CAPÍTULO SEGUNDO

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS

ESTRATEGIAS LEGALES FRENTE A LAS CIBERAMENAZAS*

JOSÉ L. GONZÁLEZ CUSSAC

**El presente trabajo se inserta en el marco del Proyecto de investigación «Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y la comunicación» (Ministerio de Ciencia e Innovación, referencia DER2008-05707).*

RESUMEN

Estrategias legales frente a las ciberamenazas

En el contexto socio-económico global actual, el desarrollo del ciberespacio ha facilitado enormemente el auge de toda clase de interacciones comerciales, sociales, gubernamentales y delictivas. Lo cual ha tenido como consecuencia que la seguridad del ciberespacio haya crecido en importancia, desde el momento en que las ciberamenazas han pasado a formar parte esencial de las nuevas agendas de seguridad nacional y defensa. Así, los países han dedicado parte de sus esfuerzos, en los últimos años, a desarrollar una estrategia legal que pueda ser efectiva para seguir el rastro de las ciberamenazas y contraatacarlas, y, al mismo tiempo, sea respetuosa con los derechos y libertades fundamentales.

Precisamente en ese ámbito se enmarca este trabajo, que encuentra su principal objetivo en el intento de ofrecer un panorama descriptivo de la evolución de las diferentes respuestas legales dadas a las ciberamenazas. En particular, el trabajo analiza sucintamente las medidas penales adoptadas para hacer frente a los cibercrímenes. Y concluye aportando algunas consideraciones críticas sobre la aproximación realizada hasta el momento a este tema.

Palabras clave: Ciberamenazas, Ciberseguridad, Cibercrimen, Medidas legales, Jurisdicción, Derecho Internacional, Internet, Globalización.

ABSTRACT

«Legal Strategies against Cyber Threats»

In the world's current global socio-economic context, the rise of cyberspace has greatly facilitated all kinds of commercial, social governmental and criminal interaction. As a result, the security of cyberspace has grown in importance, from the moment that cyber threats have become an essential part of the new agendas for national security and defense. So the countries have devoted part of its efforts, in recent years, to develop a legal strategy that can be effective to track and counteract cyber threats, but still mindful of fundamental rights.

Precisely, that is why the principal mission of this research, will be to study the development of the different legal responses into the cyber threats. Particularly, the research provides a brief analysis of the criminal measures adopted against the cybercrimes. It also concludes offering some critical considerations of this issue.

Keywords: Cyber threats, Cybersecurity, Cybercrime, Law Enforcements, Jurisdiction, International Law, Internet, Globalization.

EL PUNTO DE PARTIDA. LA EXPANSIÓN DEL CONCEPTO DE SEGURIDAD NACIONAL: *CIBERDELITOS Y CIBERAMENAZAS*

La expansión del concepto de seguridad nacional

Para poder comprender la función del Derecho –en particular del derecho penal– frente a las nuevas amenazas, y en concreto frente a las llamadas *ciberamenzas*, resulta preciso destacar algunos parámetros que están experimentando una profunda y constante transformación.

Comenzaré por la mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno propio de seguridad nacional. Si bien es cierto, que éste no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. De aquí el usual manejo

del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales (1).

Es precisamente en este contexto donde se manifiesta nítidamente la necesaria reconstrucción del concepto de seguridad nacional, para, de una parte, que resulte eficaz como criterio central de gestión de las nuevas amenazas y necesidades estratégicas actuales, y de otra, cohonestarla con nuestra forma de organizarnos políticamente: el Estado democrático y de Derecho.

Pues bien, en el transcurso de este proceso, parece claro que la categoría de seguridad nacional se construye ya hoy desde una perspectiva multidimensional: militar, política, económica, social (identitaria), y medioambiental. Es decir, como equivalente a exención de peligro, daño o riesgo en todos estos ámbitos, y por tanto entendida como seguridad colectiva, compartida y global.

Como es conocido, esta necesaria adaptación conceptual de la seguridad nacional se debe a múltiples factores: cambios en el sistema internacional; avances en la tecnología de la información, comunicación y transporte; aparición de amenazas post-guerra fría; reactivación de conflictos étnico-religiosos; estallido de crisis económico-financiera; resurgimiento de la competitividad geopolítica; mantenimiento o rebrote de conflictos locales; aparición de nuevos actores no estatales; facilidad con que grupos no estatales se organicen para atacar Estados utilizando nuevas tecnologías; etc.

Así pues, creo que resulta innecesario insistir en aspectos obvios acerca de los grandes cambios sufridos, y en curso, del mundo actual. Pero sí referirme, muy sucintamente –pues también constituyen ya lugares comunes en la literatura especializada–, a los presupuestos básicos desde los que arrancan estas reflexiones. En concreto, deseo partir de la nueva consideración que las instituciones y organismos competentes en materia de seguridad proyectan ahora sobre algunos fenómenos que tradicionalmente preocupaban en otras áreas sociales, y algunos casi exclusivamente en la esfera de la administración de justicia (derecho penal).

Para ilustrar esta tendencia, basta con citar, a título de ejemplo, entre otros muchos posibles, el documento la Estrategia Europea de Seguri-

(1) GONZÁLEZ CUSSAC, J. L.: «*Nuevas amenazas a la seguridad nacional: el desafío del nuevo terrorismo*», en «Retos de la política criminal actual», Revista Galega de Seguridade Pública (REGASP)«, nº 9, Xunta de Galicia, 2007, p. 233 a 252

dad, de diciembre de 2003 y el Informe del Parlamento Europeo sobre su aplicación (2009/2198/INI). En el primer texto se indica que «*la unión de diferentes riesgos y amenazas, como son el terrorismo empeñado en ejercer la máxima violencia, la disponibilidad de armas de destrucción masiva, la delincuencia organizada, el debilitamiento del sistema estatal y la privatización de la fuerza, constituyen una amenaza muy radical*» (2).

Como se observa, viejos fenómenos de delincuencia común, en particular terrorismo y criminalidad organizada, han pasado de ser considerados como simples «riesgos» a la seguridad nacional, hasta alcanzar la máxima categoría de «amenaza». Así pues, se encuentran al mismo nivel que los eventuales ataques de fuerzas armadas de países hostiles. Todos los documentos nacionales o internacionales sobre estrategia y seguridad así lo confirman. Por consiguiente, estos fenómenos, especialmente terrorismo y crimen organizado, ya no se abordan como una cuestión meramente criminal, sino que se afrontan también desde otras perspectivas, y desde luego comportan otras muchas proyecciones que la vieja delincuencia raramente tuvo. Todo ello conlleva muchos cambios y sobre todo abre numerosos interrogantes.

Un ejemplo es suficiente para subrayar la incidencia de estas novedosas proyecciones del terrorismo y del crimen organizado sobre las agendas de seguridad nacional: la globalización, la *deslocalización,* la ausencia de fronteras y las dificultades para identificar al atacante y capturarlo. Esta es sin duda una de las cuestiones claves a resolver por los sistemas legales en la actualidad: ¿cómo hacer frente jurídicamente a un delincuente del que no se conoce exactamente ni su identidad ni su ubicación espacial? Es evidente que las estrategias de la disuasión ya no son suficientes, ni en el terreno militar ni tampoco aparentemente en el jurídico.

Entonces, la primera consideración básica sería la siguiente: aunque hasta ahora las fuerzas armadas protagonizaban la defensa de nuestra seguridad nacional, en la actualidad, ante la diversificación de las amenazas, ya no son el aparato estatal exclusivo encargado para garantizar

(2) Ver ARTEAGA: «La estrategia europea de seguridad: cinco años después», ARI nº 15/2009, Real Instituto Elcano, 22/01/2009; Informe del Parlamento Europeo de 2 de marzo de 2010 www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2010-0026+0+DOC+XML+V0//ES, y, SHULMAN: «Medidas del Consejo de Europa para luchar contra la cibercriminalidad», en ENAC, nº 2, agosto 2009, pág. 31.

nuestra supervivencia (3). Pero a la vez, en paralelo, tampoco parece hoy posible convenir que la administración de justicia sea una herramienta suficiente para resolver los conflictos atinentes a crimen organizado y terrorismo. La premisa puede formularse con otras palabras: si en realidad lo que está en peligro es nuestro sistema de convivencia, nuestra seguridad nacional, en este marco el Derecho, la administración de justicia, y en particular el derecho penal, tampoco resulta ser el instrumento idóneo, suficiente o único para enfrentarse a estas amenazas.

En resumen, hoy parece una evidencia comúnmente aceptada que nos hallamos ante un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los Estados. Pero su control igualmente hace peligrar los valores del Estado de Derecho, especialmente la de los derechos fundamentales. Expresado en otros términos, la amenaza real de estas formas de criminalidad provocan una demanda apropiada de la respuesta estatal y con ello también se realimenta el viejo debate entre seguridad y libertad.

Nuevos escenarios, nuevas amenazas, nuevas respuestas

El desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. Hoy en día se ha encaminado el control de muchos procesos mundiales a través del ciberespacio. Por lo que no hay duda de que actualmente el ciberespacio constituye un bien valioso. Y de que la seguridad del ciberespacio ha crecido en importancia (4).

En efecto, porque si combinamos estas reflexiones con el fenómeno de las *ciberamenazas*, constatamos como la criminalidad organizada en general y el terrorismo en particular, están generalizando el uso de las nuevas tecnologías de la información y la comunicación como instrumen-

(3) BALLESTEROS MARTÍN, M. A.: «*El papel de las fuerzas armadas en la lucha contra el terrorismo internacional*», en Real Instituto Elcano de Estudios Internacionales y Estratégicos, 18/08/2006.

(4) YAR: «Cybercrime and society», London 2006.

to para desarrollar su actuación delictiva. Sin embargo, la novedad de esta circunstancia no es tanto el uso delictivo de las mismas, sino que su empleo sofisticado y masivo en un escenario global, hasta el momento no ha encontrado una respuesta adecuada y satisfactoria ni en el sistema legal ni en el de la cooperación de las diferentes agencias de seguridad.

Sin duda alguna, durante el control de Al Qaeda en Afganistán, se desarrolló una auténtica academia de ciberterrorismo con el objetivo de buscar formas de atacar las infraestructuras occidentales en el ciberespacio. Aunque no hay que dejar de recordar que parte de la complejidad en este análisis, surge del hecho de que los diferentes Estados experimentan las ciberamenazas de manera diferente, lo cual hace que resulte una asimetría en la preocupación acerca de las mismas.

Las posibilidades de globalización e internacionalización que tales tecnologías ofrecen, junto con las indudables ventajas que supone el llevar a cabo actuaciones que pueden producir sus efectos incluso en otro continente, convierte a estas categorías criminógenas en aún más peligrosas y efectivas de lo que hasta el momento venían siéndolo, y en cierta manera generan un clima de miedo, inseguridad e impunidad, unas veces real y otras distorsionado. Tales circunstancias obligan a desarrollar un análisis detenido de los ordenamientos jurídicos nacionales y de la normativa internacional, a efectos de determinar las carencias de las que adolecen, y así posibilitar un debate serio y riguroso de reformas jurídicas tendentes a aumentar la eficacia de la respuesta jurídica, que suplan las deficiencias actuales (5).

Probablemente, si hubiera que escoger una característica que definiera al siglo XXI, ésta sería, sin duda alguna, la globalización. En efecto, la disolución de las fronteras, el establecimiento de espacios comunes, cada vez de mayor amplitud, no sólo en el aspecto económico y social, sino también en el político y en el jurídico, están posibilitando espacios de actuación en continuo incremento. Como es sabido, esta realidad también provoca efectos negativos, y en nuestra temática se plasma en la generación de un idéntico proceso de internacionalización y expansión de la criminalidad.

Como se ha destacado sobradamente, en este contexto, las grandes amenazas que en el presente se ciernen sobre la seguridad pública y

(5) ROMEO CASABONA (coord.): «*El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas políticocriminales*», Granada 2006.

la seguridad nacional vienen determinadas por la criminalidad organizada y por el terrorismo. Dejando al margen las estrategias de naturaleza militar, tradicionalmente más propias de enfrentamientos armados entre Estados, en su condición de sujetos activos de Derecho internacional, la consideración de estos fenómenos como conductas delictivas, tanto en convenios internacionales como a nivel nacional, genera el que los métodos de prevención y represión en relación a ambos –particularmente complejo es el caso del terrorismo–, hayan de revestir una respuesta combinada y coordinada de la administración de justicia y de las fuerzas armadas (6). No obstante, en estas líneas el enfoque dominante es el análisis de las estrategias legales, esto es, de carácter jurídico y no tanto militar. A reforzar las mismas debiera dirigirse la labor de los poderes públicos y también de la literatura científica, posibilitando una auténtica cultura de seguridad nacional, en la que junto a la defensa de nuestra supervivencia física (*lo que somos),* se articulara la defensa de nuestros valores democráticos *(como somos)* (7).

Si a dicha profesionalización, internacionalización y globalización de la criminalidad acabada de referir, añadimos la consolidación del uso de las tecnologías de la información y la comunicación (TIC), obtenemos los ejes esenciales que configuran la realidad sobre la que gira este trabajo. En este sentido, en sí mismas las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero tampoco deben minusvalorarse las facilidades que el uso de las nuevas tecnologías ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo: el activismo, el hacktivismo y el terrorismo informático son algunos ejemplos claros de esta tendencia.

Quizás por este doble sentido de las TIC, como valor intrínseco y como instrumentos comisivos, la literatura jurídica ya comenzó a diferenciar, en la década de los ochenta, entre la criminalidad informática, consistente en la realización de determinados delitos que sólo pueden materializarse a través de mecanismos informáticos o sobre los mismos programas y sistemas informáticos; y la criminalidad clásica relacionada con la informática, relativa a las figuras delictivas tradicionalmente con-

(6) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

(7) FERNÁNDEZ RODRÍGUEZ y SANSÓ-RUBERT PASCUAL (editores): «Internet: un nuevo horizonte para la seguridad y la defensa» (Seminario de Estudios de Seguridad y Defensa de la USC-CESEDEN). Universidad de Santiago de Compostela 2010.

tenidas en los textos punitivos en los que la presencia de estas tecnologías no es sustancial a las mismas, sino instrumental (8).

Ciberdelitos y ciberamenazas

Como hipótesis, podría decirse que cibercrimen y ciberamenazas no son categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la seguridad nacional, ni todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos mencionados, determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

Para mostrar la diferente escala de gravedad que pueden revestir estas conductas, me valdré de algunos ejemplos. Con ello quiero significar que la respuesta debe distinguir igualmente la magnitud de la agresión, y no solo para ser proporcional, sino también para ser eficaz.

El actual concepto de *ciberespacio*, «como conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios», nos ofrece un primer criterio para discernir las diferentes entidades de las posibles agresiones y por consiguiente, de las necesidades de regulación jurídica. Hasta fechas recientes, la *ciberseguridad* respondía a la exigencia de tutelar la información (*Information Security)*, lo que determinaba un enfoque legislativo destinado a sancionar los accesos, usos, revelaciones, o daños ilícitos no autorizados. Sin embargo, en la actualidad, la evolución conduce hacia la gestión de riesgos del ciberespacio (*Information Assurance)*, en la que los riesgos para la seguridad se encuentran vinculados al uso, procesamiento, almacenamiento y transmisión de información o datos, y los sistemas y procesos utilizados. Hoy la *ciberseguridad* requiere de ambos enfoques, diferentes pero complementarios (9).

La importancia de la seguridad en el ciberespacio ha llevado a los principales países a desarrollar estrategias, planes y legislación tendente a prevenir y sancionar conductas delictivas, pero también a neutralizar ciberataques a su seguridad nacional –se habla de un hipotético «ci-

(8) FREUND, W., *Die Strafbarkeit von Internetdelikten*, Wien, 1998; GÜNTER, R., *Computer criminalität*, bhv, 1998

(9) FOJÓN CHAMORRO Y SANZ VILLALBA: «Ciberseguridad en España: una propuesta para su gestión», ARI 101/2010, Real Instituto Elcano 18/06/2010.

ber-11S» o de un «ciber-Katrina»– (10). Es más, en múltiples círculos se formulan listados de Estados hostiles en este ámbito. Así, por ejemplo, según la organización privada «Reporteros Sin Fronteras», en un informe de marzo de 2009, se identifica a los 12 «enemigos de Internet»: Irán, China, Cuba, Egipto, Corea del Norte, Siria, Túnez, Arabia Saudí, Vietnam, Myanmar, Turkmenistán y Uzbekistán.

Pues bien, determinados los objetos de tutela, procede identificar las amenazas a los mismos, que en todo caso son muy heterogéneas y presentan una naturaleza de alta innovación. Parece existir cierto acuerdo en clasificarlas, en consideración a su autoría e impacto, en las cuatro siguientes categorías:

A) Ataques perpetrados o patrocinados por Estados. Sería la traslación al ámbito virtual de los conflictos reales entre países. Los ataques a infraestructuras críticas o clasificadas o la denominada ciberguerra, constituyen buenos ejemplos.

B) Ataques cometidos por grupos terroristas o por cualquier otra manifestación de extremismos políticos, ideológicos o religiosos. Planificación de acciones y su ejecución, sabotajes, apología, captación o reclutamiento serían las principales conductas a considerar (11).

C) Los ataques de la delincuencia organizada. El anonimato y las fronteras nacionales ofrecen una alta rentabilidad para su uso en fraudes económicos a gran escala o explotaciones de redes de pornografía infantil.

D) Por último, se identifican los ataques de perfil bajo. Su naturaleza es muy heterogénea, incluyendo desde intromisiones en la intimidad hasta pequeños fraudes.

   Resulta fácil concluir que, dada la generalización del uso de las TIC, los ataques e intensidad de los mismos, son tan dispares que llegan incluso a difuminar los bienes a proteger. A título orientativo pueden citarse las siguientes modalidades de ataque: abusos en el acceso a correos e internet; accesos no autorizados; *bots* o redes de equipos infectados remotamente; captura de contraseñas; extorsiones debidas a informaciones; diversas clases de daños y sabotajes (v gr desfiguración de páginas web); múltiples varieda-

---

(10) Por ejemplo, consultar LEWIS, J.: «Security Cyberspace in the 44th Presidency», Report 2008; o Doctrina militar rusa y seguridad en la información: www.belt.es/expertos/HOME2_experto.asp?id=4999.

(11) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

des de fraudes; *phishing*, consistente en el uso de redes sociales para adquirir de los usuarios información personal; denegación de servicio; infección por *malware* o uso de programas de códigos hostiles; *exploit*, consistente en la utilización de piezas, fragmentos o secuencias de datos o comandos para aprovechar fallos del sistema para lograr comportamientos no deseados en los programas; explotación de servidores y navegadores; hurtos y robos de ordenadores o dispositivos móviles; etc.(12).

E) Pero en todo caso, si hasta fechas muy recientes las empresas privadas eran las que lideraban los avances en ciberseguridad, ahora son los gobiernos los que han comenzado a protagonizar una enorme inversión en proteger el ciberespacio. Por eso mismo, son también muchos los Estados que ya consideran al mismo un activo de su seguridad nacional

Ciertamente en una primera fase los ataques en el ciberespacio fueron protagonizados por jóvenes que mostraban su destreza informática; pero después se profesionalizaron y comercializaron estas prácticas ilegales al descubrirse su rentabilidad, facilidad comisiva y considerable impunidad. En una tercera fase, su generalización ha despertado, como acabamos de señalar, el interés de los Estados ante la grave amenaza que suponen, a la vez que posibilitan nuevas formas de defensa y ataque. Algunas hipótesis ilustran perfectamente esta evolución: los posibles ataques a los sistemas que manejan las infraestructuras públicas, como los servicios de telecomunicaciones, de agua, luz, y gas, o los de transporte. En ocasiones el problema de su protección se complica al estar estos servicios prestados por empresas privadas.

También se afirma, en una reciente publicación (13), que el Pentágono sufre diariamente 5.000 ciberataques. Esta cifra puede resultar orientativa del volumen e intensidad del problema.

Y por otra parte, según fuentes gubernamentales norteamericanas, las pérdidas por fraude de datos y piratería en 2008, ascendieron a una cifra estimada de 720.000 millones de euros. Este dato es significativo del volumen económico del cibercrimen (14).

---

(12) PANSIERA, F. J., y JEZ, E., «La criminalité sur l'internet», Puf, 2000; PICCOTI, L., (Coord.), «Il diritto penale dell´informatica nell´epoca di internet», Padova, 2004.

(13) *Quadrennial Defense Review*, número de febrero de 2010

(14) Enlace web cybersecurity FBI www.fbi.gov/cyberinvest/cyberhome.htm

Un resumen de los incidentes más graves conocidos en los últimos años puede sernos de utilidad para tratar de comprender exactamente la dimensión del problema (15).

Abril-Junio 2007

- Una serie de ciberataques a agencias y departamentos del gobierno de los Estados Unidos acabaron con el robo de entre 10 y 20 terabytes de información. Entre las principales víctimas se encontraba el Secretario de Defensa, Robert Gates, cuya cuenta de correo electrónico no clasificada fue penetrada.

Mayo 2007

- El Parlamento, los Bancos, Ministerios y medios de comunicación de Estonia se enfrentaron a ataques distribuidos de denegación de servicio (denominados en inglés, DDoS – *Distributed Denial of Service*–). Son ataques a un sistema de computadoras *o de red*, que causan que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conexión a la red. En los ataques DDoS, los sitios web son inundados con un tráfico tal, que origina su colapso.

Octubre 2007

- Se envió un correo electrónico a 1000 miembros de la plantilla del *Oak Ridge National Labs*, del Departamento de Energía, de los USA, con un adjunto (attach) que contenía el acceso a las bases de datos no clasificadas de los Laboratorios.

Agosto 2008

- *Hackers* lograron introducir fotos de Hitler en la página oficial del Ministerio de Asuntos Exteriores de Georgia, al tiempo que otras páginas oficiales sufrían ataques distribuidos de denegación de servicio (DDoS). Algunos analistas norteamericanos concluyeron que el gobierno ruso estaba detrás de los ataques, y probablemente había actuado a través de los canales del crimen organizado.

(15) Center for Strategic and International Studies Technology and Public Policy Program. CSIS. Washington D.C. USA.

Agosto-Octubre 2008

- *Hackers* lograron el acceso a los correos electrónicos y archivos de los ordenadores de los cuarteles generales de Barack Obama y de John McCain, durante la campaña para las elecciones presidenciales.

Noviembre-Diciembre 2008

- Algunos miles de ordenadores militares en Tampa, en los cuarteles generales para operaciones militares entre el este de África y Asia central, son infectados con *software* dañino. Los investigadores concluyeron que el programa maligno fue introducido mediante *pen-drives* que habían sido dejados en una plaza de aparcamiento.

Marzo 2009

- Investigadores de la Universidad de Toronto anunciaron que habían descubierto una amplia red de ciberespionaje, que denominaron «GhostNet.». Los operadores de esta red infectaron 1.295 ordenadores principales en 103 países, de todo el mundo. Aunque no se ha podido determinar el origen de los operadores, diversos analistas apuntan a China.

Julio 2009

- Diversos ciberataques son lanzados contra las páginas web de los gobiernos, instituciones financieras y medios de Corea del Sur y los USA. Entre los objetivos estaba la página web del Washington Post (washingtonpost.com). Corea del Sur culpa a Corea del Norte de los ataques, pero la autoría no ha podido ser determinada todavía.

Diciembre 2009

- Google, y más de otras 30 empresas norteamericanas, instaladas en China, sufrieron ataques informáticos que ocasionaron, a muchas de ellas, la pérdida de secretos tecnológicos.

Con todo, hay que reconocer que los ciberataques están llegando a ser cada vez más sofisticados y, por tanto, más difíciles de rastrear. Se asegura que los *hackers* en China, por ejemplo, son ahora mismo capaces de tomar el control simultáneamente de miles de ordenadores per-

sonales en los USA, y, por control remoto, ordenarles el envío de correos electrónicos falsos o virus.

Hasta el día de hoy, la mayoría de los ataques informáticos se han recogido bajo la denominación de la categoría de «Cibercrimen». Ciertamente, todavía no ha habido actos realmente significativos de ciberterrorismo en los USA ni en ningún otro país, según los informes oficiales (16). Lo que se atribuye al hecho que *al Qaida* y otros grupos terroristas están todavía desarrollando sus ciber capacidades. Ahora bien, el desarrollo de las mismas en estos últimos años, sobre todo desde 2008, está siendo tan importante, que se prevé que en menos de 10 años esos grupos terroristas puedan estar ya plenamente preparados para lanzar sus principales atentados en el ciberespacio (17). En realidad, como acabamos de comprobar al exponer los casos más significativos, los ataques de referencia cometidos contra gobiernos extranjeros y corporaciones empresariales han sido, en gran medida, con fines de espionaje y fraude.

En resumen, mientras parece existir acuerdo en que Internet ha tenido un gran impacto sobre la criminalidad, en lo que no parece existir tanto consenso es en determinar sobre qué delitos en concreto ha recaído dicho impacto. Muchos autores afirman que prevalecen los cibercrímenes –esto es, los llevados a cabo a través de ordenadores en la red–, pero no hay, hoy por hoy, una definición común de lo que es cibercrimen ni, por ende, de los delitos que exactamente abarca (18).

No obstante, con carácter general, el concepto de cibercrimen abarca un conjunto de actividades ilícitas asociadas con el uso de TIC, especialmente en Internet. Actividades que pueden ir desde el fraude financiero hasta la entrada no autorizada a sitios web, e incidir en ámbitos como el espionaje industrial, la pornografía o los juegos de azar, entre otros. Así, entre algunos de los ciberdelitos más comunes se encuentran: el acceso ilegal a sistemas ajenos, la intercepción ilegal, la interferencia y pérdida de datos, la interferencia de sistemas, la pornografía infantil, los delitos

(16) TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007.

(17) CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010.

(18) WALL, D. S.: «The Internet as a Conduit for Criminal Activity», INFORMATION TECHNOLOGY AND THE CRIMINAL JUSTICE SYSTEM, Pattavina, A., ed. Sage Publications, Inc., 2005, pp. 77-98.

contra la propiedad intelectual, y el fraude electrónico. Sin embargo, por diversas insuficiencias en materia de legislación, su persecución tiene ciertas limitaciones. Todavía más confusa resulta la brecha existente entre los cientos de miles de incidentes ilegales estimados y el relativamente escaso número de procesos penales abiertos (19).

En el contexto descrito, algunos autores se plantean si los cibercrímenes son realmente una nueva categoría de delitos necesitada de una nueva teoría y clasificación, o si no estamos ante unos delitos que, sin necesidad de nuevas clasificaciones ni teorías, pueden ser entendidos desde las categorías delictivas clásicas ya existentes (20). Incluso los que van más allá, se plantean que la sensación de inseguridad en la red y de la alarmante existencia de cibercrímenes no es sino producto de recursos de información creados artificialmente por la propia industria de ciberseguridad que, sin duda, tiene interés en la dramatización de los cibercrímenes; esto es, en la creación de una sensación subjetiva de inseguridad y alarma en la red.

LAS RESPUESTAS DEL SISTEMA LEGAL

Pues bien, en todo caso, ambos fenómenos –*ciberdelitos y ciberamenazas*–, separada o conjuntamente, constituyen una de las mayores preocupaciones a nivel internacional y nacional, en el campo de la legislación penal. Esta creciente preocupación se manifiesta en el elevado número de convenios, acuerdos y reformas que en relación a los mismos pueden encontrarse. Sin embargo, lo que despierta un mayor interés radica precisamente en el uso de la informática como instrumento específico para la comisión de tipos delictivos y su creciente potencialidad de daño. De ahí que quizás, en primer lugar, trazaré a modo telegráfico un marco del estado de la cuestión a nivel mundial, para después pasar al ámbito europeo y terminar con el modelo español.

Grandes líneas de la situación a escala mundial

La diferente evolución económica y tecnológica se corresponde generalmente con similar grado de desarrollo normativo. De aquí la gran diferencia entre países en esta materia.

(19) WALL, *ob.* y *loc cit.*

(20) Por todos, ver ORTS BERENGUER, E., y ROIG TORRES, M., «*Delitos informáticos y delitos comunes cometidos a través de la informática*», Valencia, 2001.

En el área de África del Norte (Magreb), el bajo índice de utilización de internet, comporta una escasa preocupación estatal por el problema y consecuentemente un prácticamente inexistente marco normativo. Muy parecida es la situación en el África Subsahariana.

El lado opuesto lo encarna la zona de América del Norte, donde los gobiernos califican esta materia como atinente a la seguridad nacional y el desarrollo comercial de las nuevas tecnologías encuentra su nivel más alto (técnicas de biometría, tarjetas inteligentes, redes privadas virtuales, criptografía, redes inalámbricas WLAN, etc.).

En América Latina, en términos generales, la preocupación por la ciberseguridad sigue siendo en la actualidad secundaria. Comienzan paulatinamente a incorporarse los procedimientos internacionales de seguridad de la información, aunque existen todavía importantes vacíos jurídicos, como por ejemplo en relación al cifrado.

La ausencia de un marco legislativo sobre seguridad en las redes en la mayoría de países de Asia, permite de una parte el libre juego de empresas y consumidores, y de otra, una creciente intervención de los Gobiernos, que se proyecta sobre la gestión de los contenidos, la identificación, el filtrado y los sistemas de criptografía.

La característica más determinante de Oriente Medio es la explotación de las telecomunicaciones en régimen de monopolio por operadores nacionales. No se han desarrollado hasta el momento normativas importantes sobre seguridad de la información.

Del escenario europeo me ocupo a continuación con un mayor detenimiento.

Convenio del Consejo de Europa, sobre cibercriminalidad

Ha de hacerse una mención especial al Convenio del Consejo de Europa, sobre cibercriminalidad, firmado en Budapest el 23 de noviembre de 2001, el cual ha sido ratificado por España el pasado 3 de junio, y en vigor desde el 1 de octubre de 2010.

Tiene como propósito el lograr una mayor cooperación entre los Estados, así como el desarrollo de una legislación armonizada y apropiada para contener, en la mayor medida posible, este tipo de delincuencia. Se articula en cuatro capítulos, además del Preámbulo: el primero dedicado a definiciones; el segundo a disposiciones de derecho penal sustantivo

y procesal; el tercero a cooperación internacional; y el cuarto a las cláusulas finales (21).

En lo que respecta a los comportamientos, que necesariamente han de ser configurados como ilícitos penales en las correspondientes legislaciones internas, se estructuran en las siguientes categorías.

A) Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos (Tít. 1). En este grupo se deben describir como infracciones penales las siguientes conductas: a) acceso ilícito doloso y sin autorización a sistemas informáticos (art. 2); b) la interceptación dolosa e ilícita, sin autorización, a través de medios técnicos, de datos informáticos, en el destino, origen o en el interior de un sistema informático (art. 3); c) los atentados contra la integridad de los datos, consistente en dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos (art. 4); d) los atentados contra la integridad del sistema, esto es, la obstaculización grave, dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (art. 5); e) el abuso de equipos e instrumentos técnicos, que comporta la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de dispositivos principalmente concebidos o adaptados para cometer las infracciones antes referidas; la de una palabra de paso (contraseña), de un código de acceso o de datos similares que permitan acceder a un sistema informático; y la posesión de alguno de los elementos antes descritos (art. 6)(22).

B) Infracciones informáticas (Tít. 2). Entre ellas, según este Convenio, deben sancionarse penalmente los siguientes comportamientos: a) las falsedades informáticas, que contienen la introducción, alteración, borrado o supresión dolosa y sin autorización, de datos informáticos, generando datos no auténticos (art. 7); b) estafa in-

(21) Por todos, ver, DE LA CUESTA ARZAMENDI y DE LA MATA BARRANCO (directores): «Derecho penal informático», Madrid 2010; GONZÁLEZ RUS: «Los ilícitos en la red (I): *hackers, crackers, cyberpunks, sniffers*, denegación de servicio y otros comportamientos semejantes», en «El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales», Granada 2006; FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Oviedo 2007.

(22) GALÁN MUÑOZ: «Ataques contra sistemas informáticos», *Boletín Información Ministerio de Justicia*, 2006; GÓMEZ NAVAJAS: *La protección de datos personales*, Madrid 2005.

formática, que precisa la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos, o de cualquier otra forma de atentado al funcionamiento de un sistema informático, siempre con la intención fraudulenta de obtener un beneficio económico (art. 8) (23).

C) Infracciones relativas al contenido. Sin embargo, dentro de este apartado únicamente se describen conductas relativas a pornografía infantil (art. 9).

D) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines (art. 10) (24).

El Convenio también contiene disposiciones técnicas respecto a la sanción de la complicidad, la tentativa (art. 11), la responsabilidad de las personas jurídicas (art. 12) y las sanciones y medidas a imponer (art. 13).

En síntesis, desde la perspectiva penal sustantiva, se trata del primer instrumento normativo en el ámbito europeo, lo que de por si supone un paso decisivo hacia la armonización de las legislaciones en esta materia. Ahora bien, no debe confundirse armonización con unificación, pero en cualquier caso constituye el presupuesto necesario para la cooperación internacional y para avanzar hacia una mayor integración legal. En este sentido, como toda norma internacional, establece los mínimos comunes que los Estados miembros están obligados a incorporar a sus ordenamientos, pero desde luego no fija los máximos de intervención punitiva. En otro orden de consideraciones, aunque el texto se refiere a comportamientos cometidos en el ciberespacio, algunos de ellos no dejan de ser estructuras típicas tradicionales, que bien por el medio comisivo empleado (nuevas tecnologías) o bien por la mayor gravedad de su uso, se incluyen dentro de esta categoría.

En cuanto a las disposiciones de naturaleza procesal, en lo referente al ámbito de aplicación, se faculta a los Estados para que instauren procedimientos o procesos específicos para la investigación de los ilícitos penales antes descritos; o de cualquier otro delito cometido a través de un sistema informático, o para la recogida de pruebas electrónicas (art. 14). Igualmente advierte que los Estados velarán para que se respeten las garantías y derechos individuales proclamados en

(23) GALÁN MUÑOZ, A., «*El fraude y la estafa mediante sistemas informáticos*», Valencia, 2005.

(24) MIRÓ LINARES: «Internet y delitos contra la propiedad intelectual», Madrid 2005.

la normativa interna de cada Estado y especialmente en la normativa internacional (art. 15).

Relevante es la obligación de los Estados de disciplinar la conservación inmediata de datos (art. 16), así como la de conservación y divulgación inmediata de los datos de tráfico (art. 17). De igual modo deben adoptar medidas tendentes a la identificación o mandato de comunicación (art. 18), al registro y decomiso de datos informáticos almacenados (art. 19), a la recogida en tiempo real de datos informáticos (art. 20) y a la interceptación de datos relativos al contenido (art. 21).

De gran interés la regulación de la competencia, que insta a los Estados para que se atribuyan jurisdicción respecto a cualquier infracción penal contenida entre los arts. 2 a 11 del presente Convenio, cuando la misma se haya cometido en su territorio, a bordo de una nave que ondee pabellón del Estado; a bordo de una aeronave inmatriculada en ese Estado, o por uno de sus súbditos (art. 22). En este sentido, advertir que el Convenio mantiene el principio de la territorialidad como criterio de atribución de competencia, y no introduce reglas de ampliación o extensión de la jurisdicción.

En lo relativo a la cooperación internacional, junto a los principios generales (art. 23), se estipulan las reglas de extradición (art. 24), y un conjunto de medidas de colaboración y asistencia (arts. 25 a 35). Todo ello supone un significativo avance para la persecución e investigación de estos ilícitos.

Recordar asimismo el Protocolo Adicional sobre incriminación de actos de naturaleza racista y xenófoba, cometidos a través de sistemas informáticos, aprobado por el Consejo de Europa el 30 de enero de 2003. Con este Protocolo, anclado en la protección de los derechos fundamentales, se corrige una importante laguna del Convenio, persiguiéndose la armonización en este sensible ámbito.

Otros instrumentos normativos de la Unión Europea

También en el ámbito de la UE se han desarrollado numerosos instrumentos para la regulación de las nuevas tecnologías y su afectación a los derechos individuales, como por ejemplo ya iniciaron 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; luego seguidas de una abundante normativa.

Más recientemente, debe destacarse la Directiva 2000/31/CE del Parlamento y del Consejo Europeo, de 8 de junio, con la finalidad de armonizar los ordenamientos europeos en materia de servicios de la sociedad de la información. La misma se conoce como «comercio electrónico», y parte de la idea de crear un espacio europeo sin barreras en la comunicación e información. Sin embargo, ya advierte de la necesidad de intervención penal frente a determinadas conductas que pueden afectar a cuatro grandes áreas necesitadas de tutela: menores, dignidad humana, consumidores y salud pública.

En esta tendencia se inscribe 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. Aquí se fijan una serie de obligaciones de confidencialidad y regulación de la conservación de datos, prohibiendo la escucha, grabación, almacenamiento u otras clases de intervención o vigilancia de las comunicaciones. Sin embargo, debe subrayarse la introducción de excepciones a estas prohibiciones cuando se vea afectada la seguridad nacional (art. 15). La reciente Directiva 2006/24/CE, sobre conservación de tráfico de las comunicaciones electrónicas consagra esta orientación, tendente a garantizar la identificación del origen, destino, fecha, hora y duración de comunicaciones, el tipo de comunicación, el equipo utilizado y la localización del mismo, por razones de seguridad nacional.

Otro hito significativo en este camino de lucha contra la cibercriminalidad, lo representa la Directiva 2000/375/JAI, destinada a la adopción de medidas, fundamentalmente de actuación policial, para la persecución de conductas de pornografía infantil.

A destacar también 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 (DO L 149 de 2.6.2001); la más reciente 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 (DO L 13/44 de 20.01.2004), en la que se hace referencia a la regulación de estos delitos cuando son cometidos a través de Internet. Y finalmente, 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

(DO L 69 de 16.3.2005), por la que se establece la obligación de los Estados miembros de configurar como infracciones penales el acceso ilícito a un sistema de información, el perjuicio a la integridad de un sistema o la intromisión ilegal en los datos. Todas las cuales contienen indicaciones relativas a la realización de tales conductas a través de sistemas de comunicación.

Criminalidad organizada y terrorismo

La criminalidad organizada ha sido a su vez, objeto de una importante labor internacional. Así, debe hacerse referencia en primer lugar a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000, mediante la Resolución A/RES/55/25, la cual tiene como objetivo, precisamente, lograr una mayor cooperación internacional en la lucha contra este tipo de delincuencia. O la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo (DO L 309 de 25.11.2005) (25).

La misma afirmación cabe hacer respecto del terrorismo, en relación al cual puede hablarse además de los respectivos Convenios firmados en el seno de la ONU, del Convenio del Consejo de Europa sobre prevención del terrorismo, firmado en Varsovia, el 16 de mayo de 2005, del cual también es parte nuestro país –aunque no ha sido ratificado–. Como es sabido, la estrategia que se ha venido estableciendo para combatir al terrorismo ha consistido en el incremento de la cooperación y del intercambio de la información, estableciéndose medidas concretas en relación a específicos aspectos relacionados con las mismas, tales como la facilitación de los procesos de entrega de los detenidos por estos delitos, mediante la Decisión Marco 2002/584/JAI del Consejo de 13 de junio de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, transpuesta a nuestro ordenamiento mediante la Ley 3/2003 de 14 de marzo, sobre la orden europea de detención y entrega (BOE núm. 65, de 17 de marzo de 2003).

(25) VVAA: GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZ, A., coord: *Financiación del terrorismo, blanqueo de capitales y secreto bancario. Un análisis crítico,* Valencia, 2009; FERRÉ OLIVÉ, J.C., y ANARTE BORRALLO, E., *Delincuencia organizada. Aspectos penales, procesales y criminológicos*, Universidad de Huelva, Huelva, 1999.

O la afectación de los recursos económicos de las organizaciones terroristas mediante la aprobación del Convenio Internacional para la represión de la financiación del terrorismo de 1999 de Naciones Unidas; la Resolución del Consejo de Seguridad de Naciones Unidas 1373, de 28 de septiembre de 2001; la Recomendación del Consejo de la Unión Europea, de 9 de diciembre de 1999, relativa a la Cooperación en la lucha contra la financiación de grupos terroristas; la Decisión marco del Consejo de 13 de junio de 2002, sobre la lucha contra el terrorismo o la Declaración de la Unión Europea sobre la lucha contra el terrorismo, de 25 de marzo de 2004 (26).

Como se aprecia, abundante es la normativa que a nivel internacional puede encontrarse sobre cada uno de los aspectos a los que se ha hecho referencia. Los ejemplos acabados de reseñar ponen de manifiesto sin embargo, dos tendencias que revisten, a nuestro modo de ver, una relevancia considerable. En primer lugar, que las actuaciones previstas versan sobre aspectos específicos que pueden ser individualizados en cada una de las categorías criminógenas referidas. En segundo lugar, que mediante el tratamiento individualizado de cada una de esos aspectos, se están comenzando a establecer instrumentos aplicables conjuntamente a las mismas. Sin duda, porque en la realidad cotidiana de las mismas, los vínculos de unión entre ellas son constantes e innegables.

Derecho penal español

Por lo que se refiere a España, el terrorismo, la criminalidad organizada y determinados delitos relacionados con las nuevas tecnologías encuentran respuesta en nuestro ordenamiento jurídico mediante su previsión, principalmente, en el Código Penal. En este sentido ya el Código Penal de 1995 supuso un avance de gran calado en estas materias, y la reforma del mismo de 2010, que entrará en vigor a partir del próximo 23 de diciembre de 2010, incorpora diversos instrumentos internacionales referidos a las nuevas tecnologías.

Igualmente hay que destacar el avanzado tratamiento que la literatura científica española ha venido realizando de estos fenómenos delictivos, conformando una consolidada y abundante doctrina al respecto. Lo mis-

(26) GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZ, A.: «*Sobre el concepto jurídico-penal de terrorismo*», en «El Estado de Derecho frente a la amenaza del nuevo terrorismo», en «Teoría y Derecho. Revista de pensamiento jurídico «(Tirant), nº 3, junio 2008, págs. 34 a 58.

mo cabe decir de nuestra jurisprudencia, con un abundante cuerpo de resoluciones en la materia. A este amplio acerbo jurídico me remito y aquí únicamente me detendré en exponer esquemáticamente los principales ejes del sistema legal español (27).

Comenzaré por reseñar la importante modificación del Código Penal de 2010 en materia de «organizaciones y grupos criminales» (Cap. VI del Tít. XXII). En primer lugar, se contiene una novedosa regulación de los delitos cometidos en el seno de organizaciones o en grupos, en el que se distinguen ambos niveles de concierto de personas para cometer delitos. Aquí, además del castigo agravado por la comisión de concretas infracciones, se castiga como figura autónoma la pertenencia a las mismas (arts. 570 bis; ter; y quáter). Además de la sanción correspondiente por la comisión de los delitos comúnmente vinculados al crimen organizado, el modelo español contempla penas agravadas precisamente cuando éstos se realizan en el seno de las mismas. A tales efectos resulta igualmente relevante la definición que de la delincuencia organizada se contiene en el art. 282 bis de la LECrim.

A continuación, el Capítulo VII se refiere a las «organizaciones y grupos terroristas y a los delitos de terrorismo» (arts. 571 a 580), en el que se encuentra una detallada y completa –en relación a la normativa internacional y Derecho comparado– tipificación de estos ilícitos. Así, junto a la definición de organización y grupo terrorista, se sancionan, entre otras, las conductas de pertenencia y colaboración a las mismas (art. 571); la comisión de concretos delitos graves por personas que pertenecen, actúan a su servicio o colaboran (art. 572); el depósito y tenencia de armas, municiones y explosivos (art. 573); realización de infracciones menos graves por personas que pertenezcan, actúen a su servicio o colabores con organizaciones o grupos terroristas (art. 574); comisión de delitos contra el patrimonio para allegar fondos (art. 575); actos de colaboración, vigilancia e información (art. 576); actos de financiación (art. 576 bis); los que sin pertenecer colaborasen con las finalidades terroristas (art. 577); apología del terrorismo (art. 578); actos preparatorios (art. 579); y, reincidencia internacional (art. 580).

El escenario difiere sin embargo en lo que a las nuevas tecnologías se refiere. Al igual que ocurre por ejemplo en Italia o en Alemania, nuestro

(27) Con carácter general puede verse VIVES ANTÓN; ORTS BERENGUER; CARBONELL MATEU; GONZÁLEZ CUSSAC; MARTÍNEZ-BUJÁN PÉREZ. «Derecho Penal. Parte especial», 3ª ed. Valencia 2010.

legislador no ha optado por desarrollar un tratamiento conjunto y unitario de las conductas tipificadas penalmente, sino que por el contrario, dada la heterogeneidad de supuestos, se ha optado por ir ubicando en los distintos Títulos, Capítulos y Secciones que configuran el Código Penal, los ilícitos que pueden encontrarse relacionados con ellos. En efecto, también en materia de delitos vinculados a las nuevas tecnologías, el texto punitivo español mantiene el criterio sistematizador del bien jurídico tutelado (intimidad, patrimonio, etc.).

También en este ámbito deben subrayarse importantes modificaciones operadas por la reforma penal de 2010. En todo caso, expondré a continuación las principales figuras delictivas vinculadas con las nuevas tecnologías:

– concertación de encuentros con menores de trece años, a través de internet, teléfono o cualquier otra tecnología de la información o la comunicación, con la finalidad de atentar contra su indemnidad sexual (art. 183 bis);
– prostitución y corrupción de menores (art. 189);
– acceso ilícito a datos o programas informáticos (art. 197,3º);
– descubrimiento, revelación y cesión de secretos por personas encargadas o responsables de los soportes, ficheros informáticos, electrónicos o telemáticos (art. 197,5º);
– robo con fuerza: descubrimiento de claves para acceder a lugar cerrado y concepto de «llaves falsas» extendido a instrumentos tecnológicos de apertura y cierre (arts. 238 y 239);
– estafa informática: manipulación informática para lograr transmisión patrimonial no consentida; fabricación, introducción, posesión y facilitación de programas informáticos específicamente destinados a la comisión de estafas; utilización abusiva de tarjetas de crédito o débito, cheques de viaje o datos allí contenidos (art. 248,2º);
– defraudaciones de fluido eléctrico y análogos (art. 255);
– daños informáticos: borrado, alteración, supresión o hacer inaccesible datos, programas informáticos o documentos electrónicos; obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264); daños a medios o recursos de las Fuerzas Armadas (art. 265);
– propiedad intelectual (arts. 270 y 271);
– propiedad industrial (arts. 273 a 277);
– descubrimiento, revelación y difusión de secretos de empresa (arts. 278 y 279);

– la fabricación o tenencia de programas de ordenador específicamente destinados a cometer delitos de falsedades (art. 400);
– infidelidad en la custodia de documentos y violación de secretos por autoridad o funcionario público (arts. 413 y ss.);
– desórdenes públicos: obstaculizar o destruir líneas o instalaciones de telecomunicaciones (art. 560,1º);
– descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (arts. 598 y ss.).

Aunque con ciertas imprecisiones técnicas y algún aspecto discutible, parece convenirse que nuestro ordenamiento penal contiene una adecuada regulación en la materia y un al nivel de incorporación de la normativa europea e internacional.

UN BALANCE DEL DEBATE JURÍDICO ACTUAL

Categorías Generales

La combinación de varios factores ya enunciados en el primer apartado, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas. A efectos meramente expositivos, éstas las podemos agrupar y enumerar como sigue:

A) En el ámbito del Derecho Constitucional, las nuevas tecnologías obligan a una profunda consideración de los siguientes aspectos: a) derecho fundamental a la intimidad (18.1 CE); b) derecho fundamental a la inviolabilidad del domicilio (18.2 CE); c) derecho fundamental al secreto de las comunicaciones (18.3 CE); d) derecho a la no intromisión en el entorno digital (18.4 CE); e) *Habeas data*; f) libertad de expresión e información (art. 20 CE).
Algún ejemplo puede servir para expresar esta preocupación. En principio, se suele aceptar que internet, como red de redes sobre la que no gobierna nadie, no conoce fronteras. Pero en algunos de los regímenes autoritarios más poderosos si se están tejiendo límites muy estrictos. Es el caso de China e Irán, que han invertido sustanciosas cantidades en TIC para controlar radicalmente la libertad de expresión en sus conexiones a la red, interceptando «webs» para capturar disidentes políticos, que luego son detenidos. En la actualidad ya no se conforman con cerrar páginas o censurar resultados en motores de búsqueda, sino que son capaces de espiar al internauta a través de sus proveedores de co-

nexión: leen sus correos electrónicos o *blogs* restringidos y controlan al detalle qué páginas visitan. El empleo de esta tecnología lesiona gravemente el derecho fundamental a la intimidad.

En efecto, pues internet funciona como una red de puertos conectados a sistemas autónomos, pequeñas redes que se unen en una gran red de redes no gobernada por nadie. Cada proveedor de una de esas redes se compromete a facilitar, en principio, que cada puerto, desde su dirección IP, comparta información –correos electrónicos, intercambio de archivos, visitas a páginas *web*– con otros puertos, en cualquiera de las demás redes autónomas. Pero cuando es un Estado, o cualquier corporación, quien controla esos puertos, puede interferir absolutamente en la navegación de sus usuarios: prohibiendo la comunicación entre dos o más puertos; desconectando a internautas; espiando o censurando los paquetes que transmiten la información en la red. Los conocidos conflictos de Yahoo (2004) y Google (2009) con el gobierno de China expresan suficientemente este grave problema. Pero idéntica pretensión han manifestado recientemente Arabia Saudí, Emiratos Árabes, Líbano, Argelia e India. Ahora solicitan el acceso al sofisticado sistema codificado de la telefonía móvil de Blackberry; este último país alegando que fue utilizado para preparar y ejecutar los recientes atentados de Bombay. Probablemente la siguiente empresa en ser requerida será Skype.

Pero esta capacidad técnica para controlar la información en la red, despertó la preocupación en gobiernos de Estados de Derecho, ante el posible abuso por parte de las grandes corporaciones. El ejemplo más evidente lo encontramos en los proveedores de internet de los Estados Unidos, que bajo la justificación de combatir lo que consideran *piratería*, emplean estas técnicas. Así sucedió en 2008 con *Comcast*, proveedora de banda ancha por cable, que según La Comisión Federal de Comunicaciones, estaba interfiriendo selectivamente sobre ciertas conexiones de programas P2P.

Lo mismo puede suceder cuando las agencias de seguridad apelan a la defensa de la seguridad nacional. Esta posibilidad obliga a una regulación legal precisa que impida prácticas arbitrarias, garantizando el derecho a la intimidad de los ciudadanos. Pues obvio es, que no solo los regímenes autoritarios están interesados en el control de las comunicaciones. La censura del blog de la embajadora del Líbano en Londres, el pasado verano, por elogiar al fallecido ayatolá Mohamed Hussein Fadlallah, considerado

mentor de Hizbulá y calificado de terrorista, es un buen ejemplo de esta tendencia. Ello obliga a la búsqueda de un equilibrio entre las libertades civiles y la seguridad nacional, que afecta por igual a Gobiernos y empresas tecnológicas.

En este contexto tampoco puede dejar de citarse la viva controversia por las revelaciones de documentos clasificados por el sitio web WikiLeaks, en torno a actuaciones de las fuerzas armadas norteamericanas durante los conflictos de Irak y Afganistán.

B) Por su parte, las nuevas tecnologías también obligan a que en el seno del Derecho Penal se proceda a una mayor precisión en la tipificación y proporcionalidad de la sanción de los siguientes comportamientos: a) delitos contra la intimidad: acceso ilícito; interceptación ilícita; descubrimiento de secretos e interceptación de comunicaciones; descubrimiento de secreto informático; b) crimen organizado y delincuencia profesional: fraudes informáticos; blanqueo de capitales; c) ciberterrorismo; d) atentados contra la integridad de datos e integridad del sistema (daños); e) fraudes informáticos: falsedad informática y estafa informática; f) responsabilidad de las personas jurídicas; g) pornografía infantil.

Así, no son pocos los problemas que en relación a la delincuencia informática pueden ponerse de manifiesto. Especialmente desde que el uso de Internet no sólo se ha generalizado, sino que se ha estandarizado. Las amenazas que la misma puede implicar para la intimidad o para el propio patrimonio, junto con el alto grado de evolución que tales técnicas experimentan, hacen que la actualización y análisis de las mismas deban ser constantes.

Dado que con las comunicaciones telemáticas las fronteras se tornan inexistentes y los espacios pierden su materialidad, a nivel jurídico pueden encontrarse multitud de problemas relativos a la determinación del lugar de comisión de los delitos, el momento en el que pueden considerarse cometidos, el esclarecimiento de la jurisdicción competente, así como la determinación de los sujetos a los que cabe atribuir responsabilidad por la comisión de los mismos.

A estos efectos, evidente resulta la controversia relativa a los *service-providers*. Pero los problemas que surgen en esta materia no lo son únicamente a efectos procesales, sino que también en materia de Derecho penal sustantivo pueden encontrarse aspectos problemáticos. Principalmente, la plasmación en un texto punitivo

de las conductas que a través de estos medios pueden llevarse a cabo, en particular sobre el derecho a la intimidad, dada la especial relación entre usuarios y servidores (28). Pero no sólo eso. Al igual que existen conductas que pueden ser cometidas mediante las nuevas tecnologías, respecto de las que nadie pone en duda su carácter delictivo, también puede aludirse a todo un conjunto de comportamientos que no sólo no se encuentran configurados como tales en la actualidad, sino que en determinadas ocasiones pueden ser reconocidos incluso como derechos, y de los que sin embargo, se está haciendo un uso del que pueden beneficiarse los grupos criminales organizados. Sin duda este es uno de los principales problemas con los que el legislador debe enfrentase. Los denominados usos pasivos que de internet y los ordenadores están realizando las organizaciones criminales para facilitar su organización y actuación constituyen sin duda, el objetivo sobre el que procede comenzar a trabajar inmediatamente.

Pero lo que ahora se pretende es centrar la atención en los novedosos procedimientos tecnológicos de los que hacen uso las organizaciones criminales en general y las terroristas en particular, a fin de poder desarrollar un balance de los instrumentos legislativos con los que contamos para afrontar esta nueva realidad. Es decir, que el uso ilícito de las nuevas tecnologías fuerza además a una tipificación altamente especializada y precisa, en constante transformación y evolución. Por citar un ejemplo de gran interés, el empleo de Internet para la propaganda y radicalización terrorista (29), o para la realización de operaciones de información de contrainsurgencia (30).

---

(28) KERR, I. & GILBERT, D.: «The Role of IPS in The Investigation of Cybercrime», en Tom Medina & Johannes J. Britz, *Information Ethics in the Electronic Age*, *Mendina, Johannes Brtiz, eds., McFarland Press, 2004*, pp. 163 a 172.

(29) LARRIBA HINOJAR: «Globalización, terrorismo y libertad de expresión: conminación penal de actividades terroristas en el entorno virtual», en «*Constitución, derechos fundamentales y sistema penal*» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia 2009; p. 1089 y ss.

(30) TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007; TAIPALE, K. A.: «Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance», *NYU Review of Law & Security, No. 7, Supl. Bull.on L. & Sec., Spring 2006;* TAIPALE, K. A: «Cyber-Deterrence», *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global,* 2010.

C) En el campo del derecho procesal, han de destacarse las problemáticas relativas a: a) competencia y jurisdicción: aplicación extraterritorial de la ley penal; cooperación internacional; extradición y euroorden; b) 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; c) responsabilidad del *service provider.*

La competencia jurisdiccional en los cibercrímenes es un asunto complicado y difícil, en particular cuando se refiere al terrorismo (31). En este sentido, acciones en Internet que son legales en el país donde se inician pueden ser ilegales en otros países, incluso aunque el acto no sea particularmente fijado como objetivo en ese único país (32).

Los conflictos sobre la competencia jurisdiccional pueden ser tanto negativos –ningún Estado reclama la competencia–, como positivos –varios Estados reclaman dicha competencia–. Pero por encima de todo lo que no está claro es qué constituye la competencia jurisdiccional: ¿Es el lugar donde se lleva a cabo la acción?, ¿El país de residencia de quien comete la acción?, ¿El lugar donde se producen los efectos de la acción?, ¿O el país cuya nacionalidad tiene el propietario del ordenador que ha sido objeto de ataque?, ¿O todos ellos a la vez? Como es sencillo observar, tras estos interrogantes se esconden diversas cuestiones jurídicas: el *forum delicti commissi*; el principio territorial; la atribución de competencia a las diferentes jurisdicciones nacionales, etc.

En todo caso, de lo que no cabe duda es que los países no se ponen completamente de acuerdo sobre esta cuestión y tienen visiones muy diferentes, produciéndose así una divergencia global. Es más, los diversos estatutos sobre el cibercrimen que han sido aprobados en las últimas décadas en numerosos países, muestran una amplia variedad de cláusulas diversas sobre la competencia jurisdiccional (33).

---

(31) TRACHTMAN, J. P.: «Global Cyberterrorism, Jurisdiction, and International Organization», Tufts University, The Fletcher School, July 20, 2004.

(32) BRENNER, S. W. & KOOPS, B-J.: «Approaches to Cybercrime Jurisdiction», Journal of High Technology Law Vol IV No 1, 2004, pp. 3 a 46.

(33) REIDENBERG, J. R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, Vol 153:1951, 2005, pp. 1951 a 1974.

Por otra parte, ya se ha aludido a la interceptación y censura en anteriores apartados, ahora solo quiero hacer mención al incremento del uso de tecnologías para bloquear sitios con contenidos ofensivos y su posterior tráfico. El caso paradigmático es la pornografía infantil. En este sentido sobresale su empleo por unidades policiales de países tan variados como los EEUU, México, Holanda o España. Y en general, debe llamarse la atención para garantizar que la investigación policial de actividades delictivas se desarrolla conforme a reglas constitucionales de confidencialidad y proporcionalidad.

De otra parte, me parece crucial hacer referencia a la problemática de la investigación criminal ultraterritorial o transfronteriza (34). Un conocido caso puede servir de muestra.

En otoño de 2000, el FBI se enteró de que unos hackers habían penetrado en las redes informáticas de bancos, grandes grupos empresariales, proveedores de servicios de Internet y otras firmas norteamericanas. Ante la sospecha de que los ataques provenían de Rusia, el FBI intentó, sin éxito, asegurarse la asistencia de Rusia para la monitorización y reparación de la actividad criminal. Tras este fallido intento, los Estados Unidos decidieron actuar unilateralmente. Después de obtener una orden de registro en los USA, empleó un programa rastreador («sniffer») de registro de pulsación de tecla, para conocer los nombres de usuario y contraseñas de los hackers. Esta información fue empleada, a su vez, para bajar información incriminatoria de los ordenadores de los hackers en Rusia.

Las acciones descritas del FBI son conocidas como *«remote cross-border searchers and seizures»*, expresión que se puede traducir como búsquedas e incautaciones remotas transfronterizas (o fronterizas). Actualmente, las búsquedas e incautaciones de esta clase son una importante herramienta en la lucha contra el cibercrimen.

Los robos transfronterizos, los sabotajes de un sistema, los gusanos, y los ataques de denegación de servicio, causan, hoy por hoy, un enorme daño a los sistemas informáticos en los Estados Unidos y en otros países. Y para poder castigar esos crímenes,

(34) GOLDSMITH, J. L.: «The Internet and the Legitimacy of the Remote Cross Border Searches», *Chicago Public Law and Legal Theory Research Paper No. 16*, The Law School, University of Chicago, 2001, pp. 1 a 15.

es crucial identificar la procedencia del ordenador del que parte la actividad criminal e incautar (o al menos inmovilizar) información relevante para el crimen antes de que la grabación sea eliminada o borrada. No hay que olvidar aquí, que la demanda de información acerca de la actividad de ordenadores que están en el extranjero –o dicho con otras palabras, fuera de las fronteras del propio país– se incrementó de manera significativa tras los ataques terroristas del 11S de 2001.

Ciertamente, una manera de obtener información sobre ordenadores que están en el extranjero es a través de la cooperación entre los organismos oficiales encargados de aplicar la ley en el país fijado como objetivo –en el ejemplo planteado al principio, los Estados Unidos– y los del país de origen –en el ejemplo planteado al principio, Rusia–. El problema es que, a menudo, esta cooperación es harto difícil. Así pues, algunas veces, el gobierno del país de origen de los ataques carece de la autoridad legal para incautar e inmovilizar información de un ordenador más allá de sus fronteras. Algunas otras, de lo que carece es de capacidad tecnológica. También porque su maquinaria legal es demasiado lenta para hacer frente a un tipo de crimen en el que las pruebas pueden ser rápidamente destruidas o convertidas en anónimas. O, simplemente, el país de origen no quiere cooperar.

Por las razones descritas, y por muchas otras, las autoridades del país fijado como objetivo se pueden encontrar con capacidad para resolver ellos mismos el problema. Sentados en sus ordenadores, pueden trazar los orígenes del cibercrimen, y explorar, recabar y almacenar información relevante localizada en ordenadores que están en el extranjero.

En la doctrina, muchos autores entienden que esas búsquedas e incautaciones remotas transfronterizas, violan la soberanía territorial del país donde los datos son localizados. Este punto de vista parece encontrar apoyo en las prohibiciones de aplicación ultraterritorial de la ley recogidas en instrumentos jurídicos de Derecho Internacional. Frente a estas opiniones, se formulan otras en las que se argumenta que las búsquedas e incautaciones remotas transfronterizas son acordes con los principios internacionales que rigen la aplicación de la ley. No afirman, no obstante, que no deban existir límites en esas búsquedas e incautaciones, sino que esos límites no deben deducirse de normas relativas a la territorialidad. En su lugar, los límites tendrán que emerger de un complica-

do proceso de examen y regulación jurídica transnacional, desde el momento en que las naciones han de ajustarse ellas mismas a los cambios crecientes de las nuevas tecnologías. Esto es, apelan a la necesidad de arrojar algo de luz en la relación entre el cambio tecnológico y la evolución de nuestros conceptos jurídicos (35).

Por último, decir que, al argumentar que las citadas búsquedas e incautaciones remotas transfronterizas pueden ser legales, desde el punto de vista jurisdiccional, estos autores no niegan que el ejercicio de estas pueda ser problemático. Es más, entienden que, aunque esas búsquedas e incautaciones estén justificadas en el terreno jurisdiccional, pueden ser injustificables desde la perspectiva de los derechos fundamentales individuales de privacidad (intimidad) y de libertad de expresión.

D) Otra cuestión de enorme complejidad es, después de analizar las medidas legislativas existentes en nuestro ordenamiento jurídico, con especial incidencia en las penales, en relación a los delitos informáticos y los delitos comunes cometidos a través de la informática cometidos en el seno de organizaciones criminales y especialmente terroristas, la interpretación y aplicación que vienen realizando nuestros Juzgados y Tribunales de justicia.

E) Por último, tras haber estudiado la normativa internacional relativa a estas materias, examinar el grado de integración de tales normativas en nuestro sistema legislativo, así como la necesidad de la misma, lo que obligará a fijarse en las dificultades y necesidades de adaptación que ello requiera.

Problemas Específicos

Después de exponer las categorías generales del Derecho afectadas por los usos y abusos de las nuevas tecnologías, dedicaré un último apartado a resaltar las cuestiones más específicas de esta creciente problemática.

A) En primer lugar, como ya se vio al examinar las respuestas legales, la situación varía considerablemente entre países y regiones, con diferente grado de implantación de las nuevas tecnologías y también con diferente grado de desarrollo de sus legislaciones. Estrechamente vinculado a este diagnóstico, se encuentra el dato de que más de 45 países han firmado el Convenio de Ciberde-

(35) GOLDSMITH, *ob.* y *loc.cit.*

lincuencia, tanto en el espacio del Consejo de Europa, como en el de Naciones Unidas. Sin embargo, aún dentro de este selecto grupo de naciones, se observa una distinta escala de operatividad del mismo, debida a múltiples circunstancias, entre ellas la efectiva incorporación a los ordenamientos nacionales de las disposiciones internacionales (36).

B) Podría decirse, en términos generales, que aunque el modelo contenido en el Convenio funciona muy aceptablemente, en particular en el espacio europeo occidental y norteamericano, algunos Estados permanecen excesivamente absortos en sus prioridades y problemas internos. Esta actitud supone un desconocimiento de las ventajas globales de la cooperación y armonización internacional.

C) La tendencia marcada por el Convenio, así como su funcionamiento en general, merece una valoración altamente positiva. Especialmente porque contribuyó a la concienciación internacional sobre la magnitud y evolución de este problema, logrando consensos políticos mínimos acerca de las conductas a prohibir y de los mecanismos de persecución y colaboración jurisdiccional. Pero también porque significó un gran avance técnico-jurídico, por ejemplo, al propiciar definiciones legales estándar, posibilitar la extradición y fortalecer la cooperación policial y judicial entre Estados.

D) Sin embargo, el crecimiento de la cibercriminalidad no se debe imputar únicamente a las insuficiencias legales, ya sean al definir los ilícitos, al establecer los procedimientos procesales o regular la cooperación de las agencias de seguridad, sino que también obedece, y en gran medida, a la simple negligencia de las personas, incluso en áreas de la alta seguridad sumamente profesionalizada. Por ejemplo, un soldado sueco ha sido declarado culpable por negligencia al haber perdido una memoria USB en un ordenador de la Universidad de Estocolmo, con detalles sobre bombas sin explosionar en Afganistán. O que el ejército norteamericano esté tomando medidas contra el uso de memorias USB tras la infección de redes de defensa con el gusano SillyFDC. O los numerosos supuestos de espionaje, fraude o robo de datos por la apertura del correo electrónico sin tomar las medidas de seguridad mínimas (37).

---

(36) HANSSEN, H-S.: «The Future of International Law: Cybercrime», *Regional Meeting of ASIL*, Golden Gate University School of Law, 17 Annual Fulbright Symposium on The Future of International Law, San Francisco, 7 April, 2007.

(37) MENN, J.: «Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet», Perseus Books, 2010.

E) Ahora bien, los logros anteriormente reseñados no pueden valorarse como absolutos ni como permanentes. Por ello, para finalizar, señalaré algunos de los problemas específicos pendientes de resolver en el plano jurídico.

1. A pesar de los avances del Convenio en esta materia, sigue siendo un reto de máxima prioridad alcanzar consensos sobre las definiciones legales, esto es, sobre la tipificación precisa y exacta de los comportamientos declarados como delitos. Sólo si la normativa internacional facilita el acuerdo acerca de lo que es delito, esto es, armoniza el Derecho penal de los diferentes Estados al describir las figuras delictivas, podrá realmente articularse una efectiva cooperación internacional. En efecto, pues si compartimos tipos delictivos similares o idénticos, entonces podremos desarrollar adecuadamente procedimientos de extradición, intercambio de pruebas y de otra clase de informaciones. De ahí la esencial transcendencia de este enorme desafío y el objetivo de corregir las cláusulas de escape detectadas en el Convenio.
2. El transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y por consiguiente tengamos la necesidad de actualizarlo. En este sentido, y a título de ejemplo, pueden citarse conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos en mundos virtuales (v. gr. el *atraco* en la red social Habbo Hotel). A la necesidad de actualizar la legislación contribuye el constante progreso de las nuevas tecnologías, pues hoy, por ejemplo, con un simple iPod se puede copiar toda la información de un ordenador que carezca de una protección adecuada. También se discute la necesidad de sancionar penalmente a las empresas que no comunican a los usuarios y a las autoridades «brechas de seguridad» en sus servidores.
3. Por fin, aunque el Convenio ha supuesto un extraordinario adelanto –aunque como hemos visto insuficiente– para la armonización de la legislación penal, adolece sin embargo de un desarrollo normativo avanzado en materia de cooperación policial. Es decir, se precisa un esfuerzo legislativo tendente a facilitar las necesidades operativas, habida cuenta de la todavía inercia policial a la actuación dentro de sus fronteras respectivas. Así, mientras la ciberdelincuencia está organizada, comparte

información y actúa en cualquier parte del mundo, se hace imprescindible que las fuerzas de seguridad posean herramientas similares: organismos internacionales *ad hoc;* intercambio de información en tiempo real e instrumentos de cooperación transfronterizos. Los aislados éxitos en este campo, como por ejemplo la reciente operación secreta del FBI en colaboración con otros cuerpos policiales, contra el foro denominado «Dark Market», avalan esta necesidad y posiblemente muestran la escasa eficacia hoy existente.

En definitiva, como expone el informe del Parlamento Europeo de 2 de marzo de 2010**,** es sumamente necesaria una normativa unificada internacional, para detener la gran cantidad de abusos, robo de identidad y demás delitos virtuales que realizan casi a diario los atacantes informáticos. La propuesta, básicamente, se basa en la creación de un conjunto de normas internacionales que definan taxativamente los actos delictivos en internet, y posibiliten la reducción de las altas cotas actuales de impunidad en la que se escudan los atacantes informáticos por la falta de normativas unificadas, por parte de la comunidad internacional, que impiden que sean castigados o capturados si se encuentran en un país remoto, al lugar al que atacaron.

La finalidad es minimizar los ataques, tanto personales como corporativos y gubernamentales, que traen consigo fraudes, robos de identidad y hasta espionaje. Aún está reciente el ataque a Google proveniente de Asia, zona que alberga una gran cantidad de atacantes que se escudan en una legislación local obsoleta y permisiva, que les facilita la comisión y posterior impunidad de delitos cometidos fuera de sus fronteras.

Por tanto, unas legislaciones armonizadas a nivel mundial permitirían a los Estados, a las corporaciones y a los particulares afectados, salvar el obstáculo de las fronteras y poder investigar, capturar y enjuiciar a los atacantes en cualquier lugar del mundo donde se encuentren –incluso si utilizan servidores Proxy–, ya que sería más sencillo ubicarlos.

En este citado Informe, se aconseja que los miembros de La Unión Europea, que poseen los mejores sistemas en línea, deben realizar un acercamiento directo en tema de ciberseguridad con países no pertenecientes a la UE, como Estados Unidos, China y Rusia, para tratar de unificar sus legislaciones e incrementar la cooperación, con el objetivo de disminuir los delitos virtuales.

De igual forma, la Unión Europea debería desarrollar una estrategia similar a la contenida en la Iniciativa Nacional de Ciberseguridad norteamericana. Como se ha conocido recientemente, en la misma se fija el objetivo de establecer estrategias efectivas para blindar las transacciones bancarias y financieras, las redes de transporte por superficie, subterráneas, aéreas y marítimas, y la protección digital de las infraestructuras de comunicaciones civiles y militares, de energía, transporte, seguridad militar, e informática, de toda la nación. Con ello se trata de evitar que los ciberatacantes provoquen apagones masivos, detengan la actividad comercial y financiera, cometan fraudes a particulares y entidades financieras, o alteren el funcionamiento de las redes de seguridad informáticas civiles y militares.

Idéntica orientación ha tomado la doctrina militar rusa en materia de seguridad en la información, como se ha publicado parcialmente en febrero de 2010 en un documento no clasificado.

CONCLUSIONES

La primera conclusión se centra en la mutación expansiva de la categoría jurídica de seguridad nacional, que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno más amplio y multidimensional como es el de seguridad nacional. Ahora bien, este nuevo concepto todavía en formación, no ha acabado de perfilarse con la suficiente concreción jurídica, discurriendo en numerosas ocasiones entre su entendimiento como idea simbólica-emotiva, o como equivalente a interés general identificado con el interés del Estado y contrapuesto al interés individual. De aquí que el usual manejo del canon de ponderación de intereses para resolver los conflictos entre seguridad nacional y derechos fundamentales, casi siempre se resuelve a favor del primero.

En segundo lugar, nos hallamos ante un nuevo escenario estratégico, criminológico y político-criminal, en el que se aprecia no sólo un salto cuantitativo sino también cualitativo. Y en este sentido se habla de una ruptura: los escenarios de ataques son muy variados, con diferentes niveles de riesgo y de muy diversa escala de impacto potencial, lo que complica extraordinariamente su prevención y respuesta estatal. Ahora el *nuevo terrorismo y la nueva criminalidad transnacional*, se muestran con una mayor agresividad y representan un auténtico desafío para los

Estados. Pero su control igualmente hace peligrar los valores del Estado de Derecho, especialmente la de los derechos fundamentales.

En tercer lugar, el desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. Hoy en día se ha encaminado el control de muchos procesos mundiales a través del ciberespacio. Por lo que no hay duda de que actualmente el ciberespacio constituye un bien valioso. Y de que la seguridad del ciberespacio ha crecido en importancia.

En cuarto lugar, ha de tenerse presente que a la profesionalización, internacionalización y globalización de la criminalidad, se suma la consolidación del uso de las tecnologías de la información y la comunicación (TIC), obtenemos los ejes esenciales que configuran la realidad sobre la que gira este trabajo. En este sentido, en sí mismas las TIC constituyen instrumentos de alto valor patrimonial, político y estratégico; pero tampoco deben minusvalorarse las facilidades que el uso de las nuevas tecnologías ofrece para la ejecución de ilícitos, lo que a su vez conlleva la generalización y aumento del recurso a estas tecnologías como instrumento comisivo.

En quinto término, podría decirse que *cibercrimen* y *ciberamenazas* no son categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la seguridad nacional, ni todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos mencionados –terrorismo y criminalidad organizada–, determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.

Y en sexto y último lugar, afirmar que la combinación de varios de los factores enunciados, ha propiciado el nacimiento o el replanteamiento de una serie de complejas cuestiones jurídicas, tanto relativas a los derechos fundamentales, como a cuestiones penales sustantivas y procesales. En este sentido, la tendencia marcada por el Convenio sobre Cibercriminalidad, así como su funcionamiento en general, merece una valoración altamente positiva. Sin embargo, el transcurso del tiempo y la constante innovación tecnológica han causado que el Convenio, en ciertas materias, haya quedado parcialmente obsoleto y por consiguiente tengamos la necesidad de actualizarlo. En este sentido, y a título de ejemplo, pueden citarse conductas graves no contenidas en el Convenio, como el *phishing*, la suplantación de identidad, o los delitos cometidos

en mundos virtuales. Igualmente se hace preciso reforzar y avanzar en materias como la competencia ultraterritorial y también en cooperación policial internacional.

BIBLIOGRAFÍA

ALBANESE, J.S., DAS, D.K., y VERMA, A., (editores), *Organized crime.* World perspectives, New Jersey, 2003;

ARQUILLA, J., y RONDFELDT, D., *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político*, Madrid, 2002;

ARTEAGA: «La estrategia europea de seguridad: cinco años después», ARI nº 15/2009, Real Instituto Elcano, 22/01/2009.

BANDINI, T., *La criminalità organizzata*, Torino, 1993.

BALLESTEROS MARTÍN, M. A.: «*El papel de las fuerzas armadas en la lucha contra el terrorismo internacional*», en Real Instituto Elcano de Estudios Internacionales y Estratégicos, 18/08/2006.

BERDAL, M., y SERRANO, M., (editores), *Transnacional organized crime and internacional security: business as usual?*, Colorado, 2002.

BOIX REIG (dir.) y JAREÑO LEAL (coord.): «La protección jurídica de la intimidad», Madrid 2010;

BRENNER, S. W. & KOOPS, B-J.: «Approaches to Cybercrime Jurisdiction», Journal of High Technology Law Vol IV No 1, 2004, pp. 3 a 46.

CARRASCO ANDRINO: «El delito de acceso ilícito a los sistemas informáticos», en «Comentarios a la reforma penal de 2010», (Dir. F. Álvarez García y J. L. González Cussac), Valencia (Tirant), 2010;

CLARKE, R. A.: «Cyber War: The Next Threat to National Security and What to Do About it», HarperCollins, 2010;

Convenio Internacional sobre el cibercrimen, 23 de noviembre de 2001 (Council of Europe CETS No 185).

[disponible en**:** http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm]

Coordinator for Counterterrorism (NCTb), *Jihadist and the internet*, Delta-Hage, La Haya, 2007, pp. 17 y ss.

[disponible en www.fas.org/irp/world/netherlands/jihadis.pdf]

CUADRADO RUIZ: «Interceptaciones telefónicas y nuevas tecnologías», en *Cuadernos Jurídicos* 1992;

DE LA CUESTA ARZAMENDI y DE LA MATA BARRANCO (directores): «Derecho penal informático», Madrid 2010;

DÍAZ SANTOS, M.R., y FABIÁN CAPARRÓS, E. A., «*El sistema penal frente a los retos de la nueva sociedad*», Madrid, 2003.

Doctrina militar rusa y seguridad en la información: [disponible en**:** www.belt.es/expertos/HOME2_experto.asp?id=4999]

Cybersecurity FBI. [disponible en**:** www.fbi.gov/cyberinvest/cyberhome.htm]

FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Oviedo 2007.

FERNÁNDEZ RODRÍGUEZ y SANSÓ-RUBERT PASCUAL (editores): «Internet: un nuevo horizonte para la seguridad y la defensa» (Seminario de Estudios de Seguridad y Defensa de la USC-CESEDEN). Universidad de Santiago de Compostela 2010;

FERRÉ OLIVÉ, J.C., y ANARTE BORRALLO, E., *Delincuencia organizada. Aspectos penales, procesales y criminológicos*, Universidad de Huelva, Huelva, 1999.

FOJÓN CHAMORRO y SANZ VILLALBA: «Ciberseguridad en España: una propuesta para su gestión», ARI 101/2010, Real Instituto Elcano 18/06/2010;

FREUND, W., *Die Strafbarkeit von Internetdelikten*, Wien, 1998.

GALÁN MUÑOZ, A., «*El fraude y la estafa mediante sistemas informáticos*», Valencia, 2005;

GALÁN MUÑOZ: «Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», en Revista de derecho y proceso penal, 15, 2006;

GALÁN MUÑOZ: «Ataques contra sistemas informáticos», *Boletín Información Ministerio de Justicia*, 2006;

GOLDSMITH, J. L.: «The Internet and the Legitimacy of the Remote Cross Border Searches», *Chicago Public Law and Legal Theory Research Paper No. 16*, The Law School, University of Chicago, 2001, pp. 1 a 15.

GÓMEZ NAVAJAS: *La protección de datos personales*, Madrid 2005;

GÓMEZ TOMILLO, M., *Responsabilidad penal y civil por delitos cometidos a través de internet. Especial consideración del caso de los Proveedores de contenidos, servicios, acceso y enlaces*, 2ªedic., Pamplona 2006.

GONZÁLEZ CUSSAC, J. L.: «*Nuevas amenazas a la seguridad nacional: el desafío del nuevo terrorismo»*, en «Retos de la política criminal actual», Revista Galega de Seguridade Pública (REGASP)«, nº 9, Xunta de Galicia, 2007, pp. 233 a 252;

GONZÁLEZ CUSSAC, J. L. y FERNÁNDEZ HERNÁNDEZS, A.: «*Sobre el concepto jurídico-penal de terrorismo»*, en «El Estado de Derecho frente a la amenaza del nuevo terrorismo», en «Teoría y Derecho. Revista de pensamiento jurídico «(Tirant), nº 3, junio 2008, pp. 34 a 58;

GONZÁLEZ CUSSAC, J. L: «*Intromisión en la intimidad y servicios de inteligencia»*, en «La protección de la intimidad», Cursos de Formación de Fiscales, Madrid (CEJ), 2010**;**

GONZÁLEZ CUSSAC/LARRIBA HINOJAR: «Un nuevo enfoque legal de la inteligencia competitiva», en »Inteligencia y Seguridad: Revista de análisis y prospectiva», nº 8, 2010, pp. 39 y ss.;

GONZÁLEZ RUS**: «**Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», Rev. De la facultad de Derecho de la Universidad Complutense, 12; 1986;

GONZÁLEZ RUS**: «**Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264,2 CP)», en La ciencia del derecho penal ante el nuevo siglo: homenaje al Prof. Cerezo Mir, Madrid 2002;

GONZÁLEZ RUS: «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en «El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales», Granada 2006;

GUISASOLA LERMA: «*Tutela penal del secreto de las comunicaciones. Estudio particular del supuesto de interceptación ilegal de telecomunicaciones por autoridad o funcionario público»,* en «Constitución, derechos fundamentales y sistema penal» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia (Tirant) 2009;

GÜNTER, R., *Computer criminalität*, bhv, 1998.

GUTIÉRREZ FRANCÉS, M.L., «*Fraude informático y estafa*», Madrid, 1991;

HANSSEN, H-S.: «The Future of International Law: Cybercrime», *Regional Meeting of ASIL*, Golden Gate University School of Law, 17 Annual Fulbright Symposium on The Future of International Law, San Francisco, 7 April, 2007.

HOFFMAN, B., «The Use of the Internet by Islamic Extremists», [disponible en www.rand.org]

Informe del Parlamento Europeo de 2 de marzo de 2010, [disponible en www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2010-0026+0+DOC+XML+V0//ES]

JAREÑO LEAL y DOVAL PAIS: «Revelación de datos personales, intimidad e informática», en *La Ley*, 4844, 1999;

JIMÉNEZ CAMPOS: «*La garantía constitucional del secreto de las comunicaciones*», en Comentarios a la legislación Penal, tomo VII, Madrid (Edersa) 1986;

JOFER, *Strafverfolgung im Internet. (Phänomenologie und Bekämpfung kriminellen Verhaltens in internacionalen Computernetzen)*, Frankfurt a. M., 1999;

KERR, I. & GILBERT, D.: «The Role of IPS in The Investigation of Cybercrime», en Tom Medina & Johannes J. Britz, *Information Ethics in the Electronic Age*, *Mendina, Johannes Brtiz, eds., McFarland Press, 2004*, pp. 163 a 172;

LARRIBA HINOJAR: «Globalización, terrorismo y libertad de expresión: conminación penal de actividades terroristas en el entorno virtual», en «Constitución, derechos fundamentales y sistema penal» (Dir. Carbonell Mateu/González Cussac/Orts Berenguer), Valencia (Tirant) 2009; p. 1089 y ss.:

LEWIS, J.: «Security Cyberspace in the 44th Presidency», Report 2008.

LÓPEZ ORTEGA: «La intimidad como bien jurídico protegido», en *Estudios sobre el Código Penal de 1995* (Parte Especial), *CGPJ*, Madrid 1996;

LÓPEZ ORTEGA: «Intimidad informática y Derecho Penal (la protección penal de la intimidad frente a las nuevas tecnologías de la informa-

ción y comunicación)», en *Derecho a la intimidad y nuevas tecnologías*, CDJ 2004;

MADRID CONESA: «*Derecho a la intimidad informática y Estado de Derecho*», Valencia, 1984;

MARCHENA GÓMEZ: «Intimidad e informática: la protección jurisdiccional del *habeas data*», en *BIMJ*, 1996;

MARCHENA GÓMEZ: «El sabotaje informático: entre los delitos de daños y desórdenes públicos», Cuadernos de Derecho Judicial, 10, 2001;

MATA Y MARTÍN: «*Delincuencia informática y Derecho Penal*», Madrid 1996;

MATA Y MARTÍN: «La protección penal de datos como tutela de la intimidad de las personas: intimidad y nuevas tecnologías», *RP* 2006;

MATELLANES RODRÍGUEZ: «El intrusismo informático como delito autónomo», *RGDP* 2004;

MENN, J.: «Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet», Perseus Books, 2010;

MIR PUIG (editor): «*Delincuencia informática*», Barcelona, 1992;

MIRÓ LINARES: «Internet y delitos contra la propiedad intelectual», Madrid 2005;

MORALES PRATS: «*La tutela penal de la intimidad: privacy e informática*», Madrid, 1984;

MORALES PRATS: «Servicios de información y espionaje del Estado y secreto de comunicaciones telefónicas», en *Actualidad Aranzadi*, 253, 1996;

MORÓN LERMA, E., «*Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*», 2ª ed., Pamplona 2002.

ORTS BERENGUER: «Revelación y uso indebido de secretos e informaciones», en *CDJ (Delitos de los funcionarios públicos),* Madrid 1994;

ORTS BERENGUER, E., y ROIG TORRES, M., «*Delitos informáticos y delitos comunes cometidos a través de la informática*», Valencia, 2001.

PANSIERA, F. J., y JEZ, E., «*La criminalité sur l´internet*», Puf, 2000;

PICCOTI, L., (Coord.), «*Il diritto penale dell´informatica nell´epoca di internet*», Padova, 2004.

QUINTERO OLIVARES: «Internet y propiedad intelectual», en Cuadernos de derecho judicial, 10, 2001;

REBOLLO BARGAS: «*La revelación de secretos e informaciones por funcionario público*», Barcelona 1996;

REIDENBERG, J. R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, Vol 153:1951, 2005, pp. 1951 a 1974.

RODRÍGUEZ MOURULLO/LASCURAIN SÁNCHEZ/ALONSO GALLO: «Derecho penal e internet», en «Régimen jurídico de internet», Madrid 2001;

ROGAN, H., *Jihadism online – A study of how al-Qaeda and radical islamist groups use the Internet for terrorist purposes,* FFI/RAPPORT-2006/00915, [disponible en http://rapporter.ffi.no/rapporter/2006/00915.pdf];

ROMEO CASABONA, C. M., «*Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*», Madrid, 1987.

ROMEO CASABONA: «La protección penal del «software» en el Derecho español», *AP* 35, sept-oct. 1988;

ROMEO CASABONA: «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», *P.J.,* 31, 1993;

ROMEO CASABONA: «*Los delitos de descubrimiento y revelación de secretos*», Valencia 2005;

ROMEO CASABONA (coord.): «*El Cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas políticocriminales*», Granada 2006;

RUEDA MARTÍN: «Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal», Barcelona 2004;

RUIZ MARCO, F., «*Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*», Madrid, 2001.

SÁNCHEZ GARCÍA DE PAZ: «La criminalidad organizada. Aspectos penales, procesales, administrativos y policiales», Madrid, 2005.

SERRANO PIEDECASAS: «Consideraciones en torno a la protección penal del «Knowhow», *ADPCP*, III, 1990;

SIEBER, U., (editor), «*Information technology crime*», Köln, 1994;

SHULMAN, C.: «Medidas del Consejo de Europa para luchar contra la cibercriminalidad», en ENAC, nº 2, agosto 2009, p. 31.

TAIPALE, K. A.: «Seeking Symmetry on the Information Front Confronting Global Jihad on the Internet», National Strategy Forum Review, Vol. 16, summer 2007.

TAIPALE, K. A.: «Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd», *Yale Journal of Law and Technology,* Vol. 7, No. 123, December 2004, pp. 123 a 201.

TAIPALE, K. A.: «Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance», *NYU Review of Law & Security, No. 7, Supl. Bull.on L. & Sec., Spring 2006;*

TAIPALE, K. A: «Cyber-Deterrence», *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global,* 2010;

TAIPALE, K. A «Internet and Computer Crime: System Architecture as Crime Control», *Center for Advanced Studies Working Paper No. 03-2003*, 2003.

TRACHTMAN, J. P.: «Global Cyberterrorism, Jurisdiction, and International Organization», Tufts University, The Fletcher School, July 20, 2004.

VVAA: «Cybercrime & Security», New York 2005;

VVAA: González Cussac J. L. y Fernández Hernández A. coord. «Financiación del terrorismo, blanqueo de capitales y secreto bancario. Un análisis crítico«, Valencia, 2009;

VIVES ANTÓN; ORTS BERENGUER; CARBONELL MATEU; GONZÁLEZ CUSSAC; MARTÍNEZ-BUJÁN PÉREZ. «Derecho Penal. Parte especial», 3ª ed. Valencia 2010.

WALL, D. S.: «The Internet as a Conduit for Criminal Activity», Information Technology and the Criminal Justice System, Pattavina, A., ed. Sage Publications, Inc., 2005, pp. 77-98.

YAR: «Cybercrime and society», London 2006;

ZÚÑIGA RORÍGUEZ, L., / MÉNDEZ RODRÍGUEZ, C., / DIEGO DÍAS-SANTOS, M.R., (Coords.), «*Derecho Penal, sociedad y nuevas tecnologías*», Madrid, 2001.