¿ESTÁ TU EMPRESA PREPARADA PARA SUFRIR UN CIBERATAQUE?: ASPECTOS LEGALES A CONSIDERAR

Junio 2017

Estimados Sres.:

El reciente ciberataque orquestado a nivel mundial y que, en las últimas semanas ha acaparado gran parte de la atención informativa, ha convertido en actualidad un aspecto que cada vez resulta más trascendente en la actividad de cualquier empresa: **la ciberseguridad**.

Acontecimientos como el ocurrido ponen de manifiesto la situación de vulnerabilidad de las empresas ante este tipo de ataques. Son los nombres de las grandes compañías atacadas los que más eco han tenido en los medios de comunicación, pero las pequeñas y medianas empresas no se encuentran libres de amenaza y, sin duda, son y continuarán siendo objetivo de los ciberdelincuentes.

Por ello, les remitimos la presente circular, con la intención de hacerles partícipes de algunas reflexiones y recomendaciones en relación con los aspectos legales de la ciberseguridad, esperando que la misma sea de su interés.

I. La empresa en la red

Para cualquier organización que opere en el tráfico económico, las tecnologías de la información tienen ya en la actualidad una importancia incuestionable (sistemas informáticos, cloud computing, comunicaciones electrónicas de toda índole, venta on-line, etc.) que, previsiblemente, seguirá incrementándose en los próximos años de la mano de la implementación y generalización de activos tecnológicos emergentes, como el Internet de las cosas o la industria conectada.

En este contexto, la exposición de los sistemas informáticos de las compañías es cada vez mayor, incrementándose asimismo los riesgos que éstas deben afrontar. Debemos asumir que, con independencia del tamaño de nuestra organización, en mayor o menor medida, estamos conectados a Internet y por ello somos susceptibles de sufrir incidentes (accidentales o deliberadamente provocados) que pongan en riesgo nuestro negocio.

II. Marco jurídico de la ciberseguridad

La ordenación de Internet y de gran parte de los avances tecnológicos vinculados a su uso no ha seguido el esquema tradicional de regulación normativa. En los últimos años, los estados y organizaciones supranacionales con capacidad normativa apenas han desarrollado un marco legislativo propio que las empresas puedan tener como referencia inequívoca en relación con dichos aspectos.

En este sentido, los ordenamientos jurídicos español y europeo no constituyen una excepción. Actualmente, al margen de algunas iniciativas aisladas aplicables al sector público (e.g. normativa del esquema nacional de seguridad) y determinadas previsiones aplicables a materias conexas (e.g. protección de datos de carácter personal, algunos nuevos tipos penales, etc.), hoy por hoy no contamos con una referencia normativa clara en relación con Internet y los entornos digitales en general, y mucho menos con una "ley de ciberseguridad".

La escasez y fragmentación normativa y la existencia de importantes lagunas nos sitúan en un escenario complejo, agravado sin duda por la dificultad que entraña la persecución de los ciberataques que sufren las empresas. No puede obviarse que los delitos cometidos on-line no siguen el esquema tradicional de los delitos: (i) en gran parte de las ocasiones los ataques no son fácilmente detectables; y (ii) cuando se detectan, resulta de enorme dificultad determinar su origen o autoría (el anonimato que ofrece Internet y la naturaleza transfronteriza que habitualmente tienen dichas actuaciones lo hacen casi imposible).

III. ¿Qué activos de mi empresa están en peligro?

No solo las grandes corporaciones tecnológicas son objetivos para la ciberdelincuencia. La realidad demuestra que cualquier empresa puede ser objeto de un ciberataque, siendo varios los activos afectados en dichas circunstancias.

La **Propiedad Intelectual y/o Industrial, los secretos comerciales y la información confidencial** pueden ser el objetivo de un ataque (e.g. espionaje industrial, encriptación de información con exigencia de pagos, etc.), pero también lo pueden ser otros datos de nuestros **clientes y proveedores** (e.g. robos de información bancaria para la realización de campañas de phising y otras modalidades de fraude, etc.).

Asimismo, los ataques pueden perseguir anular **la actividad de la empresa** (e.g. ataques de denegación de servicios, manipulación de procesos productivos a través de equipos/maquinaria conectada a Internet, etc.).

Estas y otras situaciones que se producen con cierta frecuencia pueden generar, además de un daño económico directo, un **daño reputacional** de difícil reparación.

Por si todo esto no fuera suficientemente relevante, el próximo mes de mayo de 2018 será plenamente aplicable el nuevo **Reglamento General Europeo de Protección de Datos**, que impone nuevas obligaciones en materia de protección de datos de carácter personal, alguna de las cuales guardan estrecha relación con el objeto de la presente circular. En particular, ha de tenerse en cuenta que, de producirse una **violación de seguridad** que afecte a datos personales (y los incidentes de ciberseguridad descritos podrían serlo), las empresas afectadas estarán obligadas a **notificar dicha situación a la Autoridad de Control en un plazo máximo de 72 horas** y, en algunos casos, a los propios interesados cuyos datos se hubieran visto comprometidos.

IV. ¿Qué podemos hacer ante esta situación? Recomendaciones prácticas desde el punto de vista legal

En este escenario de riesgos y falta de regulación, la recomendación solo puede ser una: **autoprotección**. Las empresas deberían proveerse de herramientas que les permitan prevenir estos ataques, en la medida en que resulte posible, y reaccionar ante los mismos de forma adecuada y persiguiendo la salvaguarda de sus intereses.

Dichas herramientas se instrumentarían a través de "Políticas de ciberseguridad" que habrían de tener en cuenta, al menos, los siguientes aspectos:

- En primer lugar, resulta necesario adoptar las **medidas técnicas** necesarias para proteger nuestra empresa de un ciberataque. Para ello debemos auditar nuestra exposición y capacidad de reacción ante un ciberataque, llevando a cabo las inversiones que, según cada caso, puedan resultar adecuadas (infraestructura, formación de personal, etc.).

  A estos efectos podemos encontrar en nuestro entorno cercano entidades de referencia en el sector, altamente especializadas en la materia y que ofrecen asesoramiento en dichos aspectos, que nos aportarán un diagnóstico claro a este respecto.

- Pero, ¿si a pesar de todo somos atacados? **Las medidas técnicas no son infalibles y la ciberseguridad absoluta no existe**. Por ello, puede ser esencial que nuestra empresa se dote de procedimientos y políticas que, desde un punto de vista legal y con carácter tanto preventivo como reactivo, permitan gestionar los riesgos, reaccionar adecuadamente ante un ciberataque y minimizar sus efectos o consecuencias.

  En este sentido, resultará indispensable llevar a cabo las siguientes actuaciones:

  (i) Revisar, elaborar e implantar **políticas de seguridad, organizativas y de privacidad que se coordinen y complementen con las medidas técnicas adoptadas y que coadyuven a la prevención y detección de incidentes de ciberseguridad**. De esta manera, previa la oportuna auditoría jurídica de los diferentes aspectos implicados (protección de datos, comercio electrónico, confidencialidad, Propiedad Intelectual y/o Industrial, etc.), se establecerían, con carácter previo a cualquier incidente de ciberseguridad, las medidas adecuadas que permitan reducir los riesgos y la exposición de nuestra empresa.

  (ii) Establecer **protocolos de actuación ante dichos incidentes que garanticen una reacción adecuada y ordenada y contribuyan a controlar los efectos jurídicos de los mismos**, dotando a nuestra empresa de mecanismos preestablecidos que nos permitirán responder a la situación. En este sentido, será recomendable establecer, entre otros y sin ánimo exhaustivo, procedimientos y protocolos relativos a la **coordinación de la investigación del incidente**, su **análisis y la elaboración de informes jurídicos**, la **definición e implantación de medidas correctoras**, la **gestión de incidentes de seguridad con los clientes/usuarios y/o proveedores**, **comunicaciones y coordinación con autoridades y organismos supervisores**, la **gestión de la responsabilidad contractual** de la empresa, etc.

- Por último, puede resultar interesante valorar la conveniencia de contratar con una aseguradora una cobertura adecuada para los daños que, pese a los esfuerzos desplegados por nuestra empresa, puedan llegar a materializarse.

  Las **pólizas de "ciberseguridad"** comienzan a ser una realidad en el mercado y, atendidas las consecuencias que puede llegar a tener un ciberataque, pueden convertirse en una herramienta útil de cara a afrontar los daños (propios o a terceros) que se deriven del mismo.

La ciberseguridad y la actuación de la empresa en dicho ámbito no son una cuestión menor. **Un incidente de ciberseguridad puede conllevar graves consecuencias que, más allá del daño directo a nuestra organización y su negocio (e.g. pérdidas, paralización de la actividad, sanciones en materia de protección de datos, etc.), podrían conllevar incluso responsabilidad para aquellos Administradores y Directivos que, prescindiendo de la diligencia exigible, obvien el establecimiento de medidas y políticas como las aquí recomendadas**.

****

Queremos advertirles que la presente circular es meramente informativa y, por lo tanto, contiene información de carácter general que no constituye asesoramiento jurídico. En este sentido, si a la vista del contenido del presente documento necesitaran aclarar cualquier aspecto en relación con el contenido del mismo, les rogamos se pongan en contacto con nosotros para que les asesoremos adecuadamente atendiendo a las circunstancias de su caso concreto.

Sin otro particular, les saluda muy atentamente.

BSK LEGAL & FISCAL
Departamento de Nuevas Tecnologías
Persona de contacto: Ramón Solórzano
rsolorzano@grupobsk.com