¿Qué es cibercrimen?

Gustavo Sain*

El filósofo Cornelius Castoriadis señala en su libro "La institución imaginaria de la sociedad" de 1975 que las sociedades desarrollan sus instituciones a partir de determinadas representaciones sociales. Para este autor, el imaginario social se construye a partir de instituciones, leyes, tradiciones, creencias y comportamientos de las personas[1]. En la actualidad existe el imaginario que los delitos informáticos son cometidos por personas con altos conocimientos en informática que con sus habilidades y destrezas técnicas realizan complejas operaciones por sobre las redes para sabotear las bases de datos de robar información o dañarlas.

Así, los denominados "hackers" son capaces de vulnerar sistemas de seguridad de organismos gubernamentales tales como los del Pentágono, la NASA o la CIA, o colapsar servicios públicos esenciales de un país en el marco de lo que hoy se denomina como "ciberguerra"[2]. Si bien existen casos de "hacking"[3] comprobados que han demostrado el acceso no autorizado a sistemas o redes informáticas estatales y de empresas o bancos, el cibercrimen no se limita en la actualidad a estas modalidades delictivas y resulta de una mirada reduccionista explicar este nuevo fenómeno desde esta perspectiva.

La palabra hacker aparece en la década del 60 en Estados Unidos, así se autodenominaban los miembros del MIT, el Instituto de Tecnología de Massachusetts, aquellos programadores que trabajaban en el campo de la informática interactiva para que las computadoras pudieran comunicarse entre sí a través de la innovación tecnológica. El termino proviene del verbo "to hack" (hachar, en inglés) a partir de lo que hacían los técnicos telefónicos cuando subían a los postes y daban golpes a las cajas telefónicas para que funcionaran. Los primeros hackers eran jóvenes contratados por empresas o centros de investigación que independientemente de los encargos de estas organizaciones buscaban crear o descubrir cómo funcionan las cosas a través del conocimiento técnico. Si bien hoy en día el término hacker aparece cargado de una connotación despectiva por la actividad ilícita de algunos de ellos, de esta subcultura salieron las principales innovaciones relacionadas con Internet tal como la conocemos[4].

Esta igualación entre delitos informáticos y hackers llevó a calificar este tipo de conductas como criminalidad organizada o "delitos de cuello blanco". Si se toma como referencia la primera definición, la Convención de las Naciones Unidas sobre la Delincuencia Organizada Transnacional del año 2000 establece que un grupo delictivo organizado debe entenderse únicamente en los casos donde;

"un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente convención con miras a obtener, directamente un beneficio de tipo económico u otro beneficio de orden material[5]"

Partiendo de esta definición, no todos los hechos ilícitos que se cometen en Internet son cometidos por más de una persona ni pueden ser calificados como "graves". A partir de las posibilidades de anonimato que brinda la red, muchos delitos comunes son cometidos en forma individual y no necesariamente con una

finalidad monetaria. Al igual que en el mundo físico, existen delitos convencionales que adoptan nueva forma en la red y pueden ser cometidos por un usuario desde de su hogar, como por ejemplo las estafas en línea, la distribución e intercambio de pornografía infantil, y las amenazas contra las personas, por ejemplo. Asimismo Internet permite la comisión de nuevos delitos tales como la desfiguración de páginas web, la distribución de virus o el acoso simultaneo por diferentes vías.

Si bien históricamente el crimen organizado hizo uso de las tecnologías de la época para el desarrollo de sus operaciones teléfonos satelitales, agendas electrónicas, computadoras, celulares encriptados, el delito informático per se no puede ser calificado como delito organizado o complejo. Estos grupos se sirven de los servicios y aplicaciones de Internet para el desarrollo de sus actividades, tal como lo hace el narcotráfico, el lavado del dinero o el terrorismo. En este sentido, en el informe anual de 2001, la Junta Internacional de Estupefacientes de Naciones Unidas señala;

“En el caso de una organización de tráfico de drogas, la estructura en red tiene claras ventajas en comparación con la jerarquía tradicional, ya que cuenta con un núcleo bien protegido y compacto de organizaciones o personas que disponen de vínculos múltiples con una periferia más disgregada, lo que le permite eludir mejor los esfuerzos de represión”[6]

En relación al concepto de delito de cuello blanco, el mismo fue acuñado por el sociólogo estadounidense Edwin Sutherland en 1939 y refiere a los delitos cometidos por los hombres de negocios a partir de la posición de poder que ocupan desde las corporaciones. Para este autor;

“El punto más significativo de diferencia reside en los conceptos que tienen de sí mismos los delincuentes y en el concepto que tiene el púbico sobre ellos. El ladrón profesional se ve a sí mismo como un delincuente y así lo ve el público en general. Como no desea tener una reputación pública favorable, se enorgullece de su reputación como delincuente. El hombre de negocios, por el contrario, se ve asi mismo como un ciudadano respetable, y por lo tanto, así lo considera el público”[7].

A diferencia de los delincuentes comunes y profesionales, para Sutherland, el delito de cuello blanco es cometido por personas de respetabilidad y status social alto en el curso de su ocupación. Asimismo tiene la capacidad de generar temor y admiración en la gente por producir ingresos en forma ilícita sin ser alcanzados por la justicia. En este aspecto la definición de delito de cuello blanco encuentra un punto de coincidencia con el de delito informático. Hasta la creación de la PC a principios de los años 80s, los usuarios de informática debían tener conocimientos específicos para el manejo de computadoras. El funcionamiento de los dispositivos estaba basado en programas que operaban mediante comandos complejos que requerían de formación y capacitación específica. Desde esta perspectiva, la informática no masiva sino que se circunscribía a un uso académico y/o profesional dependiente de los centros universitarios, organismos gubernamentales, empresas y bancos.

Pero los hackers no eran gente de negocios –muy por el contrario-, en la mayoría de las veces se revelaban contra ellos a partir de un espíritu cuasi anárquico y libertario[8]. En este contexto existe una definición que se adecúa mucho más a la de Sutherland y que se presenta como una extensión de la misma, que es la de

delito ocupacional. El concepto fue elaborado por el criminólogo estadounidense Gary Green en 1990 y es entendido como

“Cualquier acto penado por la ley que se comete a partir de las oportunidades generadas en el transcurso de una ocupación que es legal”[9].

Para este autor, son fundamentales dos criterios para que un delito pueda ser considerado como “ocupacional”: el acto ilícito debe ser penado por la ley y ser cometido a partir de la oportunidad creada por una ocupación que se desarrolla dentro del marco de la ley. Existen cuatro categorías de delitos ocupacionales: 1) delitos organizacionales, 2) delitos gubernamentales, 3) delitos profesionales, y 4) delitos cometidos por personas que son parte de una organización en su propio beneficio.

Los delitos organizacionales son delitos cometidos por miembros de la misma en beneficio de la organización empleadora, como por ejemplo, la fijación de precios, la falsificación de productos, el robo de secretos comerciales y el fraude de ventas, entre otros. Los delitos gubernamentales son crímenes que se realizan por autoridades en función del cargo que ejercen dentro del Estado tales como evasión impositiva, abuso de autoridad, sobornos, malversación de fondos, etc. Los delitos profesionales son aquellos ilícitos que se producen en el marco del ejercicio de una profesión que incluye una violación a juramentos y normas éticas (medicina, psicología, abogacía, veterinaria, etc). Por último están los delitos individuales, que se cometen por agentes o empleados en beneficio propio, tales como hurto de bienes -elementos de oficina-, robo de servicios –realización de llamadas de larga distancia, entre otros.

Partiendo de esta clasificación, el delito informático parece surgir como un delito ocupacional de tipo profesional, en tanto que los primeros usuarios de Internet eran en su mayoría ingenieros, programadores y especialistas en informática de empresas contratistas del ejército que desarrollaban su actividad en el marco de un proyecto gubernamental que requería de secretismo de sus actividades mediante firma de contratos de confidencialidad. Las conductas ilícitas cometidas en este contexto se enmarcan claramente dentro del subgrupo de delitos cometidos por profesionales en el ejercicio de su ocupación se daba a partir de las posibilidades que le brindaba su medio laboral, a saber, el acceso a computadora y redes. Pero con la creación de entornos gráficos, mouses, tecnologías táctiles la informática amplio su espectro de usuarios y salió del grupo selecto de profesionales especializados para pasar al entorno del hogar con la creación de la computadora personal y programas de fácil manejo. El surgimiento de World Wide Web en 1990 y la posterior apertura comercial de la red Internet por parte del Gobierno de los Estados Unidos en 1995 hizo que la informática se popularizara para extenderse más allá de un uso laboral y hogareño. En este sentido, la comisión de conductas indebidas y hechos ilícitos mediante el uso de tecnologías digitales y servicios y aplicaciones de Internet lo puede realizar de cualquier persona con conocimientos básicos en computación[10].

Con la apertura pública de la red adquiere una nueva dimensión del concepto de delitos informáticos a partir de un crecimiento de conductas indebidas e ilícitas en el “ciberespacio”[11]. Si bien no existe en la actualidad un consenso acerca de los alcances de este fenómeno, en la actualidad;

“los delitos informáticos son entendidos en base al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo. En

este sentido, cuando se refiere a hechos ilícitos o ilegales donde se encuentra involucrado un dispositivo informático[12] no se hace alusión a un tipo de criminalidad específica, sino a aquellas conductas donde interviene un dispositivo informático como medio para cometer un delito o como fin del delito mismo"[13].

Un dispositivo actúa como medio para la comisión de un ilícito por ejemplo cuando un adulto intenta ganarse la confianza de un menor en las redes sociales con el objetivo de concertar un encuentro con él para abusarlo[14]. En el segundo caso el equipo es el blanco del delito cuando se le planta un virus mediante un pendrive con el objetivo de dañar su funcionamiento. Asimismo, la laxitud de la definición permite considerar también como delito informático el daño físico al dispositivo, en tanto que una ruptura física intencional que tenga como finalidad el no funcionamiento del sistema o daño a los datos e información que contiene ingresa dentro de esta definición.

Otra clasificación sobre este tipo de conductas ilícitas es aquella que utiliza el criterio del entorno donde se sucede la mayoría de los delitos informáticos en la actualidad: Internet. Según el criminólogo estadounidense Majid Yar;

"La delincuencia informática se refiere no tanto a un único tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar"[15].

En síntesis, el cibercrimen no es cometido únicamente por hackers o personas con altos conocimientos en informática y sistemas en la actualidad. Cualquier usuario de computadoras e Internet puede cometer un crimen informático en la actualidad. Asimismo los delitos informáticos en su generalidad no pueden considerarse como parte del crimen organizado, ya que los mismos no se cometen en su mayoría por varias personas que actúan concertadamente ni insume una complejidad propia de este tipo de ilícitos. Si bien el cibercrimen surge como un tipo de delito ocupacional de tipo profesional más que como un delito de cuello blanco, esa definición queda obsoleta en la actualidad a la luz de los avances tecnológicos y el uso masivo y cotidiano de Internet a nivel global. Por último, los delitos informáticos no establecen un tipo de criminalidad específica con características particulares, sino que adquieren ese nombre a partir del rol que ocupa la tecnología en la comisión de hechos ilícitos, tanto como medio para llegar al delito en sí como también fin o blanco del delito mismo.

Notas [arriba]

* *Especialista en cibercrimen, asesor del Ministerio de Justicia y Derechos Humanos de la Nación y autor del libro "Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por Internet" de Editores del Puerto.*

[1] Castoriadis, Cornelius: La institución imaginaria de la sociedad. Buenos Aires, Tusquets Editores, 2013.
[2] La ciberguerra es un área militar que se plantea como objetivo encontrar las vulnerabilidades técnicas de las redes informáticas del enemigo para extraer

información o dañar sus sistemas. El ciberespacio es el campo de batalla y los programas y aplicaciones informáticas, las armas. Las tácticas de combate son la infiltración en redes enemigas, la recopilación de datos, la interferencia de señales inalámbricas, los programas informáticos falsificados y los ataques a sistemas enemigos a través de virus, gusanos y bombas lógicas, entre otras.
[3] El término "hacking" refiere en general al acceso no autorizado a una computadora o un sistema informático.
[4] Sain, Gustavo: ¿Que es un hacker? (I). Artículo publicado en la Revista Pensamiento Penal el 25 de abril de 2015. Disponible en http://www.pensamientopenal.com.ar/doctrina/40977-es-hacker-i (10 de marzo de 2016)
[5] Organización de las Naciones Unidas: Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Viena, Publicación de Naciones Unidas, 2000.
[6] Junta Internacional de Fiscalización de Estupefacientes, Informe anual 2001: La mundialización y las nuevas tecnologías; Problemas que plantean a los servicios de lucha contra las drogas en el siglo XXI. Nueva York, Publicación de las Naciones Unidas, 2001.
[7] Sutherland, Edwin: El delito de cuello blanco. Madrid, Ediciones de La Piqueta, 1999.
[8] Los hackers activistas o hacktivistas, que tienen una finalidad política. Bregan por la libertad de expresión y el derecho a la información en Internet y se manifiestan contra los gobiernos y las empresas que ellos consideran afectan estos principios.
[9] Green, Gary, Occupational Crime. Illinois, Nelson Hall Publishers, 1994.
[10] En la actualidad, cualquier usuario puede abrir una casilla de mail con un nombre ficticio y amenazar a otra desde un ciber, un locutorio o una red pública, por ejemplo.
[11] El término “ciberespacio” aparece por primera vez en 1984 en la novela futurista Neuromante de William Gibson, en la cual se hacía referencia a una realidad virtual presente en todos los ordenadores y las redes mundiales de computadoras. Con el surgimiento de la World Wide Web en 1990, ese espacio virtual fue bautizado con este término.
[12] La palabra "dispositivo" alude a un aparato o mecanismo capaz de ejecutar una o varias acciones con un fin determinado mientras que el término "informática" es una conjunción de "información y "automática" y refiere al procesamiento automático de información mediante dispositivos electrónicos. Así, un dispositivo informático es un aparato capaz de procesar en forma automática datos e información con un fin determinado. Si bien las computadoras representan los dispositivos informáticos más utilizados en la actualidad, cualquier dispositivo capaz de producir la entrada, el procesamiento y salida de información es considerado como tal, para lo cual teléfonos móviles, cámaras fotográficas digitales, televisores inteligentes, consolas de videojuegos, entre otros también entran en esta definición.
[13] Sain, Gustavo: “¿Qué son los delitos informáticos?” En Rubinzal Culzoni online http://www.rubinzalonline.com.ar/. Buenos Aires, Rubinzal Culzoni Editores, agosto de 2015.
[14] La presencia de adultos que ingresan a servicios y aplicaciones web haciéndose pasar por pares con el objetivo de ganar su confianza y acosarlos sexualmente recibe, en la jerga de Internet, el nombre de grooming -derivado del verbo en inglés to groom, preparar- y se define como el proceso de captación y manipulación de menores on line con fines sexuales. En líneas generales, el grooming tiene tres objetivos: concertar un encuentro real con el menor para concretar un abuso; el acoso virtual mediante relatos eróticos; y distribución de

imágenes pornográficas y obtener material multimedia: fotografías o videos a través de la cámara web en situación de desnudez. Para mas información ver: Sain, Gustavo: “El acoso sexual por Internet”. Artículo publicado en el Diario Página 12 el 15 de abril de 2014.
[15] Yar, Majid: Cybercrime and society. London, Sage Publications, 2006.