Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente(*)

Contemporary Criminological Studies (IX): Cybercriminology and the Profile of the Cybercriminal

Sergio Cámara Arroyo [1]

Sumario: I. La Cibercriminología como especialización. **II.** Teorías criminológicas explicativas de la ciberdelincuencia. **III.** El ciberdelincuente: algunas cuestiones generales. **IV.** El Ciberdelincuente: categorías y perfilado criminal. – Bibliografía.

Resumen: en el presente trabajo se ahonda en la nueva especialización de la Criminología en el estudio de las conductas delictivas cometidas a través el ámbito informático. Debido a la proliferación de comportamientos antisociales en el mundo online, pero con relación directa con el mundo real, nace el nuevo concepto de cibercriminología, cuya definición y nuevos desarrollos teóricos sobre la etiología del cibecrimen se exponen sucintamente en este estudio. Por último, se atiende al perfil criminal y principales características del ciberdelincuente, ofreciendo un catálogo de los diferentes grupos de hackers y subculturas criminales presentes en el ciberespacio.

Palabras clave: cibercriminología, ciberdelito, hacker, ciberespacio, cracker, transición espacial.

(*) Recibido: 07/03/2020 | Aceptado: 10/03/2020 | Publicación en línea: 01/04/2020.

[1] Prof. Dr. Derecho penal y Criminología UNED.
scamara@der.uned.es

Abstract: This work delves into the new specialization of Criminology in the study of criminal behaviors committed through the computer field. Due to the proliferation of antisocial behaviors in the online world, but with a direct relationship with the real world, the new concept of cybercriminology is born, whose definition and new theoretical developments on the etiology of cybercrime are succinctly set forth in this study. Finally, the criminal profile and main characteristics of cyber criminals are addressed, offering a catalog of the different groups of hackers and criminal subcultures present in cyberspace.

Keywords: cybercriminology, cybercrime, hacker, cyberspace, cracker, space transition.

I. La Cibercriminología como especialización

La Criminología, entre una de las conceptualizaciones posibles, puede ser definida como la ciencia empírica, de carácter inter y multidisciplinar holística del fenómeno criminal. Asumimos que, cuando se pretende hablar de conocimiento "holístico" del objeto de estudio de una ciencia, se va demasiado lejos. No obstante, no nos referimos a la omnisciencia de la Criminología en relación a su objeto de estudio, sino a la aspiración de la Criminología de estudiar y conocer cada realidad atinente al crimen, al delincuente, la víctima (ahora objeto de la Victimología, como ciencia autónoma), su prevención, control y tratamiento de forma interrelacionada y como un todo distinto de la suma de las partes que lo componen.

El estudio del fenómeno de la cibercriminalidad corresponde a la denominada parte especial de la ciencia criminológica, donde se ubican las llamadas "criminologías específicas" (HIKAL-CARREÓN, 2013 y 2016) o "criminologías alternativas" (FRANÇA, 2018), esto es, el estudio de una determinada sección de la realidad y su relación con la criminalidad, las tipologías delictivas, etc. Se trata de especializaciones por razón de la materia dentro del objeto de estudio de la Criminología.

El término cibercriminología o criminología informática es relativamente reciente y no está exento de cierta polémica doctrinal respecto al alcance de su significado. Son varios los autores que han tratado de definir esta especialización:

El término original se atribuye a JAISHANKAR, "padre fundador" de la cibercriminología, quien lo considera, con carácter general, un nuevo campo

académico, una subdisciplina de la Criminología, si bien posteriormente se referirá a la misma como una materia multidisciplinar que abarca diversos campos, tales como la Criminología, la Victimología, la Sociología, la Ciencia de Internet y las Ciencias de la computación. En sus publicaciones ha definido la cibercriminología como el estudio de la causa de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico. En esencia, la cibercriminología implica el examen del comportamiento criminal y la victimización en el ciberespacio desde una perspectiva teórica y criminológica (JAISHANKAR, 2007, 2010, 2011 y JAHANKHANI 2018). Según el autor, la elección del término y su utilización se debe dos razones: primero, el cuerpo de conocimiento que se ocupa de los delitos cibernéticos no debe confundirse con la investigación de los mismos y fusionarse con la ciencia forense cibernética (véase el apartado sobre la prueba electrónica); en segundo lugar, debe haber una disciplina independiente para estudiar y explorar los delitos cibernéticos desde la perspectiva de las ciencias sociales.

Otro de los investigadores que más ha ayudado a la expansión del término es KYUNG-SHICK CHOI (2015, 2017), coordinador del programa de investigación del cibercrimen de la Universidad de Boston, quien la identifica como la ciencia que busca estudiar las causas, factores y escenarios que permiten la materialización del cibercrimen o los delitos informáticos. Según el autor, su fin último es prevenir los delitos que se cometen en el ciberespacio o con acción de las tecnologías de la información y la comunicación.

En España, siguiendo a los autores anteriores, GONZÁLEZ GARCÍA (2016) la ha conceptualizado como una parte de la Criminología que tiene como objeto el estudio de la delincuencia y la conducta antisocial en el ciberespacio y sus implicaciones en el espacio real. La cibercriminología se ocuparía, por tanto, de conocer cómo influyen las actividades delictivas *online* en la vida *offline*.

En el ámbito iberoamericano, HIKAL-CARREÓN (2013), dentro de su teoría de las Criminologías especializadas, habla de la Criminología informática, definiéndola como aquella que "implica un estudio bastante extenso sobre la Informática (medios electrónicos) y las conductas antisociales que se dan por el uso de un sistema electrónico como medio de comunicación. La Criminología Informática es una rama de la Criminología General dedicada al estudio de las conductas antisociales y de los delitos informáticos (…). Pretende prevenir y combatir las cada vez más frecuentes conductas antisociales que se pueden realizar a través de medios informáticos". El componente de prevención inserto en la definición del profesor mexicano es, a mi juicio, importante pues, aunque puede parecer obvio, el estudio criminológico de la delincuencia informática tiene como principal pretensión

la detección y el adelantamiento a los delitos informáticos. Prescinde, sin embargo, el autor precitado, de uno de los componentes más importantes de la cibercriminología: la interrelación entre el espacio *online* y el mundo *offline*, de suma importancia en determinados delitos que se cometen a través de las nuevas TIC (como puede ser, por ejemplo, el ciberacoso).

Frente al concepto de cibercriminología, algunos autores han propuesto otras dimensiones criminológicas de estudio muy relacionadas con los cibercrímenes. Es el caso de la denominada *cyborgcriminology* o criminología ciborg, término acuñado por PÉREZ SUAREZ (2015, 2016), basado en el concepto de *cyborg* de HARAWAY (1991), entendido como un organismo cibernético, un híbrido de máquina y organismo, una criatura de la realidad social, así como una criatura de ficción que habría superado algunas limitaciones humanas asociadas con la realidad física.

Según el autor precitado, los postulados iniciales de la criminología *cyborg* serían los siguientes:

1) Se trata de una criminología especializada que considera el impacto de las tecnologías digitales en todas las facetas del comportamiento humano, y estudia la relación emocional forjada entre la humanidad y la tecnología digital (esencialmente Internet).

2) Considera las formas de delincuencia creadas por la proliferación de la tecnología digital y por la interfaz hombre / máquina, pero también conductas desviadas y / o actitudes disfuncionales, como, entre otras, adicción, obsesión, desigualdad (incluidas las desigualdades de género), desviación sexual, patología, suicidio, etc., que se producen en ese entorno digital (ciberespacio).

3) Incorpora una visión antropológica, filosófica, social, así como un discurso psicológico, sexual, crítico y cultural sobre la relación con las máquinas.

4) Tiene como objetivo desarrollar y probar teorías criminológicas para la explicación del delito cibernético teniendo en cuenta os postulados anteriores.

En definitiva, una criminología *cyborg* abordaría cuestiones más amplias que las generalmente discutidas por la cibercriminología y estaría en sintonía con el desarrollo cultural y tecnológico actual.

Aunque esta nueva teoría, basada en el interfaz hombre / maquina, pueda parecer cercana a los postulados de la ciencia ficción, supone una postura visionaría si se tiene en cuenta la amplitud que el fenómeno criminal puede tener en el ámbito de las nuevas ideologías o filosofías post y

transhumanistas. Esta clase de visiones futuristas, pero que ya tienen predicamentos actuales, pretenden que el ser humano transcienda a su realidad corpórea y física, convirtiéndose en datos informáticos para existir eternamente en el ciberespacio. Las implicaciones filosóficas, antropológicas y sociales son, por ahora, inimaginables (inmortalidad virtual, superación del género, nuevas formas de interrelación, nuevo concepto de "ser", etc.); más aún lo son para la ciencia criminológica: nuevas formas comisivas de delito, nuevas formas de desviación social, nuevo perfil criminal del ser digital, etc.

Así, por ejemplo, no han faltado autores que, con espíritu visionario, ya se han hecho eco de la problemática penal y criminológica que pueden suscitar algunas mejoras cibernéticas (*enhancements*) implantadas en el cuerpo humano. Buen ejemplo de ello serían los micro-implantes cerebrales electrónicos que podrían ser efectivos en la lucha contra algunas enfermedades neuromotoras así como para las funciones sensoriales (ROMEO CASABONA, 2013).

II. Teorías criminológicas explicativas de la ciberdelincuencia

A nivel teórico y empírico, la Criminología ha llegado tarde al estudio del fenómeno criminal de las nuevas tecnologías. La mayor parte de los desarrollos teóricos que se han realizado sobre los cibercrímenes han partido de la base de las teorías criminológicas tradicionales, fundamentalmente de las denominadas teorías totales o generales, esto es, aquéllas que pretenden dar una explicación unívoca a la génesis de cualquier tipo de delincuencia (SERRANO MAÍLLO, 2009).

Así, la Criminología ha tratado de explicar la etiología del cibercrimen desde las diferentes aproximaciones teóricas clásicas (PÉREZ SUÁREZ, 2015; CHOI, 2015; CHOI & TORO-ÁLVAREZ, 2017; CHOI, LEE & LEE, 2017; CICP, 2018):

1) la teoría del aprendizaje social y la asociación diferencial de SUTHERLAND y AKERS: esta teoría -o conjunto de teorías- parten de la base de que la comunicación con otras personas es fuente de aprendizaje. El delito también puede aprenderse mediante un proceso de asociación diferencial, esto es, un proceso en el que existen definiciones positivas de la conducta criminal, en detrimento de las definiciones negativas. Las nuevas tecnologías de la comunicación pondrían en contacto a los cibercriminales y al resto de usuarios en el entorno del ciberespacio (ambiente social virtual y asociación con cibercriminales), de lo que resultaría un proceso de contaminación criminógena (SKINNER & FREAM, 1997).

2) la teoría del control social, de los vínculos sociales y del autocontrol de GOTTFREDSON & HIRSCHI: para la teoría del autocontrol, el factor etiológico más importante de la delincuencia será la capacidad de un individuo para controlar sus impulsos y retener sus deseos (postponer las recompensas) (HIGGINS & MAKIN, 2004; HIGGINS, 2007). 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 (control social informal). Poniendo estas teorías en relación con el cibercrimen, la irrupción de las nuevas tecnologías de la comunicación podría haber coadyuvado a la destrucción de los vínculos sociales tradicionales en un mundo cada vez más conectado, pero, al mismo tiempo, con menos capacidad de comunicación real. El entorno de Internet, en el que la velocidad de obtención de información o recompensas es considerable comparada con el mundo físico, podría debilitar la capacidad de autocontrol de las personas. Por último, la escasa supervisión parental del uso de Internet en los menores de edad también ayudaría a la proliferación de comportamientos delictivos en el ciberespacio entre los más jóvenes.

3) la teoría general de la tensión de AGNEW: el crimen es producto de la frustración sufrida individualmente por ciertos estados afectivos negativos cuando el individuo "no es tratado como él o ella quiere". Existirían diferentes fuentes de tensión: la imposibilidad de alcanzar las expectativas sociales deseadas; la privación de estímulos positivos que el individuo ya tiene o espera poseer; estar sujeto a situaciones negativas ante las cuales no puede escapar. Teniendo en cuenta las frustraciones a las que un sujeto puede ser sometido en el mundo real, el cibercrimen, cometido en un entorno más "libre" como el ciberespacio, puede servir como vía de escape o superación de las tensiones. Las posibilidades del ciberespacio para reducir los medios de control social (*Deepweb*) son mucho mayores que las que pueden encontrarse en la realidad física. Además, esta teoría ha sido utilizada por algunos autores para demostrar la vinculación criminógena entre el ciberdelito y la realidad física; por ejemplo, en la generación de actitudes desviadas en jóvenes que habían sido víctimas de *cyberbullying* (BERGUER, HINDUJA & PATCHIN, 2015; HINDUJA & PATCHIN, 2007). El cibercrimen es, en consecuencia, generador de importantes tensiones que tienen su reflejo en el comportamiento en el mundo *offline* de quienes las sufren.

4) la teoría de las ventanas rotas (*Broken Windows*) de WILSON & KELLING o de la disuasión de ANWAR & LOUGHRAN: según la primera de las teorías, la inacción de los medios de control social ante la comisión de un delito redunda en la idea de desorden o decadencia social ("a nadie le importa"), lo que, a su vez, implica la comisión de nuevos hechos delictivos. El problema

de algunas tipologías de cibercrimen es que, además de no existir métodos eficaces para la detección del delito y la acción de la Justicia, tienen cierta aceptación social (por ejemplo, la piratería informática). La teoría de la disuasión pone el acento en el elemento de la percepción del riesgo de castigo por parte del delincuente. Según esta línea de pensamiento, los castigos deben ser fundamentalmente ciertos, severos y rápidos. Sin embargo, en el campo de la ciberdelincuencia la certeza del castigo no siempre es posible por diversos factores: espaciales, dificultad de identificación del ciberdelincuente, etc.

5) la teoría de las actividades rutinarias de COHEN & FELSON y de la oportunidad CLOWARD & OHLIN: estudiada en el apartado relativo a la cibervictimización, basta con recordar aquí que según la teoría de las actividades rutinarias, hay tres factores fundamentales que favorecen la victimización criminal: un ofensor motivado, víctimas propicias, y la ausencia de guardianes capaces de actuar contra una vulneración de la norma. Pues bien, dejando al margen la cuestión relativa a las víctimas, un espacio anonimizador y favorecedor de la impunidad como es el digital, en el que, además, pueden obtenerse muchos réditos producto de un comportamiento criminal, puede aumentar la motivación del potencial ofensor (que, incluso, puede ver su conducta como la superación de un reto en el ámbito de las nuevas tecnologías). Asimismo, las brechas de seguridad detectadas por los *hackers*, o la escasa vigilancia de los medios de control social formal de algunos de los derroteros de la red, suponen una relajación o ausencia de guardianes. Por otra parte, algunos estudios sugieren que la velocidad de Internet y el acceso a equipos informáticos, que son diferentes a escala mundial (brecha digital), tienen un impacto en las oportunidades de los delincuentes para cometer determinados ciberdelitos. YAR (2005), parte de la teoría de las actividades rutinarias, pero subraya las diferencias entre el mundo real y el mundo virtual, decantándose por una innovación tecnológica para poder salvar las diferenciaciones en los tres factores característicos de la teoría.

6) la teoría de las técnicas de neutralización: además de la negación de la víctima, invisibilizada en el entorno del ciberespacio (véase el epígrafe dedicado a la cibervíctima y a los procesos de victimación) o la creencia de ausencia de generación de daños, algunos *hackers* justifican sus conductas ilegales en Internet bajo la premisa de mejorar el propio sistema, la falta de necesidad de leyes reguladoras en el entorno libre del ciberespacio o el ataque al monopolio de las grandes corporaciones de *software*.

Sin embargo, el ciberespacio es una ubicación totalmente nueva que ha creado su propia criminalidad. Por ello, en los últimos años. Algunos autores

han tratado de dar respuesta a los porqués del cibercrimen a través de novedosas teorías creadas específicamente para el estudio de esta clase de delincuencia.

Algunas de estas teorías suponen simplemente la renovación de las premisas de las teorías tradicionales y su adaptación al ciberespacio, como es el caso de la *Situational Action Theory Revised for the Internet* (SAT-RI) o Teoría de la Acción Situacional revisada para Internet, que parte de la base de la Teoría de la Acción Situacional desarrollada por WIKSTRÖM (2010), estudiada específicamente para el contexto digital por PÉREZ SUAREZ (2015). En la SAT-RI el único entorno que se considera es Internet, como un contexto moral autónomo, no relacionado con el contexto moral fuera de línea. Se considera que Internet tiene su propio conjunto de valores morales y normativos por los cuales se regula a sí mismo (LESSIG, 2006). Por lo tanto, se considerarán solo las interacciones que ocurren cuando las personas entran en contacto con la red.

Básicamente, según la SAT-RI, la propensión individual al delito cibernético (P) debe ponerse en relación exponencial con la exposición (E) a Internet (entendida como un entorno criminógeno per se) y con las técnicas de neutralización (N) del usuario que, después de un proceso de deliberación moral (mediado por el autocontrol) podría resultar en la comisión de un cibercrimen (CC). La fórmula que resume la teoría podría significarse en la siguiente ecuación: P x E x N = CC.

Otro ejemplo de esta clase de teorías es la *Ciber Teoría de las Actividades Cotidianas* (Ciber TAC) y su *Modelo Estructural de Ciber TAC* (prevención) desarrollada por CHOI & TORO-ÁLVAREZ (2017), que parte de la base de la teoría de las actividades rutinarias a la que añade dos elementos:

a) Estilo de vida digital como factor importante de victimización, compuesto: a) actividades vocacionales (de trabajo) y de ocio en Internet; b) actividades arriesgadas de ocio en línea; y c) actividades vocacionales arriesgadas en línea.

b) Custodia digital eficiente, en forma de sistemas instalados de seguridad informática, que diferenciaría el nivel de victimización por delitos informáticos (guardián digital o virtual).

Otras teorías, sin embargo, parten de una nueva premisa desarrollada específicamente para la explicación del ciberdelito. Es el caso de la *Teoría de la Transición Espacial* de JAISHANKAR (2008), que pretende dar 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. Esta teoría integrada sostiene, en suma, que

las personas se comportan de manera diferente cuando se desplazan de un espacio a otro.

Las premisas de la teoría de la transición espacial se resumen en los siguientes puntos:

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. Según DANQUAH & LONGE (2011), esta premisa tiende a ser coherente con la noción de que la mayoría de los miembros de cualquier sociedad son honestos por el temor a ser atrapados (factor de disuasión). El ciberespacio, por otro lado, cambia la situación y deja espacio para ningún factor de disuasión. El anonimato puede usarse para representar alguna necesidad o emoción desagradable, a menudo abusando de otras personas; se puede usar para expresar honestidad y apertura que no podrían discutirse en un encuentro cara a cara.

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. Un buen ejemplo de lo primero es el comportamiento de los pedófilos que utilizan las TIC para embaucar a los menores y buscar un encuentro físico con ellos en el mundo físico; por otra parte, muchos comportamientos de ciberacoso y *cyberbullying*, que se originan en el mundo físico, terminan rompiendo la barrera espacial y se internan en el ciberespacio (GIL GIL & HERNÁNDEZ BERLINCHES, 2019).

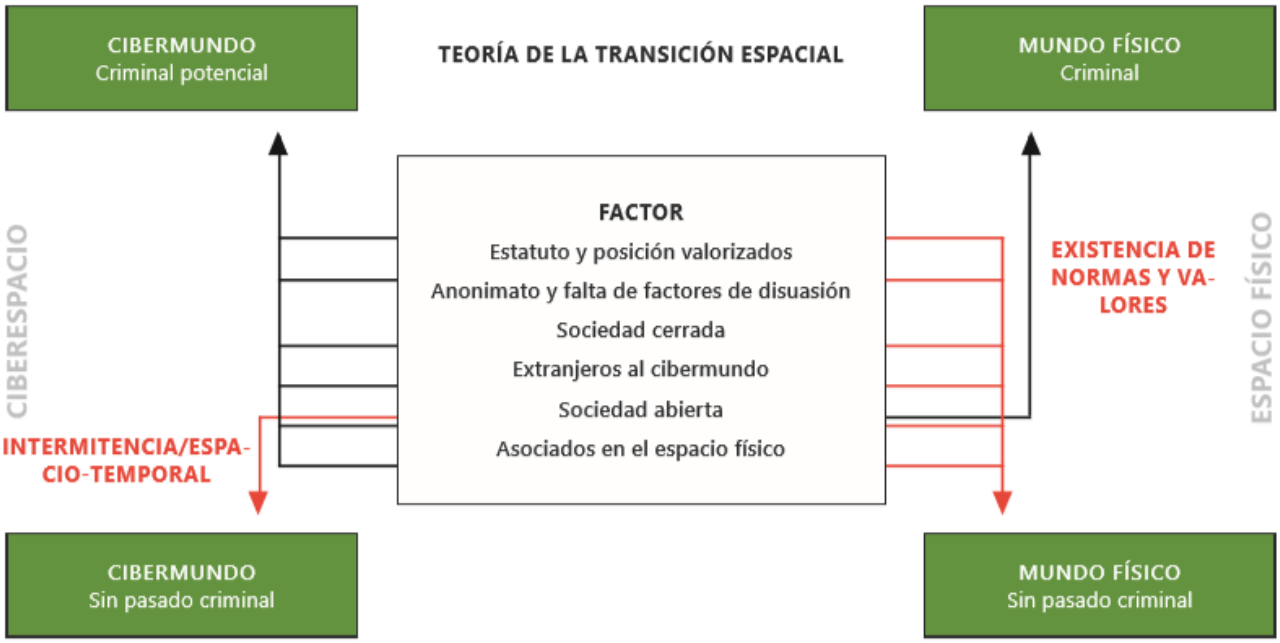
4. Las operaciones intermitentes de los delincuentes en el ciberespacio y la naturaleza dinámica espacio-temporal del ciberespacio ofrecen la oportunidad de escapar.

5. Es probable que los desconocidos se unan en el ciberespacio para cometer delitos en el espacio físico. Asimismo, es probable que los asociados en el espacio físico se unan para cometer delitos en el ciberespacio. Internet es un medio eficaz para el reclutamiento criminal y la difusión de técnicas criminales para personas de ideas afines. También se enfatiza que los individuos frustrados de las organizaciones pueden destruir el futuro de las compañías espiando, saboteando o filtrando información confidencial. Sin embargo, en la investigación empírica realizada por DANQUAH & LONGE (2011), se expone que "sin cuestionar el potencial de todas esas posibilidades, los hechos recopilados de las entrevistas indican que no

existen tales registros de extraños en el ciberespacio que se confabulan para cometer un delito en el espacio físico".

6. Las personas de una sociedad cerrada tienen más probabilidades de cometer delitos en el ciberespacio que las de una sociedad abierta. Esta premisa se basa en la creencia de que la mayoría de las personas de sociedades abiertas tienen la libertad de expresar sus sentimientos a diferencia de las personas de sociedades cerradas. Las sociedades de corte democrático, donde la libertad de expresión es uno de los pilares fundamentales, se identifican con esta definición. Así, el ciberespacio presenta invariablemente alguna forma de consuelo para las personas de las sociedades cerradas, de ahí la afirmación de que las personas de la sociedad cerrada tienen más probabilidades de cometer delitos en el ciberespacio que las personas de la sociedad abierta. Sin embargo, la evidencia empírica demuestra lo contrario, ya que hay muy poca o ninguna correlación entre las sociedades en las que residen los perpetradores y el tipo de delito cibernético que cometen (DANQUAH & LONGE, 2011). Esto puede deberse a que la perpetración del ciberdelito supone la ruptura de muchos de los valores contemplados en el mundo físico que, sin embargo, en la cultura del ciberespacio carecen de cauces de control adecuados. Probablemente el mundo *online* suponga una vía de escape para determinados individuos, pero no exista una correlación por oposición de valores con el mundo *offline* en este sentido.

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.



Fuente: Modelo de Transición Espacial derivado de JAISHANKAR (2008), por DANQUAH & LONGE (2011). CICP, 2018.

Finalmente, también la llamada Criminología plurifactorial se ha ocupado de las particularidades del ciberdelito. Se identifican, de este modo, los factores de riesgo de Internet que pueden derivar en la comisión de hechos delictivos (KOOPS, 2010, CICP, 2018):

1. *Alcance mundial de Internet:* 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 espacios de seguridad.

2. *Desterritorialización:* la ciberdelincuencia es esencialmente internacional, con retos importantes en términos de jurisdicción y colaboración internacional.

3. *Subcultura criminal en el ciberespacio* (HOLT, 2007)*:* el entorno digital permite la creación de redes flexibles y descentralizadas dentro de las cuales los delincuentes pueden organizarse para dividir el trabajo o compartir competencias, conocimientos o herramientas.

4. Anonimato a los delincuentes: 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).

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).

6. El entorno virtual facilita la manipulabilidad de datos y programas a un costo mínimo (SANDYWELL, 2010) 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. El entorno online permite la automatización de los procesos y conductas criminales: 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. Diferente escala criminal: 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", en la cual rodajas muy pequeñas apenas perceptibles, de transacciones financieras, se van tomando repetidamente de una cuenta y se transfieren a otra. 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. La información se convierte en un bien valioso en el ciberespacio, en los mercados legales e ilegales (WALL, 2007).

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).

12. 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.

III. El ciberdelincuente: algunas cuestiones generales

Desde una perspectiva criminológica, el estudio del sujeto que comete el delito reviste de una especial importancia para una adecuada política preventiva. Pese a que todo estudio criminológico debe tener en cuenta las circunstancias concretas del fenómeno criminal y de la persona del criminal, la identificación de "perfiles" puede ser una técnica eficaz para introducir políticas de seguridad y posterior identificación de los delincuentes. Por otra parte, el estudio de determinados tipos de comportamiento, asociados a perfiles socioeconómicos concretos, ha arrojado algunas conclusiones importantes en el campo de la prevención delictiva. Así, por ejemplo, estudios como el realizado por SHAW (2006), arrojan sugerentes postulados sobre el papel general de los patrones de comportamiento, pues en muchos casos estos formaron la base de la investigación para determinar y evaluar las conductas de los delincuentes cibernéticos.

Así, el estudio del cibercriminal puede ser relevante para comprender la naturaleza y el *modus operandi* que requieren los diferentes delitos informáticos, además de ayudar a la identificación de los autores cuando aún

son desconocidos para los medios de control social formal; incluso, teniendo en cuenta las especificidades de esta clase de criminalidad, el estudio de perfiles puede coadyuvar a la detección de los riesgos dentro de una persona jurídica o para comprender el funcionamiento de las organizaciones delictivas que se dedican a este tipo de delitos.

Como ya se advertía en el XIII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en 2015 (A/CONF.222/12), es probable que no exista un "perfil" estándar de ciberdelincuente. Esta poco halagüeña intuición nace de la propia naturaleza técnica, pero igualmente dinámica y constantemente innovadora de los denominados ciberdelitos: por un lado, su perpetración requiere de unos conocimientos cualificados en materia informática; por el otro, su versatilidad y el avance en la disponibilidad de las nuevas Tecnologías de la Información y la Comunicación (TICs), hacen posible que, al igual que los interfaz informáticos necesarios para su comisión, la realización de actos delictivos a través de medios telemáticos se encuentre, cada vez más frecuentemente, al alcance de cualquiera que sepa manejar –aunque sea de forma rudimentaria o a nivel "usuario"- un dispositivo. Más aún, es posible que las cualificaciones técnicas poseídas por algunos sujetos sirvan de puerta de entrada a otros con conocimientos mucho menores, que se aprovechan del trabajo ya realizado por los primeros para cometer hechos delictivos a través de medios informáticos. Esta suerte de cadena criminógena, en la que unos sujetos especialmente competentes -como principal rasgo criminológico a destacar- crean o generan oportunidades delictivas para otros menos capacitados, nos lleva a una importante problemática en el ámbito del perfilado criminal: el perfil del delincuente informático puede ser muy heterogéneo en cuanto a sus competencias en el medio informático.

En el precitado XIII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se exponía con claridad tal dificultad de identificación por la especialización del delincuente, advirtiéndose que "*un número relativamente reducido de programadores y piratas informáticos altamente cualificados pueden impulsar la innovación en el terreno de la ciberdelincuencia y ofrecer sus aptitudes como un servicio delictivo. Sin embargo, la facilidad de acceso a los exploits y los programas maliciosos implica que en muchos casos los autores ya no requieren conocimientos avanzados. Por otra parte, es posible que algunas formas de ciberdelincuencia dependan cada vez más de la presencia de un gran número de «soldados rasos»*". A tenor de la última expresión utilizada, se intuye que incluso puede existir cierta jerarquización entre ambos tipos de perfiles, siendo el *mastercode* el principal ideólogo de la ingeniería criminal

en el medio informático, que desarrollará, junto con un número mayor de personas con menores conocimientos técnicos que se limitarán a realizar tareas de programación de *software* de baja complejidad (picacódigos o *codemonkeys*), el acto delictivo completo. Finalmente, el producto informático obtenido podría ser utilizado por terceros para la comisión de nuevos hechos delictivos.

A mayor abundamiento, en ocasiones esta cadena criminógena no comenzará con los sujetos más cualificados o los creadores del *software*. Es posible una diversidad de actuantes, en la que no todos los que tienen una relación con el sistema informático o el programa utilizado como instrumento para delinquir, puedan ser considerados partícipes del delito. Teniendo en cuenta tal posibilidad, algunos sectores doctrinales han diferenciado entre diferentes tipos de actores: a) Los operadores, programadores u otros sujetos que acceden legítimamente a la elaboración del *software*; b) Cualquier sujeto, a través de las terminales públicas o interceptando las líneas de transmisión de datos a distancia; y, por último, c) Los titulares legítimos del sistema.

Junto con este primer escollo, existen otras numerosas dificultades tales como la singularidad del cibercriminales o su pertenencia a organizaciones criminales, el favorecimiento del anonimato en el ciberespacio, la clase social y profesión a la que pertenecen, la brecha de género en la delincuencia informática o la edad de los perpetradores, que hacen del delincuente informático todo un reto para los postulados clásicos de la Criminología y, en particular, de la técnica del perfilado criminal.

De ahí que algunos autores hayan afirmado que las clásicas técnicas de perfilado, basadas en los planteamientos de la Psicología criminal, sean insuficientes en el caso de la identificación de los cibercriminales, en la medida en la que si bien puede ser eficaz cuando la informática es el instrumento de la perpetración de los delitos –lo que requiere habitualmente, pero no siempre como hemos visto-, pero no cuando ésta es sólo el objeto de los actos delictivos (DE LA CUESTA ARZAMENDI & PÉREZ MACHÍO).

Para enfrentar todas estas dificultades, algunas voces en el campo de la Criminología apuntan a la necesidad de construir nuevos paradigmas teóricos que permitan explicar de manera más eficaz y efectiva este fenómeno criminal (YAR, 2006). Ante la amenaza que suponen los cibercrímenes en las sociedades actuales o tal vez recogiendo el testigo de estas recomendaciones por parte de la doctrina especializada, lo cierto es que en los últimos años se han desarrollado algunos estudios criminológicos interesantes para la construcción de un perfil de cibercriminal más exacto y depurado.

En España apenas se han realizado estudios relativos a la tipología y características del perfil criminal de los ciberdelincuentes. No obstante, según los datos del Sistema Estadístico de Criminalidad (SEC) del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad (PAYA SANTOS, CREMADES GUISADO & DELGADO MORÁN, 2017) respecto al perfil del ciberdelincuente, el 76% de los detenidos e imputados por este tipo de hechos son hombres, siendo especialmente partícipes en delitos sexuales (97%) y en interferencia en los datos y en el sistema (96%), mientras que en los delitos de falsificación informática y de fraude informático se registra una menor participación de estos (66% y 69%, respectivamente). Por otro lado, la nacionalidad de los detenidos e imputados es de forma mayoritaria española (85.7%), y entre los ciudadanos extranjeros partícipes de ciberdelitos, destacan los ciudadanos de Estados miembros de la Unión Europea (5.6%).

Paralelamente y de forma más global, un estudio realizado por *Digiware*, primer integrador de seguridad informática en América Latina, recopiló la información de sus centros de operación de seguridad informática (más de 13.000 dispositivos en diversos sectores), con el objetivo de analizar y prever las tendencias en seguridad informática para el 2016. Obtuvieron los siguientes resultados sobre el perfil socioeconómico del delincuente informático:

Se trata de una criminalidad joven, eminentemente masculina y con cierto grado de conocimientos: el 76% de los *hackers* son hombres cuyas edades están entre los 14 años (8%) hasta los 50 (11%), siendo la edad promedio es de 35 años (43%).

Estas cifras encajan con otras investigaciones que han llegado a la conclusión de que la carrera de un *hacker* –criminal o no- comienza a una edad bastante temprana (alrededor de 11 a 12 en los casos más precoces, aunque la mayoría comienza sus actividades clandestinas durante la adolescencia tardía, alrededor de los 13 a los 14 años de edad).

No es ninguna sorpresa que este tipo de criminalidad haya sido tradicionalmente asociada a la juventud. Si bien la informática en general cuenta con un desarrollo pretérito, las nuevas generaciones de usuarios han nacido en un entorno en el que el uso de las nuevas tecnologías se encuentra completamente normalizado y, más aún, podríamos decir sin empacho alguno que masificado en la mayor parte del mundo industrializado.

Habitualmente se suele hablar de menores víctimas de los delitos cometidos a través de las nuevas tecnologías de la comunicación. Sin embargo, en los últimos años también se ha evidenciado la tendencia de algunos menores a

ser también victimarios, es decir, autores de esta clase de delito (VIDAL HERRERO-VIOR, 2016). La razón, por lo demás, es bastante conocida: los jóvenes tienen un mayor acceso a esta clase de tecnologías y, además, muchos de los delitos que cometen los menores de edad tienen como víctimas a otros menores de edad, frecuentemente pertenecientes a su grupo social cercano.

Los menores suelen aparecer como autores de los denominados delitos informáticos en general, es decir, de los ilícitos realizados con el ordenador y que, en no pocas ocasiones, tienen como principal objetivo otro terminal.

El perfil habitual del "cibervándalo" o "*hacker* vándalo" suele ser el de un menor de edad temprana (alrededor de 14-15 años), varón y adicto a la utilización de medios de comunicación virtuales, con conocimientos –frecuentemente autodidactas y limitados- de informática y manejo de programas maliciosos (CÁMARA ARROYO, 2015). Normalmente actuará mediante el uso de herramientas secundarias, esto es, programas no creados por él mismo. Se siente atraído por un imaginario sentimiento dignificación derivado de la visión romántica de los *hackers*, a los que se ha conferido cierta fama y reconocimiento. La escasez de riesgos, la versatilidad del entorno virtual *online* y el anonimato que confieren las nuevas tecnologías son idóneos para sus actividades.

Actualmente, el espacio criminógeno más habitual utilizado por los jóvenes son las Redes Sociales y las nuevas TICs (teléfonos móviles, tablets, etc.). Los delitos más frecuentes cometidos por estos menores son los que atentan contra la propiedad intelectual (piratería), la tranquilidad y la libertad (amenazas, injurias, calumnias, ciber acoso o ciber *bullying* y ciber acecho o ciber *stalking*), la intimidad (descubrimiento y revelación de secretos), y la indemnidad sexual (*sexting*).

En cuanto a la necesidad de cualificación técnica en materia de programación o telecomunicaciones, el estudio arrojaba algunos datos interesantes: en la mayor parte de los casos, se trataba de personas que tienen un mediano o alto conocimiento de computadores y redes en general, así como de sujetos con conocimientos en cómputo por encima del promedio (cambio de IP, uso de programas *Keyloggers*, uso de navegadores inusuales, etc.). Como puede apreciarse, no se hace mención al conocimiento técnico de confección de herramientas informáticas para la comisión de hechos delictivos, sino que el estudio se centra en el conocimiento acerca del mero "uso" de las diferentes vías que permiten la comisión de cibercrímenes.

Y es que, como han advertido algunos organismos internacionales, actualmente la comisión de una gran parte de esos actos no requiere

competencias ni conocimientos tecnológicos avanzados (UNODC, 2013). Cualquier individuo medio con una conexión a Internet puede desarrollar una actividad delictiva o criminal. Lo que se requiere en la generalidad de los casos, es el conocimiento necesario para utilizar tales herramientas.

En el mismo sentido, la investigación realizada por FANJUL FERNÁNDEZ y la *ESERP Business School* ha concluido que, para la comisión de un delito informático, si bien se requieren de unos conocimientos mínimos relacionados con el medio informático, en general, los sujetos activos de los mismos no precisan conocimientos técnicos cualificados, bastando con un coeficiente intelectual medio y la oportunidad para delinquir.

Basándose en esta premisa inicial, los investigadores clasifican de manera general a los ciberdelincuentes en dos grandes categorías o bloques, a las que se adscribirán posteriormente otras categorías o perfiles criminales:

a) Aquellos que manejan con facilidad los ordenadores y son expertos conocedores de los sistemas en red; y

b) aquellos cuyos conocimientos y habilidades no podrían ser categorizados en el nivel de expertos.

El primero de los perfiles generales es mucho más especializado y atiende fundamentalmente a la confección de herramientas informáticas y posterior comisión de delitos informáticos, mientras que en el segundo bloque la tecnología es un medio o vehículo para cometer el delito.

Por estas razones, los investigadores precitados advierten que el perfil concreto de ambos será "diametralmente opuesto": en el primer caso estaremos ante un sujeto con competencias y aptitudes informáticas más especializadas, para quien el móvil principal del hecho delictivo puede ser el mero reto de mejorar en la adquisición de conocimientos específicos; el segundo tipo es mucho más pragmático, siendo un mero usuario de las nuevas tecnologías para fines ilícitos y su motivación podrá ser muy heterogénea pero menos elevada que en el primer supuesto, abarcando desde la venganza personal, la posibilidad de obtener algún beneficio económico, la excitación sexual, etc.

Además, como puede observarse también se aprecia una diferencia fundamental en cuanto a la focalización del ataque: el perfil especializado tendrá como objetivo principal el propio aspecto virtual, el sistema de información en sí mismo o los programas que se encuentran en él, a través de los que accederá a los datos que necesita para perpetrar el delito y conseguir los fines delictivos que se haya propuesto; por el contrario, el asalto realizado por el perfil menos técnico tendrá una relación menos

intensa con el ámbito informático, siendo la tecnología un mero instrumento para llegar al verdadero objetivo. Dicho de otro modo, para el perfil especializado el objetivo es tanto el ataque informático en sí mismo, lo que ya supone alcanzar la finalidad de resolver el reto que le plantea la vulneración de los sistemas de seguridad informática o la confección un *software* malicioso, como los posibles réditos de su conducta delictiva; para el perfil menos cualificado, el éxito del ataque no es un fin en sí mismo puesto que habitualmente se lleva a cabo mediante medios menos expeditivos o aprovechando la tecnología ya confeccionada (no supone la consecución de ningún reto), sino un mero medio por el que se alcanza el verdadero objetivo perseguido.

Con todo, algunos autores, como ROGERS (1999), proponen una clasificación basada en los objetivos y habilidades en el uso de la tecnología de los cibercriminales:

- *Toolkit/newbies* (literalmente kit de herramientas y novatos) y *scriptkiddies*: neófitos en el uso de la tecnología, con algunas habilidades técnicas y conocimientos muy bajos; suelen utilizar un *software* ya preparado.
- *Cyberpunks*: capaces de escribir programas pequeños, que utilizan principalmente para alterar páginas web, enviar correos spam, realizar actos vandálicos en el ciberespacio, etc.
- *Internals*: empleados o ex empleados de una organización o empresa. Dañan el sistema de la compañía por venganza. Sus ataques no se basan en habilidades técnicas, sino en su conocimiento preciso del nivel y tipo de seguridad presente dentro de la organización.
- *Coders* (codificadores): que escriben códigos destinados exclusivamente a dañar otros sistemas.
- *Old-guard hackers*: piratas informáticos que siguen los preceptos de la primera generación de *hackers*, también llamados *true hackers* o piratas informáticos auténticos, altamente calificados, sin intención criminal, que abrazan un código de comportamiento en el mundo virtual.
- *Professional criminals* y *cyberterrorists*: son las categorías más peligrosas, tratándose de *crackers* con elevados conocimientos y especializados en espionaje industrial y operaciones de inteligencia contra gobiernos, agencias de seguridad nacional, etc.

Posteriormente, el mismo autor (2006) propuso una tipología híbrida, basada tanto en las motivaciones de los *hackers* como en sus capacidades técnicas, identificando hasta nueve grupos diferentes de cibercriminales:

- El novato, que es el neófito que usa herramientas automáticas y busca hacerse un nombre.
- El *cyberpunk*, ligeramente superior al novato, que tiene algún conocimiento de programación y busca fama y dinero.
- El iniciado, que ataca a su empleador desde dentro para vengarse.
- 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.
- El programador de virus.
- El pirata de la vieja escuela que heredó la mentalidad de los piratas mayores y que busca La estimulación intelectual.
- El criminal profesional especializado en la criminalidad informática que busca beneficios económicos.
- El guerrero de la información cuyo objetivo es desestabilizar los centros de toma de decisiones y que está motivado por el patriotismo.
- El activista político.

Predominio de la criminalidad grupal u organizada: los ciberdelincuentes ya no actúan de manera individual, sino que operan como parte de grandes organizaciones criminales. El 50% de las bandas dedicadas al cibercrimen se componen de 6 o más personas. El 50% de los grupos de ciberdelincuentes han operado por más de seis meses, mientras que el 25% ha operado seis meses o menos. La mayor parte de su actividad se registra en Norteamérica y Sudamérica con un 19% del total de ataques generados a nivel mundial.

En líneas generales, puede compartir la idea expresada por algunos estudios sobre el perfil del pirata informático de que entre ellos existe un fuerte vínculo con la tecnología, que consideran una vía de escape, una puerta a nuevos retos interesantes e inesperados (versus la gris realidad) e, incluso, un modo de obtener un poder al que no accederían en el mundo físico. Otra característica importante para entender el pensamiento del *hacker* es la idea de secretismo y anonimato (que puede llevar a la impunidad por la comisión de un delito), de pertenencia a una subcultura *underground* "única", que se desarrollaría en el ciberespacio y que trae consigo un desdoblamiento no patológico de personalidad (la virtual –que, además, puede ser múltiple- y la física), una relajación o cambio de valores y moralidad tradicionales en el ciberespacio (desinhibición *online* o separación moral), así como una ambivalente necesidad de mantener en secreto los actos ilícitos y la necesidad de compartirlo con el grupo de iguales o los medios en busca de

reconocimiento. Respecto a este último punto, si bien es frecuente la existencia de comunidades online a las que el *hacker* puede pertenecer, lo más habitual es que estemos ante una suerte de membresía fluida: el ciberespacio es más una red informal que una organización formalmente establecida, por lo que sus fronteras son bastante permeables, y la naturaleza de este tipo de red conduce a un alto nivel de rotación.

La mayor parte de los estudios criminológicos realizados sobre el perfil del cibercriminal coinciden en el eminente predominio masculino. Se ha llegado a afirmar que "la masculinidad y la juventud son dos factores que explican la piratería" (TAYLOR, 1999). En cuanto a la breca de género y el fenómeno de la cibercriminalidad, varios factores pueden explicar este aspecto: el tipo de socialización primaria que enseña a los hombres y a las mujeres una actitud diferente hacia la tecnología; diferencias en la capacitación; e, incluso, un sesgo de género en el lenguaje informático. Después de la década de 1990, sin embargo, la presencia de mujeres (denominadas *hackse*) comenzó a aumentar progresivamente y se hizo más y más relevante.

En general, puede afirmarse que hay una falta de investigación empírica sobre las características de los delincuentes cibernéticos. Además, los estudios que se han realizado tienen limitaciones graves y se centran en un número concreto de delitos. No se sabe, si los delincuentes cibernéticos tienen características diferentes a los delincuentes tradicionales, y no se sabe si las características de los delincuentes interactúan con los motivos y la ejecución de ciertos delitos informáticos y cómo lo hacen (LEUKFELDT, 2017).

En cuanto a la prevención en materia de delincuencia informática en el interior de las corporaciones, el estudio daba algunas pautas sobre las características de los trabajadores susceptibles de perpetrar ataques informáticos:

- Personas que aprovechan espacios sociales para preguntar por datos de clientes y demás información de uso restringido.
- Personal que instala programas espías sin autorización.
- Sujetos que desactiva el software antivirus en su equipo de trabajo.
- Personas que hacen uso sin autorización de computadoras o dispositivos de los demás miembros de la organización.
- Empleados que se quedan a trabajar en horario extra en la oficina sin dar justificación.

Aunque el estudio se centra en la delincuencia informática dentro de las organizaciones, lo cierto es que ya advierte una pauta interesante sobre las

características socioeconómicas del cibercriminal: a menudo nos encontraremos con personas que ostentan un perfil alejado de la marginalidad y la exclusión social. Al margen de la actual disponibilidad y accesibilidad a esta clase de medios comisivos, la sola idea de acceso a un sistema de información o terminal para poder perpetrar el cibercrimen ya es un elemento social, económico y cultural de suma importancia.

En este sentido, hay que tener en cuenta la importancia de la denominada brecha digital en las oportunidades de cometer esta clase de hechos delictivos. A pesar de la universalización del uso de Internet y de los medios telemáticos de comunicación, el acceso al ciberespacio es fuente de numerosas desigualdades. Ahondando un poco más en esta cuestión, no solamente existe una primera brecha digital en cuanto al acceso a las nuevas tecnologías que se focaliza en las diferentes áreas geográficas, sino que también existen una segunda y tercera brechas digitales que configuran respectivamente las desigualdades en las competencias y en el uso de tales tecnologías (CENTRO INTERNACIONAL PARA LA PREVENCIÓN DE LA CRIMINALIDAD, 2018).

De esta manera, algunos autores se han aventurado a realizar un perfil geográfico del ciberdelito y su autor, el cibercriminal, distribuyendo las tipologías delictivas pertenecientes a esta categoría por regiones y perfiles de delincuente informático.

En una investigación publicada en 2016, KIGERL, propone una reveladora tipología de lo que él llama los "países de la ciberdelincuencia". Teniendo en cuenta los datos de los organismos oficiales de los países implicados en la investigación, así como los informes de las principales empresas internacionales de seguridad cibernética, el autor identificó distintos 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.

Aunque existen *hackers* de todos los grupos étnicos y nacionales, el resultado fue la clasificación en cuatro grandes grupos de países:

Grupo 1: países con escasa participación en la ciberdelincuencia, tratándose en de los países más afectados por la denominada 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.

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.

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*.

Haciéndose eco de esta investigación, el Centro Internacional para la Prevención de la Criminalidad (CIPC) de Montreal (Canadá), principal organización en materia de prevención del delito a nivel internacional, realizó su propio estudio tratando de identificar las dinámicas específicas y los temas clave para cada una de las principales regiones del mundo. Sobre las especificidades genéricas del perfil criminal dividido en las distintas regiones geográficas, cabe destacar de su estudio la siguiente información:

- África: la región en la que la actividad delictiva cibernética está creciendo más rápidamente. Sin embargo, la participación de África al respecto en el escenario mundial sigue siendo limitada. Sudáfrica, Nigeria y la región del África septentrional difieren de otros países africanos en su dinamismo en materia de ciberdelincuencia.
- El crimen organizado latinoamericano ha ocupado masivamente el ciberespacio.
- La situación asiática dista mucho de ser homogénea, especialmente en términos de volumen de usuarios, tasas de penetración y nivel de desarrollo económico. 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. 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. China es un punto focal en el panorama asiático de la ciberdelincuencia, tanto como fuente de actividades ilícitas como en términos de victimización.

- 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. Los Estados Unidos son una pieza absolutamente esencial del panorama mundial de la ciberdelincuencia en tres aspectos principales: desde el punto de vista de la delincuencia; de la victimización; y de las respuestas.
- Rusia ha desarrollado un sistema particularmente exitoso de convergencia y colaboración entre el medio de la ciberdelincuencia y el gobierno.
- En Europa ha crecido el sentimiento de inseguridad y la preocupación por el ciberdelito en los últimos cinco años; sin embargo, la prevalencia de estos crímenes sigue siendo baja y su aumento es débil en la región.

IV. El Ciberdelincuente: categorías y perfilado criminal

Una vez realizadas estas precisiones sobre las dificultades y especialidades de la confección de un perfil criminal genérico para los cibercriminales, conviene realizar a continuación una relación de las diferentes categorías de perfiles criminales a los que la doctrina penal y criminológica ha dedicado sus investigaciones (DE LA CUESTA ARZAMENDI & PÉREZ MACHÍO, 2010; FANJUL FERNÁNDEZ ET AL., 2018; MIRÓ LLINARES, 2012; PÉREZ SUÁREZ, 2015; CHIESA, DUCCI & CIAPPI, 2009):

1. Cibercriminales especializados:

a) Hacker: en primer lugar, es necesario realizar una importante precisión: no debe confundirse el término *hacker* con el concepto amplio de cibercriminal o ciberdelincuente. Por cibercriminal o ciberdelincuente entendemos a todo sujeto que perpetra un hecho delictivo utilizando como parte central el ciberespacio, a través de las nuevas tecnologías informáticas o de telecomunicaciones. Un *hacker* puede pertenecer a una categoría dentro de los cibercriminales, pero no siempre cuando estemos ante un *hacker* podremos etiquetarle como cibercriminal.

Ciertamente, el *hacker* fue el pionero de las primeras formas de cibercriminalidad, centradas en el acceso a la información en sistemas informáticos. El término *hacker* proviene de finales de los años 50 y se debe a la proliferación de un experto grupo de programadores que conseguían eliminar programas que se encontraban ubicados dentro de un sistema

operativo (*true hackers*). Sin embargo, tales prácticas no tienen por qué tener un cariz socialmente negativo o criminológicamente relevante.

Actualmente, el vocablo *hacker*, sin mayores precisiones, simplemente hace referencia a un sujeto cualificado o grupo de expertos en informática y redes, lo que incluye el dominio de áreas como la programación, *hardware* y *software*, las telecomunicaciones, etc[2]. Por otra parte, existe un concepto de *hacker* mucho más estricto, que se refiere a aquel experto en informática que busca superar barreras por el mero hecho de su existencia, sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para la mejora de la seguridad de las redes y los sistemas.

Además de ello, el *hacker* estaría especialmente interesado en la brecha de seguridad de los sistemas de información y en los porqués de las vulneraciones de dichas medidas de seguridad informática. En principio, un hacker puede dedicar sus conocimientos a intervenir o realizar alteraciones técnicas en sistemas informáticos tanto de signo socialmente positivo como negativo. Más aún, hoy en día muchos *hackers* se adscriben a su propio código de "moralidad en el mundo virtual" o *ética del hacker*, esto es, una especie de decálogo o manifiesto al que se adscriben para evitar que proliferen las conductas delictivas en su seno (CARRETERO SÁNCHEZ, 2017). En este sentido, los cibercriminales pertenecientes a la categoría de los *hackers* se configurarían como una subcultura criminal dentro de una subcultura, pues se oponen a unos valores propios de un círculo minoritario que, a su vez, ha construido su propio conjunto de directrices al margen de los valores del mundo físico.

Algunas de las características genéricas de esta clase de escala de valores compartida por el grupo de los *hackers* –independientemente de que perpetren o no hechos delictivos-, puede ayudar al criminólogo a comprender mejor su personalidad y sus motivaciones:

Los *hackers* son verdaderos adeptos virtuales, creyentes convencidos de los beneficios de las nuevas tecnologías en el espectro social. En general, consideran los avances en el campo de la informática, las redes y las telecomunicaciones como algo universalmente positivo o "bueno en sí

[2] Es lo que se ha denominado *hacker* en sentido amplio, entendiendo como tal cualquier persona con conocimientos informáticos que realiza alguna actividad ilícita, o simplemente no autorizada, en el ciberespacio. En esta categoría general querían incluidos un sinfín de términos relacionados con comportamientos delictivos concretos que, en realidad, no son demasiado útiles para el estudio del perfil criminal: *crackers, phreakers, pirates, pranksters, malicious hackers, personal problema solvers, career criminals, extreme advocates, scriptkiddies, cyberpunks, hacktivists, virus writers, professionals y cyber-terrorists, spammers, snoopers, spoofers, sniffers*, etc. (MIRÓ LLINARES, 2012).

mismo". En este sentido, entienden que estos nuevos adelantos pueden ayudar a la mayor parte de la población mundial, reducir las desigualdades y favorecer el intercambio libre de información conectando a la gente de manera ilimitada. Por otra parte, consideran que la informática es un campo abonado para la creatividad, el arte y la belleza. En ocasiones llegan a definir su identidad a través de los programas que crean o por sus "*hacks*", convirtiéndolos en signos de identidad más importantes que otros rasgos biológicos, sociales o psicológicos. En consecuencia, consideran todo avance en su área de conocimientos como un reto intelectual capaz de motivarles más que las recompensas tradicionales (aceptación social, patrimonio, etc.).

Como contrapartida, la mayor parte de los *hackers* considerarán un agravio cualquier limitación a la utilización de las nuevas tecnologías. En este sentido, es frecuente que la mayor parte de ellos sienta una fuerte desconfianza hacia la autoridad, a la que se verá como un interventor de corte represor.

Por el contrario, en su actuar, los *hackers* tradicionales suelen considerar que lo importante de sus actividades –aun aquellas al margen de la legalidad tradicional- es evidenciar cualquier falla de un sistema de información, por lo que en muchas ocasiones desarrollan su actividad publicitándola (aun cuando no ha sido solicitada por el propietario) y ofreciendo posibilidades de solución.

Todas estas consideraciones son especialmente relevantes desde las nuevas teorías criminológicas que estudian la moralidad como factor relevante en la génesis del fenómeno criminal (BIRBECK, WIKSTRÖM). Por otra parte, también es interesante el hecho de que la actual configuración de los medios de control social formal haya derivado en una hipercriminalización de la actividad *hacker*, toda vez que se tiene por delictivo cualquier intrusismo en un sistema de información ajeno independientemente de la finalidad con la que se realice y sin que sea necesaria la capación o dañado de datos.

Del mismo modo que no existe un perfil genérico de cibercriminal, no existe un único perfil de *hacker*. Así, la doctrina ha realizado diferentes clasificaciones:

Según su filosofía o conforme al seguimiento o rechazo de las premisas de la anteriormente mencionada ética del *hacker*, algunos autores distinguen entre:

White Hat Hackers, o *hackers* de sombrero blanco, son los encargados de la seguridad de los sistemas informáticos, dedicados a estudiar y fortalecer las

brechas de seguridad o errores (*bugs*) en los mismos. Su actividad es inocua desde una perspectiva criminológica (lo que no necesariamente significa que no sea delictiva formalmente para algunos sistemas de control social formal) y busca básicamente la mejora del sistema. A pesar de la imagen mediática del *hacker* asocial o carente de habilidades sociales, los hackers de este tipo son bastante activos en las Redes Sociales, pertenecen a comunidades de la Red y se adscriben a un código de conducta en sus relaciones interpersonales *online* (*nettiqueta*), con las que frecuentemente intercambian ideas, datos y herramientas. Los *Grey Hat Hackers* (sombrero gris), se dedican a traspasar los niveles de seguridad de los sistemas informáticos y ofrecer sus servicios como administradores de seguridad. Su finalidad no es delictiva, aunque tampoco es altruista como en el caso de los *White Hats Hackers*, sino que se encuentra encaminada a conseguir mayores réditos profesionales. Finalmente, los *Black Hat Hackers* (sombreros negros), encajan materialmente con el concepto de cibercriminal, puesto que se dedican a vulnerar la seguridad de sistemas, realizar intrusiones no autorizadas e ilegales a sistemas privados con intenciones delictivas: descubrir, revelar, apoderarse o dañar datos. Para ellos, violar un sistema de información y extraer sus secretos, robar la información y venderla fuera es un comportamiento normalizado.

b) Cracker, phreakers y cyberpunks: dentro de esta última categoría -los *Black Hat Hackers*- se encuentran los *Cracker*, término acuñado por los propios *hackers* a finales de los años 80 del siglo pasado para diferenciarse de aquéllos que realizaban acciones dañinas o delictivas a través del *hacking*. Originalmente, *cracker* era aquel sujeto que que eliminaba la protección de programas de *software* comerciales (esto es, los *crackeaba*). Actualmente, los *crackers* son *hackers* que realizan actividades con fines maliciosos, destructivos (*crack* significa romper) o criminales modificando el comportamiento de sistemas y redes. Según algunas investigaciones, su motivación suele ser económica o de mero reconocimiento, y sus rasgos de la personalidad encajarían con las del ególatra (obsesivos y afán destructivo e insaciable). A menudo han mantenido algún tipo de relación con sus víctimas –físicas o jurídicas- en el mundo físico o virtual, por lo que conocen perfectamente el entorno virtual en el que se mueven. A diferencia de otros grupos de *hackers*, los crackers no se adscriben a ningún tipo ética propia del ciberspacio y suelen ser especialmente esquivos, relacionándose en grupos pequeños de difícil acceso.

Dentro de los *crackers* se han diferenciado, a su vez, algunas subcategorías, fundamentalmente basadas en los recursos a los que pueden acceder o a las actividades concretas que realizan, sin que se aporten, en la mayor parte de

los casos, rasgos relevantes que ayuden a la identificación de su perfil: *crackers de sistemas*. *programadores* y *decoders* que alteran el contenido de un programa; *crackers de criptografía* (*crackear* códigos), *crackers de carding*[3] (uso ilegal de tarjetas de crédito), *crackers de trashing* (basureros, obtienen la información de las papeleras de reciclaje), etc.

Quizás las únicas dos subcategorías de *crackers* que aportan algo más de información de cara a la confección de un perfil criminal son los *phreakers* o *phreackers*[4], especializados en los sistemas de telefonía fija y móvil, redes móviles, datos de usuarios, etc. También tienen conocimientos de *hardware* y electrónica, lo que les permite construir o manipular equipos que interceptan o realizan llamadas desde teléfonos móviles sin la aquiescencia de sus propietarios. Aunque en un primer momento sus actividades estaban motivadas por el mero conocimiento, actualmente su motivación es fundamentalmente económica con tintes activistas. Así, muchos de sus ataques tienen un trasfondo reivindicativo, lo que lleva a la comisión de delitos dirigidos contra las empresas de telefonía y las grandes multinacionales, organizaciones que, bajo su punto de vista, estafan a sus clientes con facturas desmesuradas y servicios insuficientes. A diferencia de los *hackers*, que se guían por su búsqueda de un mayor conocimiento, su motivación es "extrínseca", normalmente basada en motivos económicos. Tampoco se encuentran constreñidos a ningún tipo de etiqueta en el mundo virtual, aunque a diferencia de otros subgrupos de *crackers* suelen mantener importantes valores de justicia distributiva (consideran que las grandes multinacionales de telefonía móvil son un sistema fraudulento que abusa de la población).

Una categoría especialmente paradigmática dentro de los *crackers* son los denominados *Cyberpunks* (HAFNER & MARKOFF, 1995). Esta categoría, que toma su nombre de una subcultura ficticia perteneciente a un subgénero de la ciencia ficción[5], destaca por la inclusión de valores culturales propios de

[3] El denominado "fraude en el número de tarjeta de crédito" o *carding*, es una técnica que consiste en apropiarse de los números de tarjetas de crédito, que generalmente se obtienen al violar los sistemas informáticos de los bancos o agencias financieras, y usarlos para hacer llamadas de larga distancia o para comprar productos sin el conocimiento del titular de la tarjeta.

[4] Algunos autores, como DE LA CUESTA ARZAMENDI & PÉREZ MACHÍO no incluyen a los *phreakers* dentro de los *crackers*, si bien admiten que "en el resto de los aspectos son muy similares" a ellos.

[5] La contracultura cyberpunk surge del movimiento de literatura de ciencia ficción encabezado por autores como Sterling, Gibson y John Shirley durante la década de 1980 en el seno de la literatura de ciencia ficción, siendo empleado por primera vez en ese sentido por Gardner Dozois en 1984.

la cultura *punk*, una visión distópica o negativa de la realidad y el sistema representada por la máxima "*low life, high tech*" (literalmente "bajo nivel de vida, alta tecnología"). Paradójicamente, aunque se trata de sujetos muy apegados a las nuevas tecnologías y que, de hecho, las utilizan para perpetrar fundamentalmente actos vandálicos y destructivos en el ciberespacio, también se muestran como un movimiento contracultural que siente una especial desconfianza ante el *uso* de los avances informáticos. No se trata, en este aspecto, de un movimiento reaccionario que proponga la vuelta a viejos valores, sino de una corriente que advierte –muchas veces a través de sus acciones delictivas- de los peligros de los aspectos más polémicos de la tecnología. Fundamentalmente, los *cyberpunk* contraponen la necesidad del progreso tecnológico con el proceso de eventual deshumanización que pueden acarrear. Otro problema denunciado por la cultura *cyberpunk* sería la utilización de estas nuevas tecnologías por parte de los poderosos como herramienta de exclusión o marginación social.

Ciertamente, en este último aspecto, coincidimos con algunos autores (PÉREZ SUÁREZ) que advierten que el estudio de los cibercrímenes y sus perpetradores, los cibercriminales, se ha realizado desde una óptica sesgada por parte de la Criminología, sin atender a todas las áreas de impacto de las tecnologías digitales en cada una de las facetas del comportamiento humano. A menudo se olvida el estudio de la relación emocional forjada entre la humanidad y tecnología digital (interfaz hombre/máquina).

La cultura *cyberpunk* se caracteriza también por una estética determinada, mezcla de anacronismos estéticos propios de la imagen *punk* y *heavy* de los años 80 y 90, así como composiciones futuristas en la vestimenta y ornamentos utilizados. La confluencia de los estilos *underground* del pasado reciente con el uso de las nuevas tecnologías es el sello distintivo que permite diferenciar a los *cyberpunk* de otros tipos de *crackers*. En cuanto a sus actividades y perfil personal, se caracterizan por comenzar sus acciones a una edad temprana, una menor sutileza en sus ataques informáticos y la afinidad con las redes en línea. En ocasiones han sido definidos como "vándalos de páginas web o sistemas informatizados". Aunque se muestran mucho más propensos al puro nihilismo que otros grupos de *crackers*, muchos *cyberpunk* se oponen al sistema económico de las grandes corporaciones a través de sus ataques informáticos. Comparten, en este sentido, algunos objetivos comunes con los *hacktivistas* y los *phreakers*, si bien sus acciones suelen ser menos sutiles o centradas en la lucha contra los poderosos.

c) Viruckers: los creadores de virus informáticos reciben el combinado pseudónimo de *viruckers* (término que no se utiliza en la lengua

anglosajona). Su especialidad es, por tanto, la fabricación de programas (*malware*) que permiten la intrusión en otros sistemas informáticos o la destrucción y alteración de datos (daños informáticos). Su *modus operandi* consiste en introducir un virus informático en un sistema para destruirlo, alterarlo o inutilizarlo. Normalmente un virus informático es capaz de "contagiar" otros programas o sistemas. En cuanto a sus rasgos de personalidad, les caracteriza su carácter individualista o solitario en el que no existe una ética o sentimiento de comunidad. Algunos autores consideran que muchos *viruckers* mantienen rasgos de carácter psicopático "con una dinámica psíquica reflexiva con un estilo épico". Son un grupo altamente peligroso y con una gran difusión. Más allá de estas características, un sector de la doctrina considera que los *viruckers* no constituyen un perfil diferenciado de los *crackers* o los *hackers*, al entender que se trata simplemente de una especialización por razón del programa informático que desarrollan (MIRÓ LLINARES, 2012).

d) Traficante de armas (traficante de malware, spyware, virus, etc.): se trata de una especialización en el desarrollo y venta de programas *malware*, virus y otras herramientas que permiten la intrusión en sistemas informáticos ajenos. El traficante se especializa en su facilitación a terceros para posibilitar la comisión de hechos delictivos. Normalmente operan en mercados negros virtuales dentro de la Red Profunda (*Deepweb*). También es frecuente que trafiquen con información o datos de terceros, captada en el ciberespacio (*netrunners*) mediante la técnica del denominado "secuestro de datos" gracias a la utilización de *ransomwares* (*ransom* es un término anglosajón que significa "rescate". Se trata de programas maliciosos que restringen o bloquean el acceso a determinadas partes o archivos del sistema operativo infectado). La principal motivación de los traficantes de armas virtuales es el beneficio económico y sus ataques pueden dirigirse tanto a empresas como a personas físicas.

e) Banquero: se trata de piratas informáticos especializados en el robo de información dentro del ámbito financiero. Posteriormente, podrán suministrar a terceros esa información o venderla para obtener beneficios económicos. Además de delitos relacionados con el espionaje financiero y el descubrimiento o revelación de secretos, es frecuente que utilicen la usurpación de identidad para robar las credenciales bancarias de los clientes (*phising*).

f) Contratista o hackers for hire: se trata de sicarios o mercenarios del ciberespacio: *hackers* por contrato. Mediante precio o recompensa llevarán a cabo determinados servicios para su cliente, que pueden ir desde el robo de información hasta cualquier ataque informático a un sistema de información,

bien pertenezca a una persona física o a una persona jurídica. Sus principales objetivos son económicos, pudiendo prestar sus servicios en solitario o en grupo. No comparten la ética de los *hackers* de sombrero blanco, siendo su principal motivación la obtención de un beneficio económico. Pueden actuar de manera individual o en grupo.

g) Agente especial: podría decirse que estamos ante la élite de los *crackers*, habiéndoseles otorgado el infame título de las "fuerzas especiales de los hackers de sombrero negro". Se trata de sujetos con un nivel de especialización y conocimientos informáticos muy alto. Llevan a cabo amenazas persistentes avanzadas y espionaje cibernético. Pueden pertenecer a organizaciones criminales que les faciliten los recursos y el soporte que necesitan. En otras ocasiones, pueden pertenecer a los servicios de inteligencia de los Estados o ser contratados por gobiernos extranjeros para atacar las infraestructuras críticas.

h) Ninjas e information warriors: hackers sigilosos que se infiltran en los sistemas de datos de las grandes empresas para obtener información e intercambiarla por dinero. La infiltración es un factor clave en sus operaciones por lo que pueden actuar en grupo con un "topo" en la propia empresa víctima. Su organización se encuentra muy estructurada y jerarquizada, donde los líderes se convierten en agentes profesionales que operan como las compañías legítimas que esperan atacar.

i) Ciber-soldados: se trata de *hackers* especializados en la guerra virtual, con el objetivo final de inutilizar la capacidad militar de un oponente. Su cometido es principalmente militar, siendo su tarea principal la de penetrar en los sistemas o redes de otro Estado con la intención de provocar daños, interrupciones o explotaciones de datos.

j) Spammer: el *spam* puede definirse como la creación y difusión de mensajes no deseados, en su mayoría publicitarios. Los hackers especializados en la creación y distribución de esta clase de información reciben el nombre de *spammers*. Una vez creado el contenido se procede a enviar de manera automática y en masa. Cuando los spam tienen el objetivo de molestar al receptor del mensaje podríamos estar ante delitos de acoso, mientras que si se trata de publicitar un producto o servicio mediante esta clase de medios podrían vulnerarse las normativas mercantiles y de libre competencia. No obstante, en la mayor parte de los casos la ilegalidad tiene su origen en la forma en la que los *spammers* crean sus bases de datos, lo que constituye una vulneración de las leyes de protección de datos personales.

k) Domainer: sujeto que compra y registra dominios con el fin de explotarlos económicamente: inversores en nombres de dominio. En muchas ocasiones, estos dominios son adquiridos por el *domainer* ante determinados sucesos de especial repercusión mediática, utilizando nombres no registrados. La principal actividad delictiva en la que pueden incurrir esta clase de *hackers* es la estafa consistente en montar empresas que ofrecen un servicio de comprobación de disponibilidad de dominios que, tras la realización del chequeo de inexistencia, adquirirlo para una futura reventa a la misma empresa solicitante o a una tercera de la competencia.

l) Espías Informáticos: especialistas en la intrusión informática, el robo de información, el sabotaje y el chantaje. En la mayor parte de los casos dirigen sus ataques contra empresas del sector privado (espionaje industrial), pero pueden atentar contra los sistemas de información gubernamentales.

ll) Sniffer: hackers especializados en la confección y uso de programas de ordenador capaces de controlar y analizar el tráfico red transmitido de una localización de red a otra, con el objetivo de robar información (por ejemplo, en una red de empresa). Estos programas son *softwares* muy especializados, con características no estandarizadas que registran la información que envían los periféricos, así como la actividad realizada en un determinado terminal. La amenaza de captación de datos en estas transmisiones es patente, puesto que en la mayor parte de los casos esta información carecerá de un adecuado cifrado.

m) Terrorista informático o cyberterrorist: se trata de un terrorista con conocimientos informáticos suficientes como para elevar la comisión de actos y atentados terroristas al ciberespacio. Su intención será la de atentar contra el orden estructural y constitucional del Estado al que ataca, normalmente a través de ataques informáticos que generen terror en la población. La principal característica de este perfil es la motivación y justificación de los actos criminales por motivos como la religión, la economía o la política.

n) Phisher: usurpadores y suplantadores de identidad. Su principal objetivo es la obtención de datos personales, financieros, etc., de la víctima. Su principal objetivo es el beneficio económico y su modus operandi más habitual es el envío de correos electrónicos trampa con algún tipo de *malware* espía que les permite la extracción de los datos.

ñ) Hoaxer: en la era de Internet y las redes sociales, la información es poder. Las *fake news*, la denominada *infoxicación*, son conceptos de reciente acuñado que están estrechamente relacionados con la velocidad a la que la información puede ser subida a la red y viajar por ella. Los *hoaxers* son que

difunden bulos (*hoax*) o correos electrónicos en cadena con contenido falso o engañoso y atrayente.

o) Hacktivista o anarquista: esta clase de *hacker* propugna la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos o sociales. Se consideran a sí mismos como hackers de sombrero blanco, aunque sus actividades suelen estar prohibidas en los ordenamientos jurídico-penales. Sus principales objetivos son las grandes corporaciones o los sistemas de información de los Estados. Su lucha se encuentra imbuida de un código ético prosocial y de valores antisistema, llegando a conocerse en ocasiones sus conductas como una modalidad de la desobediencia civil.

2. El ciberdelincuente no especializado

a) Emugger: son el equivalente de la delincuencia de bagatela en el ciberespacio. Se trata de un grupo numeroso que ha conseguido los conocimientos necesarios para desarrollar programas maliciosos, con el fin de obtener ganancias económicas.

b) Wannabe: aspirantes a *hackers* especializados, siendo ésta su principal motivación para llevar a cabo actividades ilegales. Tienen un conocimiento y unas aptitudes informáticas más elevadas que los *emuggers*, pero se encuentran completando su aprendizaje como expertos.

c) Poseur: aunque en ocasiones puede confundirse con los *wannabe*, la diferencia fundamental es que el *poseur* está más interesado en los réditos de la imagen del hacker que en la esencia del mismo. Su principal motivación, por tanto, no será la de aumentar sus conocimientos informáticos, sino tratar de ser admitido en el grupo para su propia vanagloria.

d) Newbie y lammer: el primero de los términos es utilizado para definir a los novatos que aún no han alcanzado un nivel de conocimientos profundo. Se trata de la primera fase de iniciación en la carrera de *hacker*. El segundo término –*lammer*- es utilizado de manera despectiva para definir a aquellos sujetos que alardean de poseer conocimientos informáticos que en verdad no tiene. Su perfil de personalidad se caracteriza por ostentar poca madurez, falta de sociabilidad o habilidades, complejo de inferioridad, falta de autoestima y necesidad de atención.

f) Script kiddie: usuarios –normalmente jóvenes- que carecen de conocimientos avanzados en el campo de la informática, pero que gracias al uso de herramientas y programas creados por otros *hackers* más especializados, interrumpen en los sistemas informáticos. La búsqueda de emociones y el riesgo que supone el reto de penetrar en terminales ajenas es

lo que motiva principalmente a estos iniciados. Actúan para lograr notoriedad, realizando actividades que se aprovechan de las brechas de seguridad de los sistemas. Realizan ataques informáticos (DoS y similares) de robo de datos, daños informáticos o bloqueo de sistemas, generalmente eligiendo las víctimas de manera aleatoria y carecen de objetivos determinados. Los *scriptkiddies* no gozan de buena reputación entre los *hackers* especializados y están etiquetados *point-and-clickers* (usuarios de apuntar y hacer click), y sus ataques se llaman despectivamente *point-and-click attacks*, lo que viene a significar que hay muy poco razonamiento o estudio involucrado en los mismos.

Además de estas categorías, otros autores (MIRÓ LLINARES 2012; FANJUL FERNÁNDEZ ET AL., 2018) destacan algunas características específicas del perfil de los cibercriminales basadas en la tipología de ciberdelito cometida.

Cibercriminal económico: su principal motivación es obtener un beneficio económico directo o indirecto en el caso de que sean contratados por grupos organizados. Entre ellos pueden diferenciarse: el *insider* que pertenece o trabaja para la institución o empresa víctima de la infracción (también se incluyen en esta categoría los antiguos empleados que ya no forman parte de la compañía), cuyos ataques informáticos (*data breachers*: destrucción, modificación o acceso no autorizado a datos de la empresa) pueden tener una tasa de éxito mucho mayor que los externos, dado que es más posible que pasen desapercibidos y suponen un riesgo, por el mayor acceso a la información; el *outsider*, cualquier cibercriminal que no pertenece a la estructura empresarial a la que ataca obteniendo sin autorización la información de la misma, realizando un escaneo de sus sistemas y medidas de seguridad para, posteriormente, proceder al acceso remoto aprovechando los fallos de seguridad y, finalmente, una vez realizado el ataque, borrar sus huellas virtuales; los grupos u organizaciones criminales tradicionales (mafias) y las llamadas ciberbandas, conjunto estructurado de *crackers*; y, por último, las denominadas *cibermulas*, que, si bien algún autor ha sostenido que "no son, desde una perspectiva criminológica, cibercriminales, puesto que no son autores del delito en el ciberespacio sino colaboradores o recolectores de los beneficios en Internet que luego envían por medios seguros de transmisión el dinero a los autores del delito (las ciberbandas) o a los responsables de los grupos organizados tradicionales que operan en Internet" (MIRÓ LLINARES, 2012), lo cierto es que son esenciales en el desarrollo de muchos fenómenos delictivos que tienen su origen en el ciberespacio. Una de las modalidades más conocidas es la del "mulero bancario": mediante una oferta de trabajo con apariencia más o menos real, aunque con unas condiciones laborales muy sugerentes, determinadas mafias

cibercriminales se aprovechan de terceros para completar un proceso delictivo. Estos muleros son una pieza clave en el entramado de la estafa informática conocida como *phising*: son los que reciben la transferencia proveniente de la cuenta corriente de la víctima y reenvían parte del dinero a los delincuentes. No obstante, aunque en un primer momento la jurisprudencia española los condenaba como coautores o cooperadores necesarios de un delito de estafa a estos intermediarios, pero lo cierto es que el mulero bancario no tiene dominio alguno sobre el engaño o manipulación informática. Además de ello, es frecuente que en esta clase de asuntos la defensa del acusado interponga la existencia de un error de tipo, por desconocimiento de los elementos del delito de estafa. Por ello, la jurisprudencia ha barajado otras opciones de castigo: el blanqueo de capitales imprudente. Se entiende que el sujeto está ayudando con su conducta imprudente a legalizar un dinero que proviene de un delito previo (la estafa informática). Al existir una modalidad imprudente es preciso demostrar la existencia de culpa grave, esto es una flagrante inobservancia del cuidado debido en la averiguación del origen ilícito de los bienes. Este tipo penal es el mayoritariamente utilizado para castigar esta clase de conductas. Otra de las modalidades de cibermula es el *reschipper* o reenviador, que envía paquetes de bienes comprados por Internet por medio de cuentas corrientes ajenas a las que se ha accedido por medio de *phishing*.

Algunas investigaciones (CIPC) también hablan de perfiles de cibercriminales económicos concretos, como es el caso de los *fraudsters hackers* o estafadores informáticos, a los que atribuyen algunos rasgos específicos: muchos de ellos son cometidos por ciberdelincuentes varones y jóvenes, provenientes de África y de la Península Arábiga, como medio de subsistencia.

En cuanto a la conceptualización del ciberdelincuente económico, existe cierta controversia doctrinal sobre su encaje en el concepto global e indeterminado de delincuente de cuello blanco. Ello se debe, fundamentalmente, a que el contexto de las nuevas tecnologías ha equilibrado o eliminado muchas de las diferencias de estatus social de esta clase de delincuentes. Actualmente se maneja en Criminología el concepto de delincuente socioeconómico como una categoría a medio camino entre la delincuencia común y la de cuello blanco. Autores como BENSON & SIMPSON (2009) ubican algunas de las tipologías de los cibercriminales económicos en esta categoría, que destaca por provenir de un entorno social y demográfico diferente al de los delincuentes comunes, ser en su mayor parte varones de edad más avanzada (entre los 40 y 50 años o más), fuertes vínculos sociales, ser económicamente estables, tener trabajo y un nivel

educativo superior a la población general. Sin embargo, no todas estas características son predicables del cibercriminal económico. El ciberespacio iguala las desigualdades sociales y económicas, por lo que será frecuente encontrar perfiles de jóvenes y cada vez más presencia femenina en el ámbito de la cibercriminalidad económica. Además de estas consideraciones, la cibercriminalidad económica conlleva generalmente un alto nivel de tecnificación y conocimientos.

Cibercriminal político: la delincuencia de corte ideológico o político cometida a través de medios informáticos y plasmada en el ciberespacio entra dentro de esta categoría, que englobaría tanto la llevada a cabo por grupos organizados, caracterizados por un funcionamiento jerárquico más horizontal y difuso, como por sujetos individuales sin conexión con las mismas. La principal motivación del cibercriminal político es la plasmación y, en ocasiones, imposición de su ideología (*cyberhate*) y la lucha contra el *establishment* por vías más o menos expeditivas (*hacktivismo*, ciberterrorismo).

Cibercriminal social: se trata de una categoría bastante heterogénea, que recoge las características de los sujetos que han cometido delitos cuyo bien jurídico protegido no es ni el económico ni el político. Existen numerosos perfiles de cibercriminales dependiendo de la tipología delictiva concreta que se haya cometido: *cyberstalker, cyberbuller, groomers*, etc. En realidad, debemos coincidir con algún autor (MIRÓ LLINARES, 2012), en que lo realmente interesante es analizar cómo el ciberespacio, al modificar el ámbito de riesgo en el que se comete el delito, también cambia en muchos casos el perfil de quien lo comete. Por esta razón, nos remitimos a los apartados correspondientes a las tipologías delictivas concretas que se estudian en este libro, donde se incluirán las pertinentes consideraciones sobre el perfil de los cibercriminales.

Otra clasificación posible del perfil de los cibercriminales es la que se extrae de su nivel de profesionalización, así como de su actuación singular o grupal. Así, se habla del *ciberdelincuente oportunista* o *ciberventajista*, persona ambiciosa, racional (realiza elecciones ponderadas de los riesgos) y sin escrúpulos que encuentra en el delito una forma de enriquecerse, por lo que esporádicamente cometerá delitos informáticos como una forma de aumentar sus ingresos puntualmente (no hay intención de una carrera criminal prolongada); el ciberdelincuente común o ciberpandillero, jóvenes que cometen ciberdelitos económicos menores, sin buscar nuevas experiencias, ni sensaciones y tampoco el reconocimiento social, su carrera criminal suele ser efímera y restringida a los años de juventud; el *ciberdelincuente habitual*, que se divide, a su vez, en *ciberneoprofesional*, *ciber-profesional* y el *ciber-*

a-sueldo: el primero de estos términos designa a quien ha convertido el delito informático en su *modus vivendi* y se caracteriza por unos conocimientos de programación limitados, por lo que hace uso de los *kits* de herramientas pre generados para llevar a cabo sus ataques y buscar reconocimiento mediático; *ciberdelincuente profesional* también ha convertido el cibercrimen en su modo de vida especializándose en la materia, pero se define como autónomo y opera en su propio beneficio; el *ciberdelincuente a sueldo* es contratado por un segundo cobrando por sus servicios.

3. Perfilado criminal

En cuanto a otras cuestiones relevantes de las características psicosociales del cibercriminal, las diferentes investigaciones criminológicas realizadas evidencian las dificultades de encontrar denominadores comunes en el perfil del cibercriminal.

Así, respecto a la estética, a excepción de algunos grupos concretos que han adoptado unos distintivos contraculturales inspirados en la ciencia ficción (como los *cyberpunks*), los cibercriminales no difieren de otros miembros de su grupo de edad (no tienen un código de vestimenta específico, se visten de manera informal), ni cumplen con los estereotipos de imagen transmitidos por la ficción televisiva, el cine o la novela.

En cuanto a los rasgos psicológicos, hay muchos tipos diferentes de personalidades presentes entre los cibercriminales. Generalmente, aquellos más especializados en el dominio de la informática son extremadamente creativos, brillantes, agudos y audaces, rebeldes y soñadores. Les resulta más satisfactorio tratar de aprender experimentando que mediante el estudio tradicional. Algunos pueden mostrar rasgos que denotan timidez e, incluso, tendencias misantrópicas, pero estos desaparecen en sus intensas relaciones en el ciberespacio: les resulta más sencillo relacionarse con otros de manera electrónica (a través de chats, foros, redes sociales, etc.), mientras que no se sienten completamente cómodos en una sola persona. Esto no significa que se trate de personas con trastornos de personalidad o personalidades duales: la protección y el anonimato del ciberespacio puede explicar esta clase de comportamiento social.

Su nivel de autoestima, a pesar de que lo pueda pensarse debido a la imagen clásica del *hacker* proyectada por los medios de comunicación, es bastante elevado. Más aún, algunos autores (CHIESA, DUCCI & CIAPPI, 2009) han explicado la comisión de hechos delictivos en el ciberespacio precisamente por la excesiva autoestima y la necesidad de estos sujetos de alimentar constantemente sus egos. Así, los ataques informáticos contra organismos gubernamentales, corporaciones, etc., es decir, los "símbolos" del

establishment, servirían al propósito de expresar su ira y mostrar su poder y capacidades. Otros, como los *crackers*, muestran su ira y agresividad al realizar ataques contra los sistemas de información.

La presencia de patologías o trastornos de la personalidad no es frecuente, como en la mayor parte de la delincuencia tradicional. De hecho, es habitual que sus habilidades de autogestión se encuentren más desarrolladas que la media. No obstante, es posible encontrar algunos supuestos en los que se han detectado rasgos psicopáticos o trastornos de la personalidad (véase el cuadro a continuación). Uno de los rasgos psicológicos que más se destaca es la tendencia a la paranoia de esta clase de criminales. Estos sentimientos son causados por el miedo constante a la detención y la incertidumbre causada por no saber con quién está tratando *online*. Es frecuente el insomnio, al alternar sus actividades nocturnas en el ciberespacio con sus ocupaciones diurnas.

PSICO-CIBERDELINCUENTE		NORMO-CIBERDELINCUENTE	
CIBER-PSICÓPATA	**INTEGRADO** Ciberdelincuente-exitoso **NO INTEGRADO** Ciberdelincuente-ejecutor	**CIBER–OPORTUNISTA**	Ciberdelincuente-ventajista
CIBER-NEURÓTICO	Ciberdelincuente-manipulable	**CIBER–COMÚN**	Ciberdelincuente - pandillero Ciberdelincuente – rebelde
CIBER-PSICÓTICO	Ciberdelincuente-enajenado Ciberdelincuente-salvador	**CIBER-HABITUAL**	Ciberdelincuente neo-profesionales Ciberdelicuente-profesional Ciberdelicuentes- a sueldo
CIBER-SOCIOPÁTA	Ciberdelicuente-inadaptado		

Fuente: FANJUL FERNÁNDEZ, M.L. *et al*, 2018.

No es excesivamente frecuente el uso de estupefacientes o el abuso del alcohol entre el colectivo *hacker*, decantándose, en la mayor parte de los casos, por el consumo de las denominadas drogas "blandas" (cannabis). Solamente los menos cualificados entre los *hackers* abusan de estas sustancias, dado que la falta de claridad mental les impide realizar un ataque sin cometer errores y evita que alcancen los niveles más altos de sus capacidades técnicas.

En lo atinente a las relaciones y antecedentes familiares, la existencia de un mayor desarraigo o debilitación de los vínculos es superior a la media: padres ausentes o excesivamente protectores, familias desestructuras o

disfuncionales, falta de atención o métodos de crianza pobres, etc. En algunos casos, esto puede explicar el refugio del sujeto en el ciberespacio y la dedicación a la adquisición de sus aptitudes y conocimientos en el campo de la informática. Uno de los métodos de crianza deficientes que se observan en la mayor parte de los supuestos es que a los padres no les importa lo que sus hijos hacen con sus ordenadores, no existiendo control al respecto.

Respecto a las relaciones con los pares, frecuentemente no se sienten aceptados por sus compañeros, experimentando cierto sentimiento de abandono. Prefieren lidiar con las computadoras, ya que las computadoras no son críticas y no discriminan. Sin embargo, esto se torna completamente distinto en el ciberespacio, donde pueden pertenecer a subculturas y comunidades clandestinas, con las que comparten valores e intereses comunes, desarrollando un sentimiento de pertenencia. En estos grupos contraculturales pueden desarrollar nuevas escalas de valores (*nettiqueta*) y obtener referencias morales que difieran con las habituales en el mundo físico.

Esta relación dentro de la subcultura virtual puede generar un caldo de cultivo criminógeno en el que los sujetos pueden aprenden que la piratería informática es un acto aceptable o, en otros casos, técnicas de neutralización que les ayudan a justificar sus conductas.

En cuanto a sus relaciones con la autoridad, recordemos que en la mayor parte de los casos los *hackers* –de uno u otro signo, criminales o no- han adoptado una posición crítica ante el sistema político y económico. En el caso de los cibercriminales, es frecuente que consideren a los agentes de la autoridad que los investigan como inferiores, sobre todo por su carencia de conocimientos técnicos.

Los ciberdelincuentes pueden provenir de cualquier estrato social y pertenecer a cualquier clase socioeconómica. Aunque algunas investigaciones indican que los delitos informáticos como la piratería informática son más frecuentes en las clases sociales altas, lo cierto es que el ciberespacio es un lugar, hasta cierto punto, libre de los condicionamientos de las clases sociales tradicionales o, al menos, ejerce un efecto nivelador. Ciertamente, como ya hemos tenido oportunidad de exponer, existen algunas diferencias en el acceso a los medios tecnológicos, pero actualmente incluso en los sustratos sociales más humildes es posible el acceso a aparatos informáticos o una conexión a Internet.

En cuanto a su nivel educativo, tampoco existe homogeneidad: si bien la mayor parte de los cibercriminales son curiosos y están dispuestos a aprender, esto no significa necesariamente que quieran hacerlo a través de

los medios tradicionales. Muchos cibercriminales han tenido altas cotas de fracaso escolar o, directamente, han abandonado sus estudios formales para dedicarse a aprender sobre lo que realmente les interesa. En los estudios realizados hasta la fecha, los datos arrojan la evidencia de que, en la mayor parte de los casos, los *hackers* tienen un nivel de estudios algo superior a la media de la población.

Bibliografía

BENSON, M. & SIMPSON, S. (2009): White collar crime: an opportunity perspective. London: Routledge.

BERGUER, A., PATCHIN J.W., & HINDUJA S. (2015). Cyberbullying Prevention and Response. Expert Perspectives. Routledge, New York.

CÁMARA ARROYO, S. (2015): Apuntes de delincuencia y criminología juvenil: adaptados a la docencia del Plan Bolonia. Logroño: UNIR.

CARRETERO SÁNCHEZ, S. (2017). "Una propuesta de estatuto legal del hacker ético en nuestro sistema. Su posibilidad limitada", en *La Ley*, N.º 1177, edición digital.

CENTRO INTERNACIONAL PARA LA PREVENCIÓN DE LA CRIMINALIDAD (2018): VI Informe internacional sobre la prevención de la criminalidad y la seguridad cotidiana: prevenir la ciberdelincuencia. CIPC, Montreal (Canadá).

CHIESA, R., DUCCI, S & CIAPPI, S. (2009): Profiling hackers: the science of criminal profiling as applied to the world of hacking. Boca Raton: Auerbach Publications Taylor & Francis Group.

CHOI, K.S. & TORO-ÁLVAREZ, M.M. (2017). Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital (Cybercriminology Guide for the investigation of cybercrime and best practices in digital security). Universidad Antonio Nariño, Bogotá.

CHOI, K.S. (2015). Cybercriminology and Digital Investigation. LFB Scholarly Publishing LLC, El Paso (Texas).

CHOI, K.S., LEE, S.S. & LEE, J.R. (2017). "Mobile Phone Technology and Online Sexual Harassment among Juveniles in South Korea: Effects of Self-control and Social Learning", International Journal of Cyber Criminology, 11(1), pp. 110–127.

DANQUAH, P., & LONGE, O. (2011). "An empirical test of the space transition theory of cyber criminality: Investigating cybercrime

causation factors in Ghana", African Journal of Computing & ICT, 2(1), pp. 37-48.

DE LA CUESTA ARZAMENDI, J.L. & PÉREZ MACHÍO, A.I. (2010): "Ciberdelincuentes y cibervíctimas", en DE LA CUESTA ARZAMENDI, J.L. (Dir.): Derecho penal informático. Cizur Menor: Civitas.

FANJUL FERNÁNDEZ, M.L. ET AL (2018): Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas. Madrid: AMEC Ediciones.

FRANÇA, L.A. (2018). "Cyber-Criminologies", en CARLEN, P. & FRANÇA, L.A. (Eds.). Alternative Criminologies. Routledge, Abington, Oxford.

FRANKS, M.A. (2010). "The banality of cyber discrimination or the eternal recurrence of September", en Denver Law Review Online, Vol. 87, pp. 1-6.

GIL GIL, A. & HERNÁNDEZ BERLINCHES, R. (Coords.). Cibercriminalidad. Dykinson, Madrid.

GONZÁLEZ GARCÍA, Abel (2016). "Cibercriminología, el futuro está aquí", en BRIGGS, D., RÁMILA, J., & PÉREZ SUÁREZ, J.R. (Dirs.). La Criminología de hoy y del mañana. Dykinson, Madrid.

HAFNER, K. & MARKOFF, J. (1995): Cyberpunks: Outlaws and Hackers on the Computer Frontier. New York: Touchstone, Simon & Schuster.

HARAWAY, D. (1991). Simians, cyborgs and women: The reinvention of nature. Free Association, London.

HIGGINS, G.E., & MAKIN, D.A. (2004). "Self-Control, Deviant Peers, and Software Piracy", Psychological Reports, 95, pp. 921-931.

HIGGINS, G.E. (2007). "Digital piracy, self-control theory, and rational choice: An examination of the role of values", International Journal of Cyber Criminology, 1(1), pp. 33-55.

HIKAL-CARREÓN, W.S. (2013). "La especialización de la criminología: De lo general a lo específico, ¿hacía una neocriminología? teoría de las criminologías específicas", en Derecho y Cambio Social, Año 10, Nº. 32, edición online.

HIKAL-CARREÓN, W.S. (2016). "Las criminologías específicas: de lo general a lo especializado", en Anuario Internacional de Criminología y Ciencias Forenses, Nº. 1, 2016, pp. 363-366.

HINDUJA, S. & PATCHIN, J.W. (2007). "Offline consequences of online victimization: School violence and delinquency", Journal of School Violence, 6(3), pp. 89-112.

HOLT, Thomas J. (2007). "Subcultural Evolution? Examining the Influence of On-and Off-Line Experiences on Deviant Subcultures", Deviant Behavior, 28, pp. 171–198.

JAHANKHANI, H. (Ed.) (2018). Cyber Criminology.: Springer International Publishing, Springer Nature Switzerland.

JAISHANKAR, K. (2007). "Cyber criminology: Evolving a novel discipline with a new journal", International Journal of Cyber Criminology, 1(1), pp. 1–6.

JAISHANKAR K., (2008). "Space transition theory of cybercrimes", en SCHMALLAGER, F. & PITTARO, M. (Eds.). Crimes of the Internet. Prentice, Hall Upper Saddle River, pp. 283-301.

JAISHANKAR, K. (2010). "The Future of Cyber Criminology: Challenges and Opportunities", International Journal of Cyber Criminology, 4(1&2), pp. 26–31.

JAISHANKAR, K. (2011). "Introduction", en JAISHANKAR, K. (Ed.). Cyber criminology: Exploring Internet crimes and criminal behaviour. CRC Press, Boca Raton (Florida), pp. xxvii–xxxv.

JAISHANKAR, K. (2018). "Cyber Criminology as an Academic Discipline: History, Contribution and Impact", International Journal of Cyber Criminology, 12(1), p. 1-8.

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

KOOPS, B.J. (2010). "The internet and its opportunities for cybercrime", Transnational Criminology Manual, 1, pp. 735-754.

LESSIG, L. (2006). Code: Version 2.0. 2nd Ed. Basic Books, New York.

LEUKFELDT, R. (Ed.) (2017): Research agenda the human factor in cybercrime and cybersecurity. The Hague: Eleven International Publishing.

MIRÓ LLINARES, F. (2012): El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.

PAYA SANTOS, C., CREMADES GUISADO, A., & DELGADO MORÁN, J.J. (2017): "El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito", en Revista policía y seguridad pública, Año VII, Vol. 1, pp. 237-270.

PÉREZ SUÁREZ, J.R. (2015). We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet. Doctoral thesis, University of Huddersfield.

PÉREZ SUÁREZ, Jorge Ramiro (2016): "Cyborgs del espacio/tiempo", en BRIGGS, D., RÁMILA, J., & PÉREZ SUÁREZ, J.R. (Dirs.). La Criminología de hoy y del mañana. Dykinson, Madrid, pp. 129-154.

ROGERS, M. (1999): "The Psychology of Hackers: The Need for a New Taxonomy", disponible en www.dvara.net/HK/hacker_doc.pdf.

ROGERS, M.K. (2006): "A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy", en Digital Investigation, Vol. 3(2), pp. 97-102.

ROMEO CASABONA, C.M. (2013). "Consideraciones jurídicas sobre los procedimientos experimentales de mejora ("enhancement") en neurociencias", en Direito biomédico Espanha-Brasil II / coord. por Carlos María Romeo Casabona, María de Fátima Freire de Sá, Leonardo Macedo Poli, pp. 1-28.

ROMEO CASABONA, C.M. (2013). "Consideraciones jurídicas sobre los procedimientos experimentales de mejora ("enhancement") en neurociencias", en Maroto Calatayud, M. & Demetrio Crespo, E. (Dir.). Neurociencias y derecho penal: nuevas perspectivas en el ámbito de la culpabilidad y tratamiento jurídico-penal de la peligrosidad. 161-184

SANDYWELl, B. (2010). "On the globalisation of crime: the Internet and new criminality", en DANS JEWKES, Y. & YAR, M. (2010), William Publishing, Cullompton, pp.38-66.

SERRANO MAÍLLO, A. (2009): Introducción a la Criminología. 6ª Ed., Dykinson, Madrid.

SHAW, E.D. (2006). "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations", en Digital Investigation, The International Journal of Digital Forensics and Incident Response, Vol. 3, Elsevier Publications, Exeter, UK, pp. 20-31.

SKINNER, W.F. & FREAM, A.M. (1997). "A social learning theory analysis of computer crime among college students", Journal of Research In Crime & Delinquency, 34(4), pp. 495-518.

TAYLOR, P. (1999): Hackers: Crime in the Digital Sublime. London: Routledge.

TAYLOR, R. (1999): Hackers -Cyberpunks or Microserfs?, in Information, Communication and Society., Boca Raton: Auerbach Publications Taylor & Francis Group.

UNODOC (2013): Comprehensive Study on Cybercrime, 2013. Disponible online en:

VIDAL HERRERO-VIOR, M.S. (2016): Delincuencia juvenil "online": el menor infractor y las tecnologías de la información y la comunicación. Lisboa: Juruá.

WALL, D.S. (2007). Cybercrime: The transformation of crime in the information age. Malden, MA: Polity Press.

WIKSTRÖM, P.H. (2010). "Explaining crime as moral actions", en HITLIN, S. & VAISEY, S. (Eds.). Handbook of the sociology of morality. Springer, New York, pp. 211-239.

YAR M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), pp. 407-427.

YAR, M. (2006). Cybercrime and society. London: Sage.