El derecho penal frente a los riesgos de internet: el ciberdelito

Pilar Otero // Catedrática de Derecho Penal de la UC3M

Estamos inmersos en una vertiginosa sociedad tecnológica, que, por un lado, ha transformado radicalmente nuestra vida invadiendo casi todas las facetas de la actividad humana, y, por otro, lleva implícita una sociedad de riesgo. El lado oscuro de este desarrollo tecnológico tiene, así, entre otras, las siguientes manifestaciones:

1. Nuevas formas de criminalidad (*hacking* o acceso ilegal a un sistema de información; *phishing* o estafa informática; *child grooming* o ciberacoso a menores; *cracking* o daños informáticos; *denial of service* u obstaculización de un sistema de información).
2. La utilización de las redes informáticas para la comisión de los delitos tradicionales (fraudes, acoso, injurias, amenazas, espionaje industrial, pornografía infantil, etc.).
   Por tanto, podemos hablar de ciberdelito tanto en relación con aquellos delitos cuyo único medio de comisión es la red, esto es, el hacking o el sabotaje informático, como aquellos otros clásicos, que utilizan las redes telemáticas como instrumento.
3. Distribución del delito a una velocidad de vértigo y a un número ilimitado de usuarios (la marco-victimización generada, por ejemplo, por los virus informáticos).
4. Transnacionalidad de los delitos lo que dificulta su persecución, pues es consustancial a Internet la ausencia de fronteras.
5. Problemas de incriminación a las personas físicas o jurídicas que prestan servicios en la Red (los proveedores de servicios) por no haber retirado los contenidos delictivos.
6. Diferencias de lugar y tiempo entre la acción y el resultado del delito, lo que puede plantear problemas de participación en el delito y de prescripción.
7. Vulnerabilidad del sistema a medida que se va haciendo más complejo.

Todo ello podría resumirse en una idea: Internet favorece el anonimato. Aunque se intente paliar esta consecuencia al ser cada vez más sencilla la identificación de las direcciones IP, y pese a los rastros digitales del delito, lo cierto es que sigue siendo en la actualidad más compleja la identificación de los autores de estas conductas en el medio virtual que la de los sujetos que cometen infracciones similares en el mundo real. La percepción del anonimato implica inevitablemente la sensación de impunidad y, como consecuencia de ella, la reiteración del delito. El ciberespacio se convierte así en un paraíso para la criminalidad y en una plataforma para la criminalidad organizada.

Por otro lado, Internet es el vehículo por el que circula la mayor parte de dinero en el mundo, en consecuencia, la cibercriminalidad tiene principalmente una finalidad económica. Es decir, cualquier ciberdelito, aunque afecte de modo inmediato a otros bienes jurídicos, como la intimidad o la seguridad de los sistemas de información, lesiona finalmente el patrimonio. No se nos escapa, a este respecto, que el delito de pornografía infantil, que vulnera la indemnidad sexual de los menores, mueve en el mundo (teniendo en cuenta la cifra negra que envuelve a todo delito) la escalofriante cifra de 1.000 millones de euros mensuales.

¿Cómo se enfrenta el Derecho penal a estos desafíos? El Derecho, en general, va a remolque de las nuevas tecnologías de la comunicación y la información. En el ámbito que nos atañe, ha motivado dos importantes consecuencias:

En primer lugar, un Derecho penal desorientado, que se manifiesta fundamentalmente en el incremento de la técnica de los delitos de peligro abstracto, los cuales adelantan la barrera punitiva a momentos en los que todavía no se ha lesionado el bien jurídico, que además de provocar una grave inseguridad jurídica, genera un debilitamiento de las garantías penales. Así, se castiga con la misma pena al que fabrica o posee programas informáticos específicamente destinados a la comisión de un fraude en Internet que al que consuma la estafa informática.

Y, en segundo lugar, se ha visto obligado a evolucionar en lo que se refiere a su concepción de determinadas categorías penales para que puedan adaptarse a este nuevo escenario. Sirvan dos ejemplos al respecto. Primero, el concepto de *daño penal* en el mundo real se caracteriza por la permanencia y su tipificación se vincula a su valor económico. En cambio, en el mundo virtual, el *daño informático*, para que sea delito, el tipo penal exige que sea *grave*, conformándose esa *grave-*

dad no necesariamente por su valor económico (¿cuánto cuesta un USB: 5-10€?), sino por el valor funcional del dato contenido en ese determinado programa, esto es, asumiendo criterios tradicionalmente vinculados a la responsabilidad civil, como el coste de limpieza del sistema informático, si había o no copia de seguridad, la cantidad de información perdida, las horas de trabajo empleadas en la elaboración del documento, etc. La permanencia tampoco es necesariamente una característica del daño informático: en este sentido, el delito de *denial of service* (denegación de servicio), consiste en obstaculizar o interrumpir el funcionamiento de un sistema informático sin necesidad de destruirlo o dañarlo (por ejemplo, mediante un envío masivo de mensajes *spam* que saturan el sistema). El segundo ejemplo al que quería hacer referencia es la evolución del concepto de *intimidad* para que sea un bien jurídico protegible penalmente en el mundo virtual. La intimidad ha pasado de ser entendida como prohibición de interferencias externas, vinculada al secreto, a ser superada esta concepción por la recepción de la cultura anglosajona de la *privacy*, que permite que esta sea concebida como un derecho activo de control vinculado a la idea de autodeterminación del individuo. La *privacidad* es así el conjunto de facetas reservadas de la persona, que aisladamente carecen de significación, pero entrelazadas conforman un retrato digital de la personalidad del individuo. Sin embargo, en la medida en que el usuario deja rastros, huellas digitales, en la medida en que los proveedores de acceso a la red registran el tiempo y localización de las conexiones (archivos logs), en la medida en que no se borren las cookies (archivos emitidos por los webs servidores visitados y que se graban en el disco duro del internauta), es difícil mantener la privacidad en Internet, por lo que ante este nuevo panorama se redefine la intimidad como *derecho al anonimato*. Bien es cierto que este *derecho al anonimato*, por los motivos aducidos, no puede hacerse efectivo plenamente, por lo que en la actualidad se limita al *derecho al olvido*.

En definitiva, las peculiares características de las TIC no permiten siempre abordar la regulación de esta nueva realidad con los tipos penales tradicionales y, por tanto, exigen una respuesta nueva. Así, ocurrió, por ejemplo, con la modalidad estrella de los fraudes en Internet, el *phishing*, donde se emplea una manipulación informática para conseguir una transferencia no consentida de un activo patrimonial. Esta modalidad comisiva no encajaba en la estafa convencional cuyo papel rector es el engaño y, como consecuencia de él, se realiza un acto de disposición voluntaria por parte de la víctima. Nótese que, en el primero de los casos, el autor de la manipulación informática lo es también de la transferencia del dinero, sin que la víctima se dé cuenta de ello, asemejándose a un hurto telemático más que a una estafa. Por exigencias del principio de legalidad penal, ante la imposibilidad de subsumir estas conductas en el delito de estafa, hubo que introducir un tipo de equivalencia que sustituye el engaño por la *manipulación*.

> Las peculiares características de las TIC no permiten siempre abordar la regulación de esta nueva realidad con los tipos penales tradicionales y, por tanto, exigen una respuesta nueva

Por otro lado, y habida cuenta de que nos encontramos ante conductas transfronterizas, una respuesta eficiente del sistema requiere reforzar los mecanismos de cooperación internacional, armonizar las disposiciones penales y dotar de eficacia los instrumentos procesales, aunque pueda implicar en ciertos aspectos una cesión de soberanía por parte de los Estados. Esta es la finalidad principal que pretende la normativa supranacional al respecto, representada fundamentalmente por el Convenio del Consejo de Europa sobre *ciber-criminalidad* (Budapest, 23-11-2001), la Decisión Marco 2005/222/JAI del Consejo, relativa a *los ataques contra los sistemas de información* y la Directiva 2013/40/UE del Parlamento europeo y del Consejo, relativa a *los ataques contra los sistemas de información* por la que se sustituye la Decisión Marco anterior.

Por lo que respecta a la armonización de las disposiciones penales, en cumplimiento de la Decisión Marco de 2005, se incluyó por primera vez en nuestro Código penal en 2010 el delito de acceso ilegal a los sistemas de información *(hacking)* y el delito de interferencia ilegal en los sistemas de información (daños informáticos). Por su parte, la Directiva de 2013 fue transpuesta a nuestro Código penal en 2015, originando una ampliación del ámbito típico de las conductas anteriormente mencionadas e introduciendo otras nuevas, como el castigo de abuso de dispositivos creados para producir bien un sabotaje informático, bien un *hacking*; la responsabilidad penal de las personas jurídicas cuando cometen estos delitos; o agravaciones cuando estas conductas se realicen en el seno de una organización criminal, cuando los daños informáticos afecten a infraestructuras críticas o se cometan suplantando la identidad del legítimo propietario de los datos utilizados.

De nada sirve la armonización de las disposiciones penales si no se cuenta con eficaces instrumentos procesales para perseguir estas conductas. La propia naturaleza de estas –caracterizada por el uso de sofisticados procedimientos técnicos– determina una mayor complejidad en la instrucción y enjuiciamiento de los delitos, que necesita el uso de las propias TICs como herramienta de investigación, con el indudable apoyo de técnicos especializados (como el agente encubierto informático). La dificultad principal a que se enfrenta el investigador en este ámbito estriba en encontrar el equilibrio entre esa eficacia investigadora, salvando los obstáculos técnicos que rodean la comisión de estos delitos, y la estricta observancia de las garantías del investigado. Es decir, por un lado, la conformación de la prueba, la evidencia electrónica (constituida por la información generada, almacenada o transmitida mediante el uso de dispositivos electrónicos con capacidad para obtener la convicción judicial), suele ser volátil, fácilmente manipulable o destruible. Por otro lado, las garantías del investigado –que acompañan a todo procedimiento penal– deben extremarse en el ámbito de la investigación de la delincuencia tecnológica, cuyas diligencias afectan a derechos fundamentales, especialmente la intimidad o el secreto de las comunicaciones. Este contrapeso se intenta conseguir a partir de la Ley Orgánica 13/2015, *para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. Adicionalmente, no podemos obviar la doctrina del Tribunal de Justicia de la Unión Europea en este ámbito, la cual viene manteniendo que no puede establecerse con carácter preventivo una conservación generalizada e indiferenciada de los datos adicionales de los procesos de comunicación, y que solo la lucha contra la delincuencia grave que amenace la seguridad nacional puede justificar la conservación de estos por parte de los proveedores de acceso y de servicios, y sometida siempre a los principios de especialidad, idoneidad, excepcionalidad, necesidad, proporcionalidad de la medida limitativa, temporalidad y control judicial.

> La dificultad principal a que se enfrenta el investigador en este ámbito estriba en encontrar el equilibrio entre esa eficacia investigadora, salvando los obstáculos técnicos que rodean la comisión de estos delitos, y la estricta observancia de las garantías del investigado

Finalmente, por lo que se refiere a la competencia para iniciar la persecución de estos delitos, dado su carácter transnacional, debe incidirse en desarrollar una interpretación global común del principio de ubicuidad (conforme al cual el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, en consecuencia, el juez de cualquiera de ellas será, en principio, competente para la instrucción de la causa). Como complemento de lo anterior resulta esencial, por un lado, la coordinación y colaboración entre Estados para procurar una óptima determinación de esa competencia, que fije claramente los criterios de priorización en caso de conflicto y, por otro lado, reforzar los instrumentos de cooperación policial internacional (Europol, Interpol).

En conclusión, el Derecho penal avanza con paso firme, pero lento, para intentar contener el desenfrenado fenómeno del cibercrimen. Cuando ha conseguido ofrecer una solución a un problema nace otra nueva modalidad delictiva. En momentos de crisis, como la generada por la pandemia, han proliferado nuevos fraudes informáticos que utilizan la ingeniería social cada vez más sofisticada, lo que supone un continuo reto a afrontar por los actuales instrumentos jurídico-penales. ●

BIBLIOGRAFÍA

- LEZERTÚA RODRÍGUEZ, Manuel, "El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa", en *Curso Internet y Derecho Penal*, Madrid: Consejo General del Poder Judicial. Servicio de formación continua, Escuela Judicial, 2001.
- LÓPEZ ORTEGA, Juan José, "Libertad de expresión y responsabilidad por los contenidos en la Red", en *Curso Internet y Derecho Penal*, Madrid: Consejo General del Poder Judicial. Servicio de formación continua, Escuela Judicial, 2001.
- MIRÓ LLINARES, Fernando, *El cibercrimen fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons, 2012.
- "Cibercrímenes económicos y patrimoniales", en *Memento práctico penal económico y de la empresa*, Madrid: Francis Lefebvre, 2016-2017.