseguridad Nacional[47] que, entre otros aspectos de interés, fija las directrices generales del uso seguro del ciberespacio, mediante una visión integradora que implique la coordinación de Administraciones Públicas, el sector

[46]Protección de infraestructuras críticas de información: hacia la ciberseguridad global (P7_TA(2012)0237). Resolución del Parlamento Europeo, de 12 de junio de 2012, sobre la protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global (2011/2284(INI)) (2013/C 332 E/03): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:332E:0022:0028:ES:PDF

[47] Accesible desde la siguiente página web: http://www.lamoncloa.gob.es/NR/rdonlyres/2A778417-DABC-4D36-89A2-3B81565C3B82/0/20131332EstrategiadeCiberseguridadx.pdf

privado y los ciudadanos bajo el prisma del principio rector incluido en esta Estrategia y relativo a la responsabilidad compartida[48].

Entre los principales objetivos de esta Estrategia está, por lo que se refiere a las empresas y las infraestructuras críticas, el impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y por los operadores de infraestructuras críticas en particular. Al efecto, se debe considerar el impacto que para España puede tener una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales a la sociedad, en gran medida, en manos del sector privado.

Por lo tanto, resulta lógico en el marco del documento relativo a esta Estrategia, se afirme de forma literal que: *"[…] las medidas que se adopten en materia de ciberseguridad deberán estar alineadas con los requisitos expresados en la normativa reguladora de Protección de Infraestructuras Críticas, para alcanzar un conjunto*

[48] En relación a este principio, se debe tener en cuenta lo previsto en el Considerando 6 de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección que indica: *"(…) La responsabilidad principal y última de proteger la ICE corresponde a los Estados miembros y a los propietarios u operadores de tales infraestructuras (…)".* Por su parte el Considerando11 de la misma Directiva indica que *"(…) En toda las ICE designadas deben existir planes de seguridad del operador o medidas equivalentes (…). En caso de que no existan tales planes, cada Estado miembro intervendrá oportunamente para asegurarse de que se ponen en marcha las medidas adecuadas (…)".* Remítase a la siguiente URL para la oportuna descarga, si así lo desea, del documento legal de referencia*:* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF

integrado de medidas de aplicación a los sectores afectados (…)"[49] y que, además, entre las líneas de actuación específicas, la Línea 3 disponga lo que sigue: *"[…] Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales. Es necesario incrementar la resiliencia de las Infraestructuras Críticas españolas para evitar una potencial alteración del normal funcionamiento de los servicios esenciales que podrían afectar a la actividad diaria de los españoles. En este ámbito, el Gobierno de España adoptará, entre otras, las siguientes medidas:*

- *Asegurar la implantación de la normativa sobre Protección de las Infraestructuras Críticas con el fin de conseguir una seguridad que abarque tanto el ámbito físico como el tecnológico. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan.*

- *Ampliar y mejorar las capacidades del CERT de Seguridad e Industria, potenciando la colaboración y coordinación con el Centro Nacional para la Protección de Infraestructuras Críticas, con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado.*

[49] Remítase a la página 23 del Documento relativo a la Estrategia Nacional de Ciberseguridad: http://www.lamoncloa.gob.es/NR/rdonlyres/2A778417-DABC-4D36-89A2-3B81565C3B82/0/20131332EstrategiadeCiberseguridadx.pdf

- *Impulsar la participación del sector privado en los Programas de Ejercicios de Simulación de Incidentes de Ciberseguridad.*

- *Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas.(…)".*

En nuestro caso, Energías Estatales de España (EEES) es una sociedad anónima establecida en España cuyo objeto social se enmarca en la prestación de servicios de suministro energético y de distribución a empresas y consumidor final a nivel nacional (energía eléctrica), por lo que está sujeta a la normativa reguladora del sector eléctrico, la relativa a la protección de las infraestructuras críticas (pudiendo ser calificada como operador crítico del sector privado, la normativa protectora de datos personales, etc.).

IV. Análisis de la eventual responsabilidad de la empresa proveedora de servicios Cloud, SCADA, etc.

Introducción.

La externalización de servicios que podemos caracterizar, en términos generales, como de carácter tecnológico, convierten a los proveedores de los mismos en actores relevantes, lo quieran o no,

de la prevención, la detección y la reacción frente a ciberataques. Lógicamente, podemos pensar que la responsabilidad primera y principal frente al ciberataque es de la empresa que lo recibe o sufre, y no de los prestadores de servicios que se ubican "detrás" de ella y que prestan sus servicios en su nombre y por su cuenta, y en definitiva en su beneficio.

Sin embargo, la cuestión es que los proveedores de servicios Cloud, SCADA u otros servicios relevantes, y en igual medida sus propios subcontratistas, no ocupan una posición tal que se pueda señalar, sin más y desde el inicio, su ausencia de responsabilidad. Antes bien, puede haber escenarios y supuestos en que es posible que sí se les pueda atribuir cierta responsabilidad propia y significativa, en relación a la ocurrencia y consecuencias del ciberataque.

Responsabilidad contractual, dónde empieza y dónde acaba el contrato.

Lógicamente, la primera responsabilidad de tales proveedores que parece que se puede señalar es la de carácter contractual que se deriva de la relación jurídica que mantienen con la empresa que sufre el ataque. Y hablamos de relación jurídica, que no únicamente de contrato, porque en muchas ocasiones tal relación jurídica se configura a través de una suma de elementos, cada uno con su propio peso específico, su proceso de evolución y su mayor o menor cercanía o relevancia en caso de ciberataque.

Así tenemos en primer lugar el propio contrato, que debería establecer el régimen de responsabilidad del proveedor, al menos en términos generales. Añadido, adjunto o anexo al contrato, debería estar el Acuerdo de Nivel de Servicio, que rige la vida o ejecución del servicio contratado, y que por tanto es clave en su delimitación.

Pero es que en muchos casos, además de la relevancia de los acuerdos y pactos precontractuales, van a ser críticas en la posible atribución de responsabilidad al proveedor las modificaciones que del contrato, acuerdo de nivel de servicio y demás elementos se puedan llevar a cabo durante el tiempo de vida del servicio adquirido. Además de que hay una realidad no escrita, sino de carácter puramente fáctico, que viene determinada por el modo en que, en la práctica, se presten los servicios, con conocimiento y aceptación siquiera tácita de las partes, que puede ser que haga que la relación jurídica se haya de medir y valorar, así como la responsabilidad en caso de ciberataque, por parámetros (total o parcialmente) externos al contrato y sus anexos.

Además, cabe señalar dos aspectos que además pueden hacer más compleja aun la delimitación, exigencia y concreción o cuantificación de tal responsabilidad:

- *Subcontratación. Es habitual, por no decir que siempre ocurre, que el proveedor contratado tenga a su vez subcontratadas*

determinadas partes de su servicio en uno o varios subcontratistas.

En principio, lo normal es que la responsabilidad del proveedor se le exija plenamente a él, que habrá en su caso de repetir contra sus subcontratistas. Pero la falta de regulación de las consecuencias de la subcontratación en escenarios como el analizado en este Estudio, da lugar a que los entramados de responsabilidad se conviertan en un laberinto arduo y complejo.

- *Seguros. Cada vez es más habitual que los prestadores de servicios como los señalados contraten "ciberseguros", que les permitan externalizar las consecuencias dañosas para terceros de un ciberataque en el que se les pueda atribuir una responsabilidad propia.*

  En tal caso, la relación con la correspondiente Aseguradora (coberturas, exclusiones, determinación del siniestro, cuantificación del daño, modo de indemnización, etc.), pueden ser elementos a valorar en la contratación del proveedor, y a analizar con detalle en la fase reactiva frente al ciberataque y aun tras este en la valoración de consecuencias y los medios para evitar su repetición.

Responsabilidad extracontractual, posibilidad de que concurra.

La existencia, en mayor o menor medida o dicho de otro modo con mayor o menor grado de exigibilidad (teórica y práctica), de responsabilidad contractual del proveedor de servicios como los relativos a Cloud o SCADA, en caso de ciberataque, no permite excluir en todo caso la posibilidad de una responsabilidad extracontractual diferenciable.

Así, a efectos meramente teóricos, pensemos en el caso de una actuación del proveedor, en la fase de reacción del ciberataque, que provoca o produce un daño de naturaleza reputacional a la empresa que ha sufrido el ciberataque. Sería el caso de falta de colaboración del proveedor con las Fuerzas y Cuerpos de Seguridad del Estado u otras Administraciones Públicas competentes (siendo que esta actuación ya de por sí puede tener consecuencias graves para el contratante del servicio), que trasciende a los medios de comunicación y se atribuye a la empresa que ha sufrido el ataque (que al fin y al cabo es quien resulta la relevante para la opinión pública).

En tal caso, podemos pensar que el daño reputacional causado, una vez demostrado y cuantificado, puede ser atribuido al proveedor por vía del régimen de responsabilidad civil extracontractual.

En definitiva, este tipo de responsabilidad no va a ser la más común o habitual de cara a proveedores de servicios como los señalados, pero eso no hace que se pueda descartar sin acudir antes a las circunstancias del caso concreto.

V. Actuaciones reactivas de las Fuerzas y Cuerpos de Seguridad después del ataque (Investigación, Policía, Fiscalía, Guardia Civil)

Analizando la situación descrita, las actuaciones de las Fuerzas y Cuerpos de Seguridad del Estado ante este supuesto de hecho se encuentran reguladas, aunque no de un modo específico, tanto en la Ley Orgánica del Poder Judicial[50] y en la Ley de Enjuiciamiento Criminal (LECrim)[51], como en la Ley 8/2011, de infraestructuras críticas[52] y, a nivel internacional, en el Convenio de Budapest de 2001 sobre Ciberdelincuencia[53].

Ante la carencia de legislación específica en lo atinente a medios de prueba electrónicos en el proceso penal, nos referiremos también a

[50] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
[51] Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.
[52] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
[53] Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 (Instrumento de Ratificación por España en BOE de 17 de septiembre de 2010).

la reciente propuesta de Texto articulado de Ley de Enjuiciamiento Criminal (2013)[54].

Recibida la oportuna denuncia de los hechos relatados por parte de EEES, bien ante la Guardia Civil, o policía correspondiente, se deberán abrir diligencias de Policía Judicial (arts. 282 y ss LECrim), dando oportuna cuenta al Juzgado de Instrucción correspondiente y al Ministerio Fiscal en el plazo máximo de 24 horas (art. 295 LECrim) y conteniendo las mismas en el Atestado (art. 292 LECrim), en el cual especificarán los hechos por ellos averiguados, insertando las declaraciones e informes recibidos, y anotando todas las circunstancias que hubiesen observado y pudiesen ser prueba o indicio del delito.

Entre las diligencias a practicar por la Policía Judicial, se encontrarían las siguientes:

1. Toma de declaración de técnicos y responsables de EEES y de sus proveedores (292 LECrim).

2. Entrada y registro en las instalaciones de las tres empresas y, en su caso, en el domicilio del técnico usuario del PC afectado, bien sea con consentimiento de los afectados o con la preceptiva Autorización Judicial mediante Auto motivado

[54] *Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión Institucional creada por Acuerdo del Consejo de Ministros de 2 de marzo de 2012*, editado por el Ministerio de Justicia, Madrid, 2013.

(arts. 573 y ss. LECrim). Dicho Auto, deberá autorizar expresamente el registro de los dispositivos afectados (servidores y PC del técnico).

3. Intervención o aprehensión de los equipos afectados, los cuales se han de incorporar al proceso bajo la responsabilidad del Secretario Judicial, o quedarán conservadas a disposición judicial en organismo adecuado para su depósito (Art. 338 LECrim), así como de los datos, en su caso, obrantes en archivos, registros y logs, como prueba documental (Art. 726 LECrim)[55].

4. Clonación o copia de los dispositivos de almacenamiento aprehendidos para ulterior análisis, con adecuada conservación y reserva de los soportes originales a fin de garantizar su autenticidad e integridad (Art. 230.2 LOPJ).

[55] Siguiendo a Joaquín Delgado, "los dispositivos electrónicos pueden ser ocupados o aprehendidos en tres supuestos: como cuerpo del delito, es decir, la cosa objeto de la infracción penal o contra la que se ha dirigido el hecho punible; como instrumentos del delito, esto es, los medios u objetos a través de los cuales se ha llevado a cabo la comisión de la infracción penal; y como piezas de convicción, entendidas como los objetos, huellas y vestigios que, no estando incluidas en las dos categorías anteriores, tienen relación con el delito y pueden servir de prueba o indicio en la comprobación de la existencia, autoría o circunstancias del hecho punible." Asimismo, "únicamente han de ser ocupados aquellos dispositivos que resulten estrictamente necesarios para la tramitación del proceso (argumento ex art. 574 LECrim.), procediendo en otro caso únicamente a la ocupación de los datos." - Joaquín DELGADO MARTÍN / La prueba electrónica en el proceso penal - Diario La Ley, No 8167, Sección Doctrina, Editorial LA LEY / Octubre 2013.

5. Dictamen pericial, llevado a cabo por peritos informáticos expertos sobre las copias previamente clonadas (Arts. 456 y ss LECrim).

6. Solicitud de asistencia judicial internacional a fin de que, por un lado, se libre oficio al ISP correspondiente para que aporte los datos del titular de la línea correspondiente con los números IPs presuntamente origen del ataque y, por otro lado, se autorice y ejecute, por la autoridad competente, la entrada y registro en la sede o domicilio correspondiente, con aprehensión de los dispositivos informáticos encontrados (Art. 31 del Convenio de Budapest de 2001 o precepto análogo de Convenio aplicable) y, en su caso, detención, toma de declaración y puesta a disposición judicial de los presuntos autores, sin perjuicio de la ulterior solicitud de extradición correspondiente.

VI. Especial mención a la protección de la información de los clientes en los despachos de abogados

Como punto de partida, debemos hacer mención que en virtud del secreto profesional, los abogados en el ejercicio de su profesión ya disponen de un elemento adicional que les obliga a mantener el máximo recelo en la custodia de todos aquellos datos que obtiene debido a la relación que les une con sus clientes[56].

Además, debido al tipo de información que es tratada por el despacho de abogados en conjunto con la empresa EESS, también debe tenerse presente que resulta de plena aplicación a los mismos la legislación sobre Protección de Datos, regulada en la Ley 15/1999 de 13 de diciembre, LOPD, y su reglamento de desarrollo Real Decreto 1720/2007 de 21 de diciembre.

La citada normativa regula el deber de secreto en materia de protección de datos por la condición del despacho de abogados como responsable del tratamiento de los datos y el incumplimiento de este deber está sancionado por la Ley Orgánica de Protección de Datos con sanciones de elevadas cuantías.

[56] Este deber de secreto profesional se regula en el Código Deontológico de la Abogacía Española de 27 de noviembre de 2002 y en Ley Orgánica 6/1985, Ley Orgánica del Poder Judicial, como el derecho a no revelar la información facilitada por los clientes e impone el deber de custodia y protección de dicha información.

Debemos tener presente que los despachos de abogados hacen uso de la información en muchas ocasiones ajustada a un nivel de seguridad de conformidad con lo establecido en la normativa, nivel alto de seguridad, lo que implica la necesidad de que los datos a los que tiene acceso en relación a los servicios que presta, deban contar con las máximas medidas de protección que garanticen que esos datos no van a ser utilizados por terceros con finalidad distinta a la que fueron recabados.

Y no estamos hablando de aplicación de medidas de seguridad sólo a nivel documental, sino que en la actualidad y por el uso generalizado de los servicios de cloud computing, en muchas ocasiones, el almacenamiento de los datos a los que tienen acceso, se encuentran ubicados fuera de su propio control y gestionados por terceros que pueden hacer uso de los datos si no exigimos una garantías a nivel contractual que nos permita reforzar la seguridad de los mismos.

En el supuesto de hecho nos encontramos con una sustracción de información de un despacho de abogados a consecuencia del ataque del que ha sido víctima la empresa EESS, lo que nos lleva a un supuesto de comisión de un delito perpetrado a dos víctimas a consecuencia de la relación de colaboración existente entre la empresa EESS y el despacho de abogados.

En este aspecto, debemos tener presente que EESS, por la aceptación del acuerdo de colaboración, se convierte en responsable frente al despacho de abogados al no haber garantizado unos niveles de seguridad idóneos para la protección de la información que compartían, así como las posibles consecuencias negativas tanto a nivel económico como reputacional que puede recaer sobre el despacho de abogados al no haber realizado la empresa EESS una eficaz gestión de los Sistemas de Seguridad establecidos.

A la hora de calcular los daños causados, debemos tener en cuenta el plan de contingencias establecido por la empresa EESS y el despacho de abogados, a través del cual, se podrá verificar el daño real sufrido y la posibilidad de restaurar el estado de los sistemas atacados o la recuperación de la información que ha sido sustraída.

En nuestro caso particular, debemos tener expresa constancia de cuál es el protocolo de conservación de los datos, con qué frecuencia se hacen copias de seguridad, en caso de pérdida de los datos, que mecanismos de recuperación de los datos se encuentran implantados, etc.

La problemática con la que nos encontramos hoy en día, tanto en las empresas como en los despachos de abogados, versa sobre la nula "puesta en práctica" de las medidas de seguridad establecidas en la leyes y la escasa implantación de programas de Compliance y análisis de riesgos, así como la aplicación de medidas de índole técnica que permitan definir protocolos a la hora de poner en

marcha los planes de recuperación una vez evaluado el daño recibido y erradicada la amenaza que provocó el ciberataque.

Las consecuencias de un ciberataque son difíciles de calcular de manera preventiva si no disponemos de un buen plan de contingencias o Programas de Compliance, pero lo que si podemos conocer son las herramientas de las que podemos disponer para depurar responsabilidades y determinar al autor del ilícito cometido; cabe mencionar como ejemplo, la posibilidad de interposición de querella invocando el artículo 197.3 del Código Penal para la investigación del delito cometido.

Una de las consecuencias negativas más frecuentes son las posibles reclamaciones que podemos tener por parte de los clientes a través de la interposición de denuncias ante la AEPD por incumplimiento de la LOPD y de la obligación del deber de secreto profesional.

Como se ha mencionado con anterioridad, podemos encontrarnos con una situación *a priori* ajena a nuestra actividad profesional (ciberataque a una empresa colaboradora) que puede afectar a uno de los activos más importantes de nuestro despacho de abogados como es la información y las bases de datos de nuestros clientes.

Por todo lo expuesto, se establecen las siguientes pautas y/o recomendaciones para reducir o minimizar en la medida de lo posible los efectos negativos de un ciberataque:

- Establecer programas de Compliance donde se realicen análisis de riesgos sobre en qué infraestructuras es necesario reforzar la Seguridad de los Sistemas de Información.

- Elaborar un plan de contingencias donde podamos vislumbrar los escenarios posibles tras la perpetración de un ciberataque y que medidas podemos aplicar para paliar los efectos negativos del mismo.

- En caso de establecer acuerdos de colaboración con terceros, verificar que garantías y medidas de seguridad aplican en la gestión de los procesos de Seguridad de la Información y determinar la responsabilidad en caso de incumplimiento del acuerdo de colaboración por la inadecuada gestión de los Sistemas de Seguridad de la Información al no ofrecer un nivel de protección similar a la implantada en nuestro despacho de abogados.

Conclusiones y mejoras observadas

I. Estado actual de la legislación aplicable a este supuesto e identificación, en su caso, de mejoras legislativas.

Es innegable que la ciberseguridad es un objetivo estratégico de seguridad nacional. La ciberseguridad afecta al correcto funcionamiento de la sociedad de la información en su conjunto, alcanzando distintos planos: político, social, económico, legal, técnico y de gestión. Desde esas distintas perspectivas se insinúa la complejidad de proteger los diversos bienes jurídicos susceptibles de sufrir daños. Es preciso por tanto voluntad política para diseñar e implementar una estrategia efectiva. Una reacción firme sin duda generará confianza en el conjunto de la sociedad.

No obstante lo anterior, la diferente situación económica y tecnológica existente a escala mundial se traduce en diversos grados de desarrollo normativo. En áreas como África del Norte y África Subsahariana el bajo índice de instauración de internet conlleva poca preocupación por el problema de la seguridad. El ejemplo contrario lo encontramos en zonas como América del Norte, o la emergente América Latina. El caso más intervencionista sobre seguridad en las redes es el de Asia, donde los Gobiernos están actuando de forma incipiente en la gestión de contenidos,

identificación, filtrado y sistemas de criptografía. Finalmente, en Oriente Medio existe una explotación monopolística de las redes de comunicaciones, circunstancia que determina el diseño del marco normativo aplicable. Para terminar con este breve repaso a la situación internacional, mención especial merece el estudio «Comprehensive Study on Cybercrime», publicado en febrero de 2013 por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) como respuesta a la petición recibida por la Comisión sobre Prevención del Delito y Justicia Penal, en la Resolución 65/230 de la Asamblea General.

En Europa, el punto de arranque lo encontramos en el Convenio del Consejo de Europa, sobre cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001. Como primer instrumento normativo en el ámbito europeo, supone un paso decisivo hacia la armonización de las legislaciones en esta materia. Sin embargo, la constante innovación tecnológica y la creciente profesionalidad de la delincuencia han provocado la necesidad de numerosas actualizaciones. Posteriormente han destacado otros instrumentos como el Convenio 108/81 del Consejo, de 28 enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; o la Directiva 95/46CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de los datos personales de las personas físicas y a la libre circulación de estos datos. A los anteriores, les han seguido otros como la Directiva 2000/31/CE del Parlamento y

del Consejo Europeo, de 8 de junio, en materia de servicios de la sociedad de la información; la Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; la Directiva 2006/24/CE, sobre conservación de tráfico de las comunicaciones electrónicas; la Directiva 2000/375/JAI, destinada a la adopción de medidas, fundamentalmente de actuación policial, para la persecución de conductas de pornografía infantil; la Decisión marco 2001/413/JAI del Consejo, de 28 de mayo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; la Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil; la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero relativa a los ataques de los que son objeto los sistemas de información, derogada por la vigente Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.

En nuestro Ordenamiento interno, destaca en primer lugar la implicación de ciertos derechos constitucionalmente reconocidos como el derecho fundamental a la intimidad (18.1 CE), el derecho fundamental a la inviolabilidad del domicilio (18.2 CE), el derecho fundamental al secreto de las comunicaciones (18.3 CE), el derecho a la no intromisión en el entorno digital (18.4 CE), el Habeas data,

la libertad de expresión e información (art. 20 CE). Por otro lado, en materia penal destaca la necesidad de mayores precisiones, en cuanto al grupo de delitos contra la intimidad (acceso ilícito, interceptación ilícita, descubrimiento de secretos e interceptación de comunicaciones, descubrimiento de secreto informático), crimen organizado y delincuencia profesional (fraudes informáticos, blanqueo de capitales), ciberterrorismo, atentados contra la integridad de datos e integridad del sistema, fraudes informáticos (falsedad y estafa informática), responsabilidad de las personas jurídicas, pornografía infantil. Por último, no podemos dejar de destacar los problemas procesales, representados fundamentalmente por la competencia y jurisdicción (aplicación extraterritorial de la ley penal, cooperación internacional, extradición y euroorden), medios de investigación y prueba (interceptación de comunicaciones, diligencia de entrada y registro y confiscación de discos duros, registro y decomiso de datos informáticos almacenados, recogida en tiempo real de datos informáticos, interceptación de datos relativos al contenido, interceptación de datos externos o de tráfico), responsabilidad del proveedor de servicios.

En suma, de lo que aquí se ha tratado es de ofrecer algunas soluciones al problema de un ciberataque. En todo caso, no estará de más recordar que nos encontramos en el albor, tanto desde la perspectiva de la tipología de los ataques, como desde las soluciones que el sistema jurídico puede aportar.

II. Mejoras operativas: colaboración público – privada: la labor de los CERT´s, investigación de las Fuerzas y Cuerpos de Seguridad, colaboración internacional, reserva de la confidencialidad y salvaguarda de la reputación corporativa.

La creciente conectividad y el uso masivo del ciberespacio, un nuevo entorno totalmente transversal e imbricado en todos los estamentos de una sociedad moderna, es una constatación más de la necesidad de fijar una base común que pueda hacer frente a un ataque o una acción delictiva a ciudadanos, empresas o estados, perpetrada parcialmente o en su totalidad por medios digitales.

Si bien es cierto que este nuevo entorno conlleva ciertas dificultades inherentes jurídico-técnicas, la aparente despreocupación política a nivel internacional no puede obviar este nuevo entorno que aglutina en la actualidad la variedad delictiva de mayor crecimiento en la actualidad, el cibercrimen, habiéndose datado el volumen total de las pérdidas asociadas al mismo en 87.000 millones de euros a nivel mundial en 2013.

Este hecho ejemplifica a la perfección la vulnerabilidad sistémica del nuevo entorno: el crecimiento, ubicuidad y nivel de penetración de las nuevas tecnologías supera con creces la velocidad de los procesos legislativos existentes.

Es necesario plantearse si, ante este escenario, las empresas privadas preparadas para afrontar una acción criminal de estas características de una forma garantista que respete sus derechos en un mercado competitivo como el actual, teniendo en cuenta que:

- La potencial ubicuidad de las actuaciones criminales realizadas a través del ciberespacio pone de manifiesto la fragmentación jurídica existente en el plano internacional, si bien existen acuerdos multilaterales que agrupan determinadas regiones de extensión variable (como sucede en la UE). En muchos países, las disposiciones jurisdiccionales reflejan la idea de que la ejecución completa de un delito no necesita tener lugar en el mismo país con el fin de hacer valer su jurisdicción territorial. Los vínculos territoriales pueden realizarse con referencia a los elementos o efectos de la acción, a la ubicación de los sistemas informáticos o a los datos utilizados por el delito. De especial relevancia es el vacío en términos de cooperación en la lucha contra el cibercrimen existente entre España y Latino América. Sería lógicamente deseable que los estados latinoamericanos pudieran adherirse al Convenio de Budapest, lo cual aportaría al tejido empresarial español con intereses en dicha región, las garantías jurídicas mínimas necesarias en cuanto a cibercriminalidad y estabilidad del ciberespacio nacional latinoamericano.

- La divergencia, o ausencia en algunos casos, de una tipificación formal a nivel internacional de los actos considerados como delictivos en el ciberespacio, supone un serio problema, pudiendo crear lagunas jurídicas y dando lugar a regiones opacas o "paraísos de cibercrimen". Si bien en determinadas regiones existe un cada vez más nutrido grupo de normas nacionales en materia de ciberdelito, se hace notar la falta de tipificaciones comunes.

- La falta de armonización y estandarización procesal de las pruebas electrónicas pueden conllevar la aplicación errónea de procedimientos de garantía de cadena de custodia que no sean admisibles en sede judicial o bien que violen determinados derechos básicos.

- La alta fragmentación entre los actores estatales con competencias en la lucha contra el cibercrimen dificultan la efectividad en la lucha contra la ciberdelincuencia y provoca cierta confusión ante empresas y ciudadanos. El ciberespacio, debido a su alcance transregional, constata la falta de operatividad de los mecanismos de cooperación judicial y policial existentes en la actualidad. Los medios tradicionales de cooperación internacional formal en materia de cibercrimen no se encuentran habilitados para garantizar la obtención de pruebas electrónicas, por lo general, de difícil acceso, volátiles y ubicuas. En este sentido, la ubicación

como elemento de prueba en el ciberespacio debe ser replanteado, permitiendo un acceso directo a datos extraterritoriales por parte de autoridades policiales nacionales.

De esta forma, a fin de evitar impactos no previstos derivados de la falta de madurez regulatoria y procedimental y del creciente número de amenazas ciber, las empresas deberían disponer de una estrategia integral a través de una hibridación jurídico-técnica, tanto a nivel empresarial como a nivel sectorial, pivotando sobre los siguientes ejes:

1. Verificar la adhesión, de los mercados y países en los que opera, a los instrumentos multilaterales de cooperación internacional sobre prueba electrónica en materia penal (marco legislativo de aplicación).

2. Reacción ágil ante un ciberdelito, posibilitando la recuperación y la vuelta a la normalidad en un lapso de tiempo mínimo (resiliencia), permitiendo además realizar procesos de investigación para dilucidar los hechos con garantías jurídicas y poder tomar acciones en base a esa información.

3. Disponer de sistemas de detección de acciones maliciosas en curso, incluso en estadios tempranos, conocido como ciberinteligencia.

4. Prevenga la ocurrencia de ciberataques, eliminando la oportunidad y proteja la empresa ante los mismos.

III. Protocolo de denuncia ante un ciberataque y medidas para ser más eficiente en la gestión posterior y minimizar impactos.

Un supuesto de estas características requiere de una adecuada y rápida reacción, lo que puede conseguirse a través de protocolos internos de actuación, que detallen los procesos que debe seguir la organización tanto en la fase de detección de la amenaza como en las fases posteriores al ataque.

En una situación como la descrita, resulta de suma importancia la puesta en conocimiento del ataque tanto al correspondiente CERT como a las fuerzas y cuerpos de seguridad del Estado y, en su caso, al regulador competente.

A estos efectos, a continuación se especifica en mayor detalle cuáles son las actuaciones que, desde las fuerzas y cuerpos de seguridad del Estado, se recomienda adoptar en caso de sufrir un ciberataque y cuál debe ser la información y documentación a recopilar tras tener conocimiento de un ataque de este tipo:

- Direcciones IP, incluyendo fecha, hora y puerto.

- Completa y detallada descripción del incidente, fecha, duración y alcance.
- Identificación de los equipos comprometidos y activos afectados.
- Informe/resumen de las medidas adoptadas tras el ataque.
- Valoración económica aproximada del impacto.
- Extracto de los *logs* del sistema (eventos, seguridad, sistema, etc.): recomendable recogida con firma con certificado digital con sello temporal (*time stamping*).
- Descripción del estado actual de la resolución del incidente.

PROTOCOLO DE DENUNCIA ANTE UN CIBERATAQUE

En previsión de eventuales ciberataques a una organización, se recomienda el estudio de la GUÍA STIC CCN-CERT 403, sobre GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICOS. En ella pueden encontrarse indicaciones y recomendaciones dirigidas a cómo debe organizarse la empresa ante una situación de ataque informático, de cara a poder responder adecuadamente a un incidente, recopilar datos para su investigación, y obtener las evidencias de forma apropiada.

Dónde denunciar

GDT-Guardia Civil

Email - gdt@notificaciones.guardiacivil.es

Web - www.gdt.guardiacivil.es

Telf. - +34 91 503 13 00 Fax - +34 91 503 14 37

BIT-Policía Nacional

Email - delitos.tecnologicos@policia.es

Web – www.policia.es/org_central/judicial/udef/bit_contactar.html

Telf. - +34 91 582 27 51 Fax - +34 91 582 27 56

Sección Central de Delitos en Tecnologías de la Información (SCDTI)-Ertzaintza (País Vasco)

Email - delitosinformaticos@ertzaintza.net

Web – www.ertzaintza.net

Mossos d'Esquadra- (Catalunya)

Web – http://www20.gencat.cat/portal/site/mossos

Fiscalía

Web – www.fiscal.es

INTECO

Email – PIC@cert.inteco.es

Web – www.inteco.es

Telf. - +34 98 787 71 89 Fax - +34 98 726 10 16

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)

Email – PIC@cert.inteco.es / ses.cnpic@interior.es

Web – www.cnpic-es.es

Telf. - +34 91 537 25 57 Fax - +34 91 537 19 44

Anexo I: "El papel de los CERTs y su regulación en la LSSI"

La Disposición Final Segunda de la Ley 9/2014, de 9 de mayo, de Telecomunicaciones, introduce varias y muy relevantes modificaciones en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

A los efectos que aquí nos interesan, el apartado Dieciséis de dicha Disposición Final introduce en la LSSI una disposición final novena de gran importancia para la potenciación de la ciberseguridad en España. Dicha disposición adicional novena es del siguiente tenor literal:

> *[…] 1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven. Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las*

autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de

conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar

a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y

> *vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley."*

Dicho artículo introduce la figura del CERT (Computer Emergency Readiness Team) como equipo de respuesta a incidentes de seguridad y emergencias informáticas, cuya preceptiva existencia se contempla en el artículo 7, y donde sus obligaciones y tareas se regulan en el Anexo I de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes de la información en la Unión (2013/0027 (COD)). Entre estas tareas se encuentran las de supervisar incidentes a escala nacional, difundir alertas tempranas sobre riesgos e incidentes de ciberseguridad, dar respuesta a dichos incidentes efectuando un análisis dinámico de riesgos e incidentes y de conocimiento de la situación, y lograr una amplia concienciación del público sobre los riesgos vinculados las actividades en línea. Además de las indicadas, la nueva disposición adicional novena de la LSSI los reconoce como entidad competente para ofrecer recomendaciones de seguridad a aquellos prestadores de la Sociedad de la Información, registros de nombres de dominio

y sus agentes registradores establecidos en España que lo precisen como consecuencia de algún tipo de incidencia de seguridad producido a través de Internet, obligando a estos agentes a prestar su colaboración con el correspondiente CERT, cuya competencia vendrá determinada reglamentariamente, tal y como señala el apartado 5 de esta disposición adicional novena.

La reforma considera el *intercambio de información* como la piedra angular sobre la que debe girar la ciberseguridad. En este sentido, destaca el reconocimiento del intercambio de información sobre amenazas e incidentes de seguridad como una de las principales y más eficientes prácticas de colaboración utilizadas en múltiples ámbitos e incluso en la gestión de incidentes de seguridad cibernéticos entre los CERTs no sólo a nivel nacional sino europeo e internacional.

Este precepto supone el reconocimiento de una reiterada pretensión de estas entidades, las cuales venían reclamando mayor seguridad jurídica y un fortalecimiento de la cooperación entre los distintos actores de la red en la lucha e investigación de las ciberamenazas. En efecto, para realizar su trabajo los CERTs requieren recabar información de diferentes agentes implicados en el ciberespacio, tales como los prestadores de servicios de sociedad de la información, otros equipos de gestión de incidentes de seguridad y, en último término, de los propios afectados (particulares y empresas).

En este contexto, la nueva regulación da un paso al frente en la lucha contra la ciberdelincuencia y las ciberamenazas y aporta nuevas herramientas para enfrentarse a estas amenazas de una manera real y efectiva. Así, como puede observarse en la norma, no sólo se establece una obligación de colaboración, sino que, a su vez, se contempla la posibilidad de aislamiento de aquellos equipos infectados.

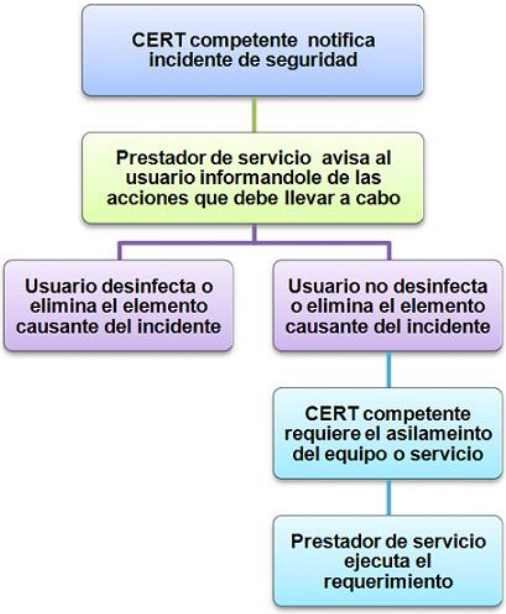
En cuanto a esta primera previsión de la obligación de colaborar con las autoridades competentes para la aportación de las evidencias técnicas, información o datos necesarios para la persecución de actividades ilícitas y/o derivados de incidentes de ciberseguridad, el proceso es el siguiente:

Las entidades de registro de nombres de dominio establecidas en España	Los Equipos de Respuesta a Incidentes de Seguridad del sector público (CERT)	Los Prestadores de servicios de la Sociedad de la Información (PSSI) establecidos en España
•Facilitan los datos relativos a los titulares de los nombres de dominio cuando las infracciones administrativas que se persigan tengan relación directa con la actividad de una página de internet identificada con los nombres de dominio que asignen. •Colaboran con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de internet •Cumplen con los códigos de conducta que se desarrollen y a los que se adhieran.	•Intercambian información con otros CERTs o autoridades competentes a nivel nacional e internacional para la prevención de incidentes en su ámbito de actuación.	•Colaboran con las autoridades competentes y el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de internet siguiendo lo previsto en los códigos de conducta. Se habla expresamente de las direcciones IP comprometidas o implicadas cuyo único límite será el respeto al secreto de las comunicaciones.

Asimismo, la ley legitima a dichos CERTs competentes para decidir sobre el aislamiento de cualquier equipo o servicio de internet geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo registro esté establecido en España, con tal de minimizar los potenciales daños que pueda estar provocando un ciberataque.

Ahora bien, hay que esperar al desarrollo reglamentario de la ley para conocer con exactitud qué entidades tendrán competencias como CERT a los efectos de lo previsto en la presente disposición.

El proceso descrito sería el siguiente:



En relación al sector de las infraestructuras críticas, la situación actual en España ha derivado en un acuerdo suscrito entre la Secretaría de Estado de Seguridad del Ministerio de Industria y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, en el que se sientan las bases para la colaboración del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO) en materia de respuesta a incidentes para las tecnologías de la información de infraestructuras críticas ubicadas en España. De este modo, INTECO se convierte en un esencial apoyo al CNPIC en la gestión de incidentes de ciberseguridad en este tipo de infraestructuras, y se pone en marcha un servicio de respuesta especializado y con capacidad especializada en el análisis y gestión de problemas e incidencias de seguridad tecnológica.

Más información:

www.ismsforum.es

C/ Castelló, 24, 5º Dcha. Esc. 1
28001 Madrid
T.: +34 91 186 13 50

www.enatic.org

Paseo de Recoletos, 13
28004 Madrid