Ciberseguridad: marco jurídico y operativo

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

Los retos en materia de ciberseguridad demandan la adaptación del marco legislativo y la efectiva implantación de las medidas operativas establecidas en los Planes Estratégicos.

Resumen

Ciudadanos, empresas y Estados afrontan en la actualidad notables retos de ciberseguridad. Las ciberamenazas y ciberataques tienen efectos directos en la seguridad de las personas, la economía y las propias tecnologías de la información. Los gobiernos han desarrollado estrategias, políticas y legislación diseñadas para un contexto tecnológico y de seguridad que está cambiando muy deprisa.

Este análisis estudia la primera generación de medidas adoptadas para hacer frente a los retos del ciberespacio, su implantación y la evolución del marco legal europeo y nacional en materia de ciberseguridad actualmente en desarrollo, con el propósito de reforzar la confianza digital a ciudadanos y empresas, así como garantizar la seguridad de los Estados. Nos encontramos ahora en el inicio de una nueva etapa de transformación digital en torno a la economía de los datos en Internet, que demandará en breve la adopción de medidas de nueva generación para consolidar las actuales reformas legales y actuaciones operativas en el ámbito europeo y nacional de la ciberseguridad.

Análisis

De la sociedad de la información hacia la economía de los datos

Las tecnologías de la información, los servicios de telecomunicaciones e Internet han habilitado al ciberespacio como un nuevo espacio de relación de escala y alcance global a lo largo de las dos últimas décadas. El ciberespacio crea nuevas dinámicas que afectan a los modelos de negocio con cobertura global, a las nuevas formas de relación entre personas o al acceso universal a la información, entre muchos otros. Son dinámicas que establecen realidades disruptivas que transforman los ámbitos sociales, económicos y políticos y que concurren con el mundo físico: la Sociedad de la Información, la Economía Digital, la Administración Electrónica, la Cultura Digital y la Identidad Digital. La transformación propicia modelos de negocios disruptivos que alcanzan todos los ámbitos económicos y sociales, en donde se desvanecen las barreras entre el mundo digital y el físico. Así, la Economía Digital ha desarrollado mercados a partir de nuevas formas de encuentro entre la demanda y la oferta en el ciberespacio (Uber, Netflix, Airbnb, WhatsApp, Spotify y Facebook).

Mientras tanto, una segunda transformación se inicia actualmente en torno a la economía de los datos, gracias a tecnologías como el Internet de las Cosas (IoT), los servicios entre maquinas (M2M) o el uso generalizado de la inteligencia artificial en el análisis de los datos que habilitarán una revolución en la producción industrial (Internet Industrial). Surgen complejos debates en torno a la ética del uso de los datos, la distinción entre lo público y lo privado, el papel de la transparencia en la confianza digital, así como nuevos retos de ciberseguridad.

Internet, el catalizador, es una red de redes que fue diseñada con unas características muy concretas (escalabilidad, simetría e inteligencia en los extremos) para su uso en entornos de confianza, no primando en su inicio la seguridad. En virtud de sus características, su uso se ha globalizado, pasando al ámbito público, con múltiples fines sociales y económicos. Esta revolución digital se puede ver hoy limitada por ciberamenazas cuyo objetivo son el ciberespacio y el mundo físico. La ciberseguridad tiene por objetivo securizar a individuos (identidad digital y privacidad), empresas (procesos, secretos comerciales y propiedad intelectual) y Estados (servicios esenciales ofrecidos por las infraestructuras críticas e información estratégica) en respuesta a la ciberdelincuencia y el ciberterrorismo. Para ello, los Estados y el sector privado cuentan con dos vías complementarias: la legislación (Directivas, Leyes y Regulaciones) y los procedimientos operativos que establecen objetivos, planes de actuación, prioridades y asignan recursos (Plan Estratégico de Ciberseguridad del Estado y marcos de colaboración público privada).

En la ciberseguridad intervienen múltiples agentes nacionales e internacionales del sector privado de las *tecnologías de la información y la comunicación –TIC–* (proveedores de *software*, suministradores de terminales y equipos, operadores de servicios de telecomunicaciones, proveedores de aplicaciones y servicios de Internet), del sector público (Administración, Fuerzas de Seguridad y Gobierno), de sectores transversales (Banca, Sanidad y Comercio) además de los propios usuarios de Internet. A ellos hay que añadir actores geopolíticos internacionales como EEUU, China, Rusia, Europa o América Latina que tratan de articular un modelo de Internet estructurado en grandes bloques de influencia donde prevalecen los elementos geopolíticos internacionales sobre los países individuales y las fronteras geográficas. Por consiguiente, es vital garantizar una óptima coordinación, un marco de colaboración público-privada y un modelo de gobernanza nacional en el plano legislativo y operativo.

Sin ser exhaustivos, los principales sujetos obligados por la legislación en materia de ciberseguridad son los proveedores de servicios de comunicaciones electrónicas y los proveedores de servicios esenciales, aumentando la presión regulatoria sobre los proveedores de aplicaciones de Internet. Sin embargo, la seguridad viene dada por el eslabón más débil de la cadena de valor que se establece entre el usuario final y el proveedor de Internet (terminal, operador de acceso fijo o móvil, proveedor de *cloud*, de *caching* y medio de pago *on-line*). Por consiguiente, cualquier nuevo requisito regulatorio que implique la adopción de prácticas de gestión de riesgo debería contemplar al conjunto de los agentes que intervienen en su prestación. En un futuro próximo y con antelación a la consolidación de la segunda ola de la transformación digital, será

necesario incorporar en la legislación la industria de *sofware* y *hardware*, haciendo especial énfasis en servicios M2M e IoT.

Los riesgos de la ciberseguridad

Los retos de seguridad más relevantes del ciberespacio tienen que ver con los incidentes, la confianza digital de los ciudadanos y empresas, la ciberdefensa y la seguridad nacional. Sólo en 2015 [1] el CERTSI, gestionó 50.000 incidentes de ciberseguridad que afectaron a ciudadanos, empresas y operadores estratégicos, un 18% más que en el año anterior. El CERT del Centro Criptográfico Nacional resolvió 21.000 incidentes en 2016,[2] el 15% más que en 2015 (18.232). De ellos, 756 casos (el 3,6%) en 2016 fueron clasificados muy graves o críticos frente a 430 (el 2,3%) en 2015. Los ciberataques a gran escala han demostrado tener capacidad para causar graves perjuicios económicos, tanto por la paralización de los sistemas de información y de comunicaciones como por la pérdida o alteración de información privada, financiera o estratégica que a menudo es crítica para el desempeño de los sectores público y privado. La evolución exponencial revela cómo el ciberespacio ofrece al crimen organizado, terroristas y delincuencia una plataforma de actuación privilegiada por encima de las fronteras nacionales y regionales. Es necesaria, por tanto, una respuesta coordinada en Europa entre las Instituciones de la Unión y los Estados, así como la cooperación internacional de todos los agentes.

La sustracción de datos de carácter personal, la suplantación de la identidad, el fraude, la extorsión, el acoso a través de la red, los delitos contra menores y los daños a terminales y equipos personales debilitan la confianza digital depositada por los individuos en la sociedad de la información. El reciente ataque mundial (*WannaCry ransomware*) ha elevado las alertas de las instituciones y de la opinión pública, erosionando notablemente la confianza digital: el 54% de los consumidores digitales se muestran desconfiados a utilizar sus datos de carácter personal en la red.[3] En este sentido, la transparencia de los proveedores de Internet juega un papel muy importante en la confianza y seguridad de los ciudadanos; no sólo en la comunicación de incidentes sino también en las comunicaciones y contratos de productos y servicios TIC (sistemas operativos, terminales y aplicaciones de Internet). Por ejemplo, el retraso en comunicar un incidente ha expuesto a millones de usuarios ante riesgos innecesarios. Por ejemplo, en diciembre de 2016 Yahoo[4] anunció que en agosto de 2013 había sufrido una brecha de seguridad que afectó a más de 1.000 millones de cuentas; unos meses antes, Yahoo confirmó el robo de 500 millones de cuentas en 2014. En mayo de 2016, cuatro años después que LinkedIn notificara que había sido atacada, aparecieron a la venta en *darkweb* 117 millones de cuentas de correo electrónicos y claves de acceso.

[1] Informe Anual de Seguridad Nacional 2015, p. 55, http://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2015.

[2] Informe Anual de Seguridad Nacional 2016, p. 60, http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/140217-Informe_Anual_de_Seguridad_Nacional_2016.pdf.

[3] *Accenture, Digital Trust in the IoT era*, 2015, https://www.accenture.com/us-en/insight-digital-trust.

[4] 2017 Bomgar Secure Access Report.

También juega un papel particularmente relevante la concienciación y formación de los ciudadanos en materia de ciberseguridad, para lo que son necesarios programas de concienciación preparados por la administración, proveedores de Internet y suministradores. En relación a la legislación en materia de ciberseguridad, se plantea un equilibrio entre los derechos individuales (por ejemplo, la privacidad de los ciudadanos o el secreto de las comunicaciones) y la efectividad del marco legal con que cuentan las fuerzas de seguridad. Este debate se intensifica porque la tecnología ofrece mayores capacidades de interceptación y aumenta la gravedad de las ciberamenazas. Aparecen así debates sobre la legitimidad de la interceptación masiva de las comunicaciones, las potenciales obligaciones de los fabricantes de terminales y operadores en descifrar las comunicaciones privadas, los límites temporales y el alcance de la retención masiva de datos, etc. La complejidad del tema se acentúa en Europa dado que la privacidad es un derecho fundamental de los ciudadanos de carácter irrenunciable, a diferencia de otras geografías (por ejemplo, en otras regiones es un derecho que ha estado vinculado a la protección del consumidor).

Los ciberataques causan importantes daños económicos y reputacionales a las empresas (espionaje industrial, robo de propiedad intelectual y pérdida de información) y las exponen a severas sanciones económicas. Por ello, enfocan su gestión de riesgo a hacia la prevención y hacia la resiliencia, segurizando las plataformas TIC y los procesos de producción. Para esto, incluyen la seguridad en el diseño de sus procesos, establecen planes de contingencia, implantan certificaciones o sensibilizan a sus empleados. También invierten en mecanismos de protección que mejoren la resiliencia de los sistemas y permitan en tiempo real la detección de vulnerabilidades de seguridad, supervisando el uso de la información, evitando filtraciones de información o bloqueando con rapidez y efectividad ciberataques. Unos mecanismos, entre otros, que no están al alcance de todas las PYME.

Las empresas diseñan sus políticas de ciberseguridad en función de las oportunidades y amenazas que pueden favorecer o perjudicar su competitividad. Desde la perspectiva corporativa, la gestión del riesgo adopta en ocasiones criterios que priorizan el impacto económico y reputacional en el negocio frente al impacto en la seguridad de terceros. Por otra parte, las empresas que ofrecen productos o servicios más seguros cuentan con una ventaja competitiva que es vital en determinados ámbitos como el de los mercados financieros. La regulación de las políticas empresariales es controvertida en la medida en que tienen elementos de diferenciación competitiva y de obligación reglada. En este sentido, la legislación debe limitar malas prácticas (por ejemplo, la demora injustificada en comunicar las brechas de seguridad) en base a principios y a la fijación de objetivos, sin por ello distorsionar la libertad de empresa en la gestión del riesgo.

Las políticas gubernamentales e intergubernamentales

Garantizar la seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los Gobiernos ante amenazas a la Seguridad Nacional. Cada vez preocupa más la posibilidad de ataques terroristas, de naturaleza política o de la criminalidad organizada contra sistemas de información que formen parte de las infraestructuras críticas de los Estados. Los ciberataques pueden contribuir a

desestabilizar un país, o poner en jaque sus instituciones y procesos democráticos, tal como han evidenciado los incidentes de ciberespionaje durante la última campaña electoral en EEUU que han provocado la psicosis y la adopción de medidas preventivas en las elecciones de los Países Bajos y Francia. Los ciberataques son también un componente fundamental de las amenazas híbridas: coordinados de modo preciso con amenazas físicas, por ejemplo, en relación con el terrorismo, pueden tener un impacto devastador. Dado que se es más dependiente de las tecnologías, redes y servicios de Internet, las infraestructuras y servicios esenciales pueden ser cada vez más vulnerables.

Los gobiernos han desarrollado estrategias, estructuras y planes de actuación para hacer frente a esos riesgos en el marco de sus competencias. En España, el Consejo de Seguridad Nacional aprobó en diciembre de 2013 la Estrategia de Ciberseguridad Nacional[5] concretada en seis objetivos, entre ellos, "garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques". Para su consecución se establecieron ocho líneas de acción y 45 medidas concretas. En octubre de 2014 el mismo Consejo aprobó el Plan Nacional de Ciberseguridad que identifica de manera más exhaustiva los riesgos y amenazas para el desarrollo de las líneas de acción.

En el campo militar se desarrolla en paralelo el concepto "ciberdefensa", donde el ciberespacio es el nuevo dominio de la defensa de los Estados (tierra, mar, aire, espacio y ciberespacio) en el que se planean, dirigen y ejecutan operaciones militares. Actualmente, cualquier acción bélica convencional se ve acompañada de acciones en el ciberespacio. En un futuro, el ciberespacio desempeñará un papel central y transversal en los conflictos bélicos. En este nuevo contexto, los Estados necesitan disponer de capacidades para proteger sus intereses en el ciberespacio y responder de manera oportuna, legítima y proporcionada ante un ciberataque. Se abre, por tanto, una nueva área de análisis, en la que se incluyen elementos de la ciberseguridad del ámbito civil (por ejemplo, la protección de servicios esenciales e infraestructuras críticas) y donde el reconocimiento de la soberanía de los Estados en el ciberespacio adquiere una importancia clave. En España el Mando Conjunto de Ciberdefensa (MCCD), órgano subordinado al Jefe de Estado Mayor, es responsable desde febrero de 2013 del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Para lo anterior, los gobiernos coordinan sus esfuerzos en el marco de instituciones multilaterales como la OTAN y la UE. En este campo, la OTAN publicó en agosto de 2013 un estudio de referencia sobre la aplicación de las leyes internacionales a conflictos entre Estados en el contexto de la ciberdefensa: el *Tallinn Manual on the International Law Applicable to Cyber Operations*,[6] actualizado en febrero de 2016

[5] http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad.

[6] https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

(cont.)

(*Tallinn Manual 2.0*).[7]. Asimismo, la Comisión Europea, ENISA y el Parlamento Europeo (*European Parliament's Science and Technology Options Assessment*, STOA) trabajan conjuntamente con la OTAN, la *Organisation for Security and Co-operation in Europe* (OSCE), la ONU e instituciones académicas en el marco del Plan Estratégico de Ciberseguridad de la CE iniciado en 2013 para establecer políticas comunes desde el punto de vista estratégico y operativo en materia de ciberseguridad y ciberdefensa: el *EU Common Security and Defence Policy* (CSDP).[8]

La legislación en el ámbito de la ciberseguridad: presente y tendencias

La legislación en el ámbito de la ciberseguridad tiene dos objetivos principales: (1) securizar el ciberespacio (sistemas de información y personas); y (2) proporcionar instrumentos jurídicos efectivos a las autoridades y fuerzas de seguridad para la investigación y persecución de la delincuencia y terrorismo. Toma como punto de partida regulaciones que es necesario adaptar con rapidez y efectividad a los nuevos retos del ciberespacio. Coincidiendo con el lanzamiento del Plan Estratégico de Ciberseguridad, la UE presentó la Directiva relativa a la criminalización de ataques contra los sistemas de información[9] (aprobada en agosto de 2013) y la Directiva sobre la Seguridad de las Redes y de la Información (Directiva NIS),[10] aprobada en julio de 2016. La Directiva NIS es el elemento central de la estrategia de ciberseguridad europea. Tiene por objeto garantizar un nivel armonizado mínimo de seguridad en las redes y sistemas de información utilizados por operadores de servicios esenciales y por proveedores de servicios digitales de Internet. Finalizada la transposición, será de aplicación en mayo de 2018. La Directiva pone a prueba la efectiva coordinación basada en la confianza entre Estados en materia de ciberseguridad, así como el modelo de gobernanza adoptado por cada Estado. Asimismo, plantea puntos abiertos tales como su engarce con la Directiva de Infraestructuras Críticas, el solape con las obligaciones de reporte y regímenes sancionadores de otras regulaciones y los mecanismos de supervisión ex-post de aplicación a proveedores de servicios digitales de Internet.

La gestión de la seguridad de los servicios de telecomunicaciones viene establecida en la Directiva Marco de Comunicaciones Electrónicas[11] que define los principios sobre seguridad e integridad de las redes y los servicios aplicables a éstos. La Directiva de Servicios de la Sociedad de la Información y de comercio electrónico [12] y la correspondiente Ley [13] regulan actualmente a proveedores de Internet tales como Google, Facebook y Amazon. La actual división en dos regímenes regulatorios provoca desequilibrios en la actuación regulatoria ante servicios ofrecidos por operadores de telecomunicaciones y proveedores de Internet que sean funcionalmente equivalentes

[7] https://ccdcoe.org/tallinn-manual.html.

[8] *Cybersecurity in the EU Common Security and Defence Policy* (CSDP), Challenges and risks for the EU, 16/V/2017, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2017)603175.

[9] Directiva 2013/40/UE relativa a la criminalización de ataques contra los sistemas de información, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0040&from=en.

[10] Directiva SRI, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[11] Articulo 13bis de la Directiva 2009/140/CE, 25/XI/2009.

[12] Directiva sobre el comercio electrónico 200/31/CE, 8/VI/2000.

[13] Ley de Servicios de la Sociedad de la Información y de comercio electrónico, 34/2002, 11/VII/2002.

(por ejemplo, el servicio telefónico y aplicaciones de voz en Internet), situación que también afecta al ámbito de la seguridad.

En el campo de la protección de la privacidad de personas físicas y jurídicas, la UE aprobó en diciembre de 2015 la Regulación General para la Protección de Datos de Carácter Personal (GDPR). Regula las condiciones y responsabilidades en el acceso, almacenamiento y tratamiento de los datos de carácter personal. Será de aplicación directa (sin transposición) en mayo de 2018, afectando a todos los sectores, incluyendo el público.

Asimismo, la Comisión presentó en enero de 2017 la propuesta de Regulación sectorial *e-Privacy Regulation*. Establece obligaciones adicionales a las fijadas por la GDPR a operadores de comunicaciones electrónicas (por ejemplo, a operadores de acceso a Internet) y a proveedores de Internet (Facebook, Google y Amazon), incluyendo los servicios de comunicaciones entre máquinas (M2M e IoT) para la protección de la privacidad de datos y metadatos. La propuesta *e-Privacy* ha sido muy cuestionada ya que se solapa a la GDPR, de aplicación también a operadores de telecomunicaciones y proveedores de Internet al ser ésta multisectorial. Esta superposición añade obligaciones y pone en desventaja competitiva a compañías europeas de telecomunicaciones, proveedores de Internet, *cloud*, *big-data* e IoT, entre otros; situación que puede ser contraproducente en la efectiva protección de los ciudadanos europeos.

Simultáneamente, varios Estados, entre ellos Alemania, España, Francia y el Reino Unido han revisado desde 2015 los instrumentos legales a disposición de las autoridades judiciales y fuerzas de seguridad en la lucha contra el crimen organizado y el terrorismo en la red, incorporando, entre otras medidas, nuevas y controvertidas obligaciones a los operadores para la interceptación individual y masiva de comunicaciones en redes de telefonía e Internet así como el registro remoto de equipos informáticos[14] (por ejemplo, ordenadores personales) y de dispositivos informáticos de almacenamiento (por ejemplo, servidores *cloud*).

Finalmente, es preciso subrayar el importante papel que desempeña la autorregulación y la transparencia de los agentes ante vulnerabilidades e incidentes ya que la percepción de seguridad afecta directamente la confianza depositada por los ciudadanos y empresas en los operadores, proveedores e instituciones. En contrapunto, la transparencia se ve limitada en ocasiones por la debilidad a la que se exponen los agentes ante la publicación de vulnerabilidades.

Tal como se ha indicado anteriormente, gran parte de la legislación europea sobre privacidad y comunicaciones electrónicas se encuentra en proceso de revisión o de implantación, al igual que la Directiva NIS. Pero es importante tener en cuenta que el marco regulatorio de comunicaciones electrónicas se encuentra actualmente en revisión

[14] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

(cont.)

(*European Electronic Communications Code*)[15] desapareciendo en un futuro la actual división regulatoria entre operadores de telecomunicaciones y proveedores de Internet. Esto facilitará enormemente, por ejemplo, la actuación de las fuerzas de seguridad y las autoridades judiciales en Internet.

La creciente gravedad de los ciberataques y atentados terroristas en Europa han impulsado desde mediados de 2016 nuevas acciones legislativas y operativas en el marco de la ciberseguridad, promovidas por la Comisión y lideradas por los Ministerios de Justicia e Interior del Consejo de Europa. Destacan la propuesta de Directiva e-Evidence sobre pruebas electrónicas que la Comisión presentará a mediados de 2017, la Directiva Antiterrorista aprobada en febrero 2017 y un análisis de situación sobre el cifrado, es decir, soluciones prácticas que permitan la relevación de comunicaciones y dispositivos cifrados, evitando la elaboración de legislación específica al efecto.

El Consejo solicita una mayor cooperación en las investigaciones criminales entre cuerpos de seguridad, cuerpos judiciales (LEA) y proveedores de servicios de comunicaciones electrónicas, especialmente a aquellos proveedores de Internet no establecidos en la UE. En particular, el Consejo requiere la colaboración técnica en el marco de la lucha antiterrorista para la monitorización de tráfico, bloqueo de contenidos, descifrado de comunicaciones e identificación de usuarios. Estas medidas vuelven a suscitar debate sobre los balances entre la seguridad Nacional y los derechos a la privacidad, la libertad de expresión o el secreto de las comunicaciones de los ciudadanos.

Conclusiones

La consolidación de las economías digitales sólo será posible si los servicios digitales ofrecen un alto nivel de confiabilidad, se asegura la privacidad de las personas y los Estados garantizan la prestación de los servicios esenciales frente a ciberamenazas.

Los planes estratégicos de ciberseguridad establecidos por la Comisión Europea y los Estados en 2013 se encuentran en fase de ejecución. Es necesario redoblar los esfuerzos en la adopción de medidas operativas para mejorar la concienciación, prevención, cooperación y transparencia.

Las Instituciones Europeas y los Estados trabajan en la revisión e implantación de marco legal para adecuarlo a las crecientes exigencias en materia de ciberseguridad en las áreas de los servicios esenciales (Directiva NIS), la privacidad (Regulaciones GDPR, e-Privacy) e instrumentos legales a disposición de las autoridades judiciales y fuerzas de seguridad en la lucha en la red contra el crimen organizado y el terrorismo.

Urge completar la implantación del marco legal y operativo e iniciar una evaluación de este primer ciclo. La nueva etapa de Internet que ahora se inicia en torno a la economía de los datos, las comunicaciones entre dispositivos (M2M e IoT) y el Internet Industrial causarán un salto cualitativo en materia de ciberseguridad.

[15] https://ec.europa.eu/digital-single-market/en/telecoms y https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-590-EN-F1-1.PDF.