MOISÉS BARRIO ANDRÉS

Ciberdelitos 2.0

Amenazas criminales del ciberespacio

Ciberacoso. Porno venganza (*sexting* y *revenge porn*)
Estafas. Intrusismo (*hacking*). Daños y sabotajes (*cracking*)
Pornografía infantil. Indemnidad sexual (*child grooming*)
Calumnias e injurias. Revelación de secretos
Propiedad intelectual. Ciberterrorismo

2ª edición actualizada y ampliada

ASTREA
BUENOS AIRES - BOGOTÁ - PORTO ALEGRE
2020

V

Barrio Andrés, Moisés
Ciberdelitos 2.0 / Moisés Barrio Andrés
2ª ed. - Ciudad Autónoma de Buenos Aires: Astrea, 2020.
184 p.; 23×16 cm.

ISBN 978-987-706-357-8

1. Delitos Informáticos. I. Título

CDD 342.066

Astrea está indexada como Editorial de Calidad Científica
con Claro Prestigio Internacional (Fondecyt).

1ª edición, 2017.
2ª edición, 2020.

Esta obra ha sido evaluada conforme a los estándares internacionales de calidad científica de referato externo, con sistema doble ciego.

Lavalle 1208 - (C1048AAF) Ciudad de Buenos Aires
(54-11) 4382-1880 - 0800-345-ASTREA (278732)
www.astrea.com.ar - editorial@astrea.com.ar

La edición de esta obra se realizó en Editorial Astrea, y fue impresa en su taller, Berón de Astrada 2433, Ciudad de Buenos Aires, en la primera quincena de octubre de 2020.

Queda hecho el depósito que previene la ley 11.723
IMPRESO EN LA ARGENTINA

A Roberto,
cuya personalidad renacentista
y curiosidad desbordante sugieren
atinadas pautas de pensamiento

A la memoria de mis abuelos
Moisés y María

VIII

PRÓLOGO A LA SEGUNDA EDICIÓN

La gran acogida por los lectores a la primera edición de *Ciberdelitos: amenazas criminales del ciberespacio*, motivó que se agotara en menos de un mes, e incluso haya sido seguida de varias reimpresiones posteriores.

Esta segunda edición, calificada de *2.0* en su título, incluye tres nuevos capítulos y una ampliación de los contenidos de la parte especial frente a la primera edición. Asimismo, y en aras de la claridad expositiva, los distintos tipos penales se exponen individualmente, y no sistematizados conforme a la clasificación anteriormente utilizada del Convenio de Budapest, para facilitar así su lectura por aquellos profesionales no familiarizados previamente con los ciberdelitos.

Concluyo este prólogo agradeciendo a varios amables lectores las sugerencias enviadas respecto de áreas puntuales que estaban necesitadas de complemento. Esa es la auténtica finalidad de esta obra: tratar de ser un instrumento útil y práctico en una materia cambiante, compleja, extensa y excepcionalmente atractiva.

MOISÉS BARRIO ANDRÉS

X

PRÓLOGO A LA PRIMERA EDICIÓN

Internet es, sin duda, la clave de bóveda de la sociedad de la información y desempeña un papel crucial en el desarrollo económico de nuestro tiempo. La popularización de la Red a escala global ha permitido la creación del "ciberespacio virtual", tal y como lo concibiera el autor que acuñó tal término, WILLIAM GIBSON[1], al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la última década del siglo XX, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales. Incluso ha surgido una nueva disciplina jurídica, el "Ciberderecho" o "Derecho de internet" (*Cyberlaw*), para dar respuesta a las situaciones jurídicamente disruptivas que plantea internet y que hemos analizado en otra obra reciente[2].

Algunos de los avances técnicos proporcionados por internet podrían sintetizarse en la enorme facilidad y rapidez con la que se accede, copia, modifica y distribuye todo tipo de información, siempre a distancia y con posibilidad de ocultar la identidad real. Cada sujeto puede ser, a la vez, emisor y receptor de contenidos, fortaleciendo así libertades garantizadas constitucionalmente. Estas características han convertido a internet en una herramienta insustituible

[1] El prefijo *cyber* proviene, a su vez, del término *cyberspace* creado por el novelista de ciencia ficción WILLIAM GIBSON y su obra *Neuromancer*, en la que el autor describe una sociedad tecnológicamente avanzada donde las personas viven en un mundo virtual separado del mundo real.

[2] Ver BARRIO ANDRÉS, *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*.

para cualquier tipo de usuario[3]. En la actualidad, los sistemas informáticos resultan de extraordinaria importancia para todos los sujetos: desde administraciones públicas, prestadores de servicios públicos, empresas, entidades privadas hasta, por supuesto, los ciudadanos. En este sentido, la integración de internet en prácticamente todas las actividades, tanto públicas como privadas, y el proceso de globalización que caracteriza la economía actual han permitido nuevas formas de organización de la producción y de la comercialización. Tampoco debe olvidarse su utilización como forma de diversión, con las redes sociales y la *web 2.0* como forma de interactuación social.

Lo anterior conduce a que, en casi todos los ámbitos de la vida, se dependa, de forma muy intensa, de las Tecnologías de la Información y la Comunicación (en adelante, TIC)[4], que integran un concepto amplio, abierto y dinámico, que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en el milenio digital[5]. Y, a medida

[3] La doctrina destaca, unánimemente, la afectación transversal de internet. Vid., al respecto, entre otros: Brenner, Susan: *Cybercrime and evolving threats from cyberspace*, Editorial Praeger Publishers Inc., 2ª ed., Toronto, 2018; Asencio Mellado, José María (dir), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, 2017; Clough, Jonathan, *Principles of Cybercrime*, Cambridge University Press, Cambridge, 2015, 2ª ed.; Hilgendorf, Eric; Frank, Thomas y Valerius, Brian, *Computer- und Internetstrafrecht: Ein Grundriss*, Editorial Springer, Berlín, 2005; Barrio Andrés, Moisés, "Criminalidad e Internet: Retos del Siglo XXI", en *Sentencias de TSJ y AP y otros Tribunales*, nº 15, 2003; Morales Prats, Fermín: "Internet: riesgos para la intimidad", en *Cuadernos de Derecho Judicial*, nº 10, 2001, p. 70; Matellanes Rodríguez, Nuria, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", en Sánchez López, Virginia (coord.), *Hacia un derecho penal sin fronteras*, Editorial Colex, Madrid, 2000, p. 129; o Morón Lerma, Esther, *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Editorial Aranzadi, Pamplona, 1999.

[4] Así, Rovira del Canto, Enrique, advierte que sin las TIC las sociedades actuales colapsarían, generándose lo que se conoce como la *computer dependency* (*Delincuencia informática y fraudes informáticos*, Editorial Comares, Granada, 2002, p. 9).

[5] En inglés el acrónimo utilizado es ICT, correspondiente a las siglas de "Information and Communications Technology". No existe una lista cerrada de elementos que configuran las TIC, sino que se incluyen

que las redes de comunicaciones se hacen más convergentes y prestan mayores servicios, aumenta, de forma pareja, su vulnerabilidad, de modo que ambos factores –dependencia y vulnerabilidad– se han ido incrementando progresivamente desde los años 90[6]. Por tanto, se trata de una tendencia que implica numerosas ventajas, pero que también va acompañada de nuevos riesgos.

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

---

en ella no solo los que conforman los modos actuales de tratamiento y transmisión de la información, sino también los futuros. En todo caso, se engloban dentro de las TIC tanto las redes (entre las cuales destaca internet, pero también comprende las de telefonía móvil y otras redes telemáticas), como los equipos terminales (entre los que predominan los ordenadores personales, pero también ya son gran vehículo de comunicación los *smartphones*, las tabletas o las consolas) y los servicios, entre los que sobresalen la descarga de archivos –directa, mediante redes P2P o su visualización directa en *streaming*–, el comercio electrónico, la banca electrónica, la realización electrónica de actividades relacionadas con la Administración Pública y, cada vez más, las redes sociales.

[6] Ver WALL, DAVID, *Cybercrime: the transformation of crime in the Information Age*, Editorial Polity Press, Cambridge, 2007. Entre nosotros, RODRÍGUEZ MOURULLO, GONZALO; ALONSO GALLO, JAIME y LASCURAIN SÁNCHEZ, JUAN ANTONIO: "Derecho Penal e Internet", en AA.VV., *Régimen jurídico de Internet*, Editorial La Ley, Madrid, 2002, p. 257.

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

Habiéndose originado internet en los Estados Unidos[7], fueron sus tribunales quienes primero van a enjuiciar los incipientes ciberdelitos y sus particulares consecuencias a principios de 1990. Así, en *United States v. Morris*[8], el acusado, un estudiante de ingeniería informática de la Universidad de Cornell, creó un virus diseñado para infectar internet con el propósito de demostrar las insuficiencias de las medidas de seguridad en las redes electrónicas. Su programa informático funcionó increíblemente bien, y pese a los intentos del acusado de detener la propagación del virus, éste causó daños importantes a ordenadores de todo el país pertenecientes a instituciones académicas, militares y comerciales. Robert Morris fue condenado en primera instancia en virtud de la *Computer Fraud and Abuse Act* de 1986[9] (CFAA), condena que fue confirmada en apelación.

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

Así, como advierte en nuestra doctrina Miró Llinares[10], la evolución del cibercrimen también conlleva una evolu-

[7] Vid., al respecto, Barrio Andrés, Moisés, *Fundamentos del Derecho de Internet*, Editorial Centro de Estudios Políticos y Constitucionales, Madrid, 2017, p. 55 y siguientes.

[8] 928 F.2d 504, 505 (2d Cir. 1991).

[9] 18 U.S.C. § 1030.

[10] Miró Llinares, Fernando, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Editorial Marcial Pons, Madrid, 2012, p. 27 y siguientes.

ción en sus protagonistas esenciales, los criminales y las víctimas: del ya mítico *hacker* estereotipado en el adolescente introvertido y con problemas de sociabilidad, encerrado en su casa y convertido en el primer ciberespacio en un genio informático capaz de lograr la guerra entre dos superpotencias usando solo su ordenador, hemos pasado a las mafias organizadas de cibercriminales que aprovechan este nuevo ámbito para aumentar sus actividades ilícitas y sus recursos. Y al no ser los cibercrímenes solo los realizados con ánimo económico, también varían los perfiles de cibercriminales que cometen delitos, que ya no son únicamente réplicas en el ciberespacio de los que ejecutarían en el espacio físico. Y lo mismo ocurre con las víctimas. Las personas jurídicas siguen siendo objeto de victimización debido tanto al uso generalizado de las TIC en ellas como a sus recursos económicos objeto de deseo por los cibercriminales. No obstante, muchas suelen ocultar los ciberdelitos de los que son víctimas. La actitud poco favorable a la denuncia se debe al temor de que la trascendencia del hecho se traduzca en una suerte de descrédito de la fiabilidad de la gestión de la propia entidad (que, en este ámbito, se ciñe a una pérdida de confianza en sus sistemas de seguridad) y de su prestigio. De este modo, a fin de evitar mayores pérdidas, prefieren "resolver" el problema internamente.

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

gar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país[11].

En cualquier caso, las diversas manifestaciones de conductas delictivas vinculadas a las tecnologías cibernéticas, cuyo rasgo definitorio y diferenciador es el de realizarse en otro espacio distinto a aquel en el que siempre se habían ejecutado las infracciones penales, han planteado importantes retos y desafíos jurídicos, frente a los cuales ya se han promulgado respuestas normativas, de ámbito estatal, comunitario e internacional. Ahora bien, la ciberdelincuencia conforma una delincuencia amplia, variada y cambiante, que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un preciso sector de la actividad social. Y es ese ámbito y su carácter innovador y mutante lo que determina una problemática particular de la misma que va a ser objeto de atención en esta obra, brindando especial atención a las novedades y cambios introducidos por la ley orgánica 1/2015, del 30 de marzo, por la que se modifica la ley orgánica 10/1995, del 23 de noviembre, del Código Penal. Solo mediante una comprensión global del fenómeno que identifique los caracteres comunes del evento criminal cometido en internet podremos mejorar la prevención de "la delincuencia del siglo XXI".

MOISÉS BARRIO ANDRÉS

[11] Ver BARRIO ANDRÉS, MOISÉS, *Internet de las cosas*, Editorial Reus, Madrid, 2018, p. 111 y siguientes.

ÍNDICE GENERAL

Prólogo a la segunda edición IX
Prólogo a la primera edición XI
Abreviaturas XXIII

CAPÍTULO PRIMERO

CARACTERIZACIÓN GENERAL

§ 1. Introducción 1
§ 2. Del delito informático al ciberdelito 5
§ 3. Los problemas jurídico-legales de la ciberdelincuencia 11
a) Un nuevo grupo de delincuentes cibernéticos 12
b) Problemas de persecución 14
1) El anonimato 15
2) Delitos a distancia y competencia territorial .. 21
c) Otros problemas 25
§ 4. Derecho comparado e internacional 26
a) Derecho comparado 27
b) Derecho internacional 28
c) El Convenio de Budapest sobre la ciberdelincuencia 28
d) Derecho de la Unión Europea 32
§ 5. Su tratamiento en el derecho penal español 35

CAPÍTULO II

CIBERDELITOS CONTRA LA INTIMIDAD Y EL DERECHO A LA PROPIA IMAGEN

§ 6. Introducción 43
§ 7. Descubrimiento y revelación de secretos 43
a) Tipo básico 43
1) Tipo objetivo 44
2) Tio subjetivo 47
3) Penas 47
b) Protección penal de datos personales 48
1) Tipo objetivo 53
2) Tio subjetivo 57
3) Penas 58
c) Revelación de secretos de origen ilícito 58
d) Tipos agravados 59
§ 8. Intrusismo informático e interceptación de las comunicaciones ("hacking") 60
a) Intrusismo informático 62
1) Tipo básico 62
2) Tipo objetivo 63
3) Tipo subjetivo 66
4) Penas 66
b) Interceptación ilegal de comunicaciones entre sistemas de información 66
1) Tipo básico 66
2) Pena 68
c) Delito de facilitación de herramientas informáticas dañinas 68
§ 9. Utilización no autorizada de imágenes previamente obtenidas con el consentimiento de la víctima en un lugar privado ("sexting" y "revenge porn") 70

CAPÍTULO III

CIBERDELITOS DE DAÑOS Y SABOTAJES ("CRACKING")

§ 10. Introducción 75
§ 11. Daños informáticos y sabotajes ("cracking") 76
a) Tipo básico de daños informáticos 77
1) Tipo objetivo 77
2) Tipo subjetivo 82
3) Pena 83
b) Tipos agravados 83
§ 12. Obstaculización o interrupción de un sistema informático 84
§ 13. Delito de facilitación de herramientas informáticas dañinas 86

CAPÍTULO IV

CIBERDELITOS CONTRA EL PATRIMONIO

§ 14. Introducción 87
§ 15. Estafa 88
a) Estafa genérica 88
b) Estafa informática 91
1) Tipo básico 91
2) Tipo objetivo 91
3) Tipo subjetivo 96
c) Estafa mediante utilización fraudulenta de tarjetas de crédito o débito o cheques de viaje 96
§ 16. Abuso de sistemas informáticos ("phreaking") 98

Capítulo V

CIBERDELITOS CONTRA EL HONOR Y LA LIBERTAD PERSONAL

§ 17. Introducción 101
§ 18. Calumnias e injurias 102
a) Calumnia 104
b) Injuria 106
§ 19. Ciberacoso ("cyberstalking") 108

Capítulo VI

CIBERDELITOS CONTRA LA LIBERTAD E INDEMNIDAD SEXUALES

§ 20. Introducción 113
§ 21. Pornografía infantil 114
§ 22. Delito de acercamiento y embaucamiento por medio de tecnologías de la comunicación ("child grooming") 115
a) Acercamiento 116
b) Embaucamiento para la obtención o exhibición de material pornográfico 117

Capítulo VII

CIBERDELITOS CONTRA LA PROPIEDAD INTELECTUAL Y DERECHOS CONEXOS

§ 23. Introducción 119

§ 24. Los delitos contra la propiedad intelectual 120
a) Tipo básico 123
1) Tipo objetivo 125
2) Tipo subjetivo 131
b) Penas 133
c) Exportación e importación 133
d) Tipo atenuado de distribución al por menor .. 134
e) Tipo agravado 134
§ 25. Páginas web de enlaces 134
§ 26. Supresión de las medidas de protección 137

CAPÍTULO VIII

CIBERTERRORISMO

§ 27. Introducción 139
§ 28. Delitos de terrorismo 141
§ 29. Ciberterrorismo 143

Conclusiones 147

Bibliografía 153