foro de debate jurídico

Ciberdelitos
Amenazas criminales del ciberespacio

Moisés Barrio Andrés
Letrado del Consejo de Estado

REUS
EDITORIAL

PRÓLOGO

Internet se ha consolidado como pieza estructural de la Sociedad de la Información y desempeña un papel crucial en el desarrollo económico. La popularización de la Red a escala global ha permitido la creación del «ciberespacio virtual», tal y como lo concibiera el autor que acuñó tal término, William GIBSON[1], al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la última década del siglo XX, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales.

---

[1] El prefijo *cyber* proviene, a su vez, del término *cyberspace* creado por el novelista de ciencia ficción William GIBSON y su obra *Neuromancer* (Editorial AceBooks, Nueva York, 1984), en la que el autor describía una sociedad tecnológicamente avanzada donde las personas vivían en un mundo virtual separado del mundo real.

Algunos de los avances técnicos proporcionados por Internet podrían sintetizarse en la enorme facilidad y rapidez con la que se accede, copia, modifica y distribuye todo tipo de información, siempre a distancia y con posibilidad de ocultar la identidad real. Cada sujeto puede ser, a la vez, emisor y receptor de información, fortaleciendo así libertadas garantizadas constitucionalmente. Estas características han convertido a Internet en una herramienta insustituible para cualquier tipo de usuario[2]. En la actualidad, los sistemas informáticos resultan de extraordinaria importancia para organismos públicos, infraestructuras básicas, sanidad (en su vertiente de gestión y de investigación científica), particulares y, por supuesto, empresas. En este sentido, la integración de Internet en las actividades empresariales y el proceso de globalización que caracteriza la economía moderna han permitido

[2] La doctrina destaca, unánimemente, la afectación transversal de Internet. Vid., al respecto, entre otros: HILGENDORF, Eric; FRANK, Thomas y VALERIUS, Brian: *Computer- und Internetstrafrecht: Ein Grundriss*. Editorial Springer, Berlín, 2005; BARRIO ANDRÉS, Moisés: «Criminalidad e Internet: Retos del Siglo XXI», en *Sentencias de TSJ y AP y otros Tribunales*, Nº 15, 2003; MORALES PRATS, Fermín: «Internet: riesgos para la intimidad», en *Cuadernos de Derecho Judicial*, Nº 10, 2001, pág. 70; MATELLANES RODRÍGUEZ, Nuria: «Algunas notas sobre las formas de delincuencia informática en el Código Penal», en SÁNCHEZ LÓPEZ, Virginia (coord.): *Hacia un derecho penal sin fronteras*. Editorial Colex, Madrid, 2000, pág. 129; o MORÓN LERMA, Esther: *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*. Editorial Aranzadi, Pamplona, 1999.

nuevas formas de organización de la producción y de la comercialización. Tampoco debe desdeñarse su utilización como forma de diversión, con las redes sociales como forma de interactuación social.

Lo anterior conduce a que, en casi todos los ámbitos de la vida, se dependa, de forma muy intensa, de las Tecnologías de la Información y la Comunicación (en adelante, TIC)[3], que integran un concepto amplio, abierto y dinámico, que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual[4]. Y a medida que las redes de comunicación se hacen más convergentes y prestan

[3] Así, ROVIRA DEL CANTO advierte que sin las TIC las sociedades actuales se colapsarían, generándose lo que se conoce como la *computer dependency*: ROVIRA DEL CANTO, Enrique: *Delincuencia informática y fraudes informáticos*. Editorial Comares, Granada, 2002, pág. 9.

[4] En inglés el acrónimo utilizado es ICT, correspondiente a las siglas de «Information and Communications Technology». No existe una lista cerrada de elementos que configuran las TIC, sino que se incluyen en ella no sólo los que conforman los modos actuales de tratamiento y transmisión de la información, sino también los futuros. En todo caso, se engloban dentro de las TIC tanto las redes (entre las cuales destaca Internet pero también comprende las de telefonía móvil y otras redes telemáticas), como los equipos terminales (entre los que predominan los ordenadores personales, pero también comienzan a ser gran vehículo de comunicación las consolas o los *smartphones*) y los servicios, entre los que sobresalen la descarga de archivos –directa, mediante redes P2P o su visualización directa en *streaming*–, el comercio electrónico, la banca electrónica, la realización electró-

mayores servicios, aumenta, de forma pareja, su vulnerabilidad, de modo que ambos factores —dependencia y vulnerabilidad— se han ido incrementando progresivamente desde los años 90[5]. Por tanto, se trata de una tendencia que implica numerosas ventajas pero que también va acompañada de nuevos riesgos.

En general, los riesgos generados por Internet pueden reconducirse a dos grandes categorías. En primer lugar, las amenazas sobre bienes jurídicos tradicionales cuya peculiaridad deriva del empleo de las nuevas tecnologías. Así, por ejemplo, en la protección de la intimidad, los peligros derivados de la utilización de programas espía (*sniffers*), la monitorización digital (*cookies*, *spyware*), etc.; en el caso del patrimonio, de las técnicas de suplantación de identidad (*phishing*); en los supuestos de pornografía infantil, las nuevas formas de producción y distribución de material a través del uso de *webcams*, *smartphones*, plataformas P2P, etc.; y, por último, en la tutela de los derechos de propiedad intelectual, el especial impacto que ha tenido en los mismos la utilización de las plataformas P2P, etc. En segundo lugar, los riesgos que pesan sobre las propias infraestructuras electrónicas cuando son atacadas con el objetivo de alterar o impedir el normal funciona-

---

nica de actividades relacionadas con la Administración Pública y, cada vez más, las redes sociales.

[5] Vid. RODRÍGUEZ MOURULLO, Gonzalo; ALONSO GALLO, Jaime y LASCURAIN SÁNCHEZ, Juan Antonio: «Derecho Penal e Internet», en AA.VV.: *Régimen jurídico de Internet*. Editorial La Ley, Madrid, 2002, pág. 257.

miento de los sistemas de información. Estos incidentes suelen ejemplificarse en conductas como el acceso no autorizado, la difusión de programas informáticos perjudiciales —en sus múltiples modalidades de virus, bombas lógicas, caballos de troya o gusanos— y los ataques intencionados de denegación de servicio (*DoS*), que perturban los servicios ofrecidos por Internet y pueden causar daños a las entidades que cuentan con un portal propio desde el cual realizan operaciones con sus clientes y usuarios.

Habiéndose originado Internet en los Estados Unidos, fueron sus tribunales quienes primero van a enjuiciar los incipientes ciberdelitos y sus particulares consecuencias a principios de 1990. Así, en *United States v. Morris*[6], el acusado, un estudiante de ingeniería informática de la Universidad de Cornell, creó un virus diseñado para infectar Internet con el propósito de demostrar las insuficiencias de las medidas de seguridad en las redes electrónicas. Su programa informático funcionó increíblemente bien, y pese a los intentos del acusado de detener la propagación del virus, éste causó daños importantes a ordenadores de todo el país pertenecientes a instituciones académicas, militares y comerciales. Robert Morris fue condenado en primera instancia en virtud de la *Computer Fraud and Abuse Act* de 1986[7] (CFAA), condena que fue confirmada en apelación.

---

[6] 928 F.2d 504, 505 (2d Cir. 1991).

[7] 18 U.S.C. § 1030.

De este modo, en el momento presente asistimos a un momento álgido de la criminalidad en el ciberespacio, tanto en sentido cuantitativo dado el creciente uso de Internet en todo el mundo y por todo el mundo, como cualitativo al aparecer nuevas formas de delincuencia relacionadas con los nuevos servicios y usos surgidos en el ecosistema digital.

Así, como advierte MIRÓ LLINARES[8], la evolución del cibercrimen también conlleva una evolución en sus protagonistas esenciales, los criminales y las víctimas: del ya mítico *hacker* estereotipado en el adolescente introvertido y con problemas de sociabilidad, encerrado en su casa y convertido en el primer ciberespacio en un genio informático capaz de lograr la guerra entre dos superpotencias usando sólo su ordenador, hemos pasado a las mafias organizadas de cibercriminales que aprovechan este nuevo ámbito para aumentar sus actividades ilícitas y sus recursos. Y al no ser los cibercrímenes únicamente los realizados con ánimo económico, también varían los perfiles de cibercriminales que cometen delitos, que ya no son únicamente réplicas en el ciberespacio de los que ejecutarían en el espacio físico. Y lo mismo ocurre con las víctimas. Las personas jurídicas siguen siendo objeto de victimización debido tanto al uso generalizado de las TIC en ellas como a sus recursos económicos objeto de deseo por los cibercriminales.

---

[8] MIRÓ LLINARES, Fernando: *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Editorial Marcial Pons, Madrid, 2012, pág. 27 y ss.

No obstante, muchas suelen ocultar los ciberdelitos de los que son víctimas. La actitud poco favorable a la denuncia se debe al temor de que la trascendencia del hecho se traduzca en una suerte de descrédito de la fiabilidad de la gestión de la propia entidad (que, en este ámbito, se ciñe a una pérdida de confianza en sus sistemas de seguridad) y de su prestigio. De este modo, a fin de evitar mayores pérdidas, prefieren "resolver" el problema internamente.

Pero la aparición de los cibercrímenes *sociales* convierten a cualquier ciudadano que se relacione en Internet, que interactúe con otros, envíe mensajes, charle en foros o comparta sus fotos, en objeto de un posible ciberataque personal a su honor, intimidad, libertad sexual o similares bienes jurídicos. Y lo mismo sucede con otras instituciones supranacionales o estatales en relación con los cibercrímenes *políticos* o *ideológicos* cometidos con intención de desestabilizar un Estado o de difundir un determinado mensaje político aprovechando las posibilidades de comunicación masiva que ofrece el ciberespacio: la ciberguerra, el *hacktivismo* o el ciberterrorismo han convertido a las infraestructuras tecnológicas de Estados en objetivo prioritario de ataques de denegación de servicio (*DoS*), de infecciones de *malware* u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país.

En cualquier caso, las diversas manifestaciones de conductas delictivas vinculadas a las tecnologías cibernéticas, cuyo rasgo definitorio y diferenciador es el de realizarse en otro espacio distinto a aquél en

el que siempre se habían ejecutado las infracciones penales, han planteado importantes retos y desafíos jurídicos, frente a los cuales ya se han promulgado respuestas normativas, de ámbito estatal, comunitario e internacional. Ahora bien, la ciberdelincuencia conforma una delincuencia amplia, variada y cambiante, que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social. Y es ese ámbito y su carácter innovador y mutante lo que determina una problemática particular de la misma que va a ser objeto de atención en esta obra, brindando especial atención a las novedades y cambios introducidos por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Sólo mediante una comprensión global del fenómeno que identifique los caracteres comunes del evento criminal cometido en Internet podremos mejorar la prevención de «la delincuencia del siglo XXI».

Madrid-Londres, marzo de 2017.

Moisés Barrio Andrés
Letrado del Consejo de Estado
Doctor en Derecho
Abogado
moises@moisesbarrio.es

Introducción

Con la publicación de la obra de BECK[9] se identifica la nueva sociedad postindustrial de nuestro tiempo como una «sociedad del riesgo»[10]. El extraordinario avance de los medios tecnológicos y técnicos, en particular las TIC vinculadas a la informática e Internet, ha tenido y sigue teniendo repercusiones directas en un incremento del bienestar individual. Pero, a su vez, semejante progreso social conlleva un coste de signo negativo: el funcionamiento de esos medios técnicos es el factor originador de la presencia de una elevación, en número y entidad, de los

---

[9] BECK, Ulrich: *La sociedad del riesgo: hacia una nueva modernidad*. Editorial Planeta, Barcelona, 1998.

[10] Y se caracteriza, según el citado autor, porque: a) los riesgos no son limitables espacial, temporal y socialmente (en cuanto al ámbito de afectados); b) no son imputables según las vigentes reglas de la causalidad, culpabilidad y responsabilidad; y c) no pueden ser compensados ni asegurados. Cfr. BECK, Ulrich: *La sociedad del riesgo, op. cit.*, pág. 19 y ss.

factores de riesgo en nuestra sociedad; mayor nivel de riesgo que se mide no solo por la aparición de nuevos focos desencadenantes del mismo, sino también por la mayor capacidad de proyección de los futuros daños, sobre un colectivo de ciudadanos cada vez más grande. La presencia de todos estos riesgos, como coste aparejado indisolublemente a la evolución científica, ha determinado que éstos se constituyan en pieza estructural de la sociedad actual, como elemento que la define y la identifica.

Por su parte, Internet presenta una peculiaridad adicional. Dado su carácter descentralizado, no es posible que un organismo dirija y gestione la Red. Su funcionamiento es consecuencia del empleo, por una gran cantidad de operadores de sistemas informáticos y de redes de telecomunicaciones, de unos protocolos y arquitecturas comunes; esto es, de un mismo conjunto de convenciones relativas a la transmisión de datos e interoperabilidad de los sistemas.

Estos atributos propios de Internet originan dificultades de aplicación y adaptación de los ordenamientos jurídicos, siendo los más relevantes los que se citan a continuación: su estructura descentralizada, la deslocalización de los participantes, su aptitud como medio de publicación de alcance universal y, en fin, la internacionalidad inherente a las actividades en la Red. De este modo, el carácter transfronterizo y mundial propio de Internet exige un refuerzo de la cooperación internacional, así como la coordinación y compatibilidad de las normas estatales sobre las actividades desarrolladas en Internet, que es la base

necesaria para una sucesiva armonización de los ordenamientos nacionales. Esta es la senda jurídica a transitar, no exenta de complejidad, habida cuenta que el Derecho de Internet debe tener estructura en red y ser multipolar, mediante la participación de instancias internacionales, estatales y locales, así como de organizaciones privadas[11].

A la postre, la expansión de Internet ha provocado, a la vez, una aparición de un elenco de actividades nocivas para los ciudadanos, algunas de las cuales producen la lesión de bienes jurídicos relevantes protegidos por el Derecho Penal[12]. Por lo general, un número importante de estas actividades constituye una peculiar adaptación al espacio virtual de conductas lesivas más o menos clásicas desde la perspectiva penal, para cuya ejecución se aprovecha la viralidad y globalidad de este canal de comunicación (como ocurre, por ejemplo, con las estafas). Ahora bien, Internet

---

[11] MUÑOZ MACHADO, Santiago: *La regulación de la red. Poder y Derecho en Internet*. Editorial Taurus, Madrid, 2000, pág. 42.

[12] A los efectos del Derecho Penal, existen determinadas técnicas y modos de proceder cibernéticos constitutivos de ilícito penal (por ejemplo, acceso inconsentido a un sistema informático, interceptación ilícita de comunicaciones, interferencias en el sistema, prácticas de *phising*, ataques de denegación de servicio –*DoS*–, abuso de dispositivos, fraude informático, etc.) y también ciertos contenidos cuya vulneración se ve facilitada por el medio Internet (v. gr. delitos de pornografía infantil, contra la propiedad intelectual e industrial o revelación de datos personales).

ha convertido de igual forma una serie de conductas residuales en hechos delictivos masivos, como ocurre con la pornografía infantil, habiendo sacado a la luz una ingente demanda de este tipo de materiales.

También debe apuntarse cómo la intranquilidad generada por un avance tecnológico tan notable como es Internet y la influencia de una opinión pública, en ocasiones muy alarmada, han contribuido a que se haya generalizado una creciente sensación social de amenaza o de inseguridad en un momento de progreso y de primado indiscutible de las TIC, que, sin embargo, pueden ser utilizadas por delincuentes y, en esa medida, quedar al servicio de fines criminales[13].

El Derecho Penal y Procesal penal clásico, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de delincuencia física, marginal e individual. Sin embargo, la aparición de la informática primero y de Internet después ha resquebrajado este paradigma, al tiempo que los distintos organismos encargados de su represión se han ido enfrentando a un cauce de ejecución criminal capaz de cuestionar muchos de los principios tradicionales de la investigación penal[14].

---

[13] En este sentido, para un amplio análisis sobre la necesaria puesta en relación de dicha sensación social de inseguridad frente al delito con el modo de proceder de los medios de comunicación, vid. SILVA SÁNCHEZ, Jesús María: *La expansión del derecho penal*. Editorial Aranzadi, Navarra, 2001, pág. 37 y ss.

[14] Una visión general en CORCOY BIDASOLO, Mirentxu: «Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación cri-

ÍNDICE