Criminalidad virtual: ¿Vino viejo en botellas nuevas? Traducción y nota previa de Miguel A. Cano Paños

Peter N. Grabosky
Australian Institute of Criminology.

Cano Paños, M. A. (2019). Criminalidad virtual: ¿Vino viejo en botellas nuevas? Traducción y nota previa de Miguel A. Cano Paños. *Revista Electrónica de Criminología, 02-01*, 1-8.

RESUMEN: El siguiente trabajo tiene como objetivo presentar, en lengua española, el sugerente artículo publicado hace ya casi veinte años Peter Grabosky, en el cual analizaba el binomio delito e Internet. Y ello en una época en la que la denominada «era digital» se encontraba todavía inmersa en una fase de implantación a nivel mundial. El postulado fundamental de Grabosky era que el delito cometido en Internet no difería esencialmente del ejecutado en el espacio terrestre, exceptuando quizá el medio en el que el evento criminal tiene lugar.

PALABRAS CLAVE: Ciberdelito, Internet, actividades cotidianas, ciberespacio, criminología ambiental

VIRTUAL CRIMINALITY: OLD WINE IN NEW BOTTLES? TRANSLATION AND PREVIOUS NOTE BY MIGUEL A. CANO PAÑOS

ABSTRACT: The following work aims to present the Spanish version of the suggestive article published almost twenty years ago by Peter Grabosky, in which he analyzed the relationship between crime and Internet. And this at a time when the so-called «digital era» was still immersed in a worldwide implementation phase. Grabosky's fundamental postulate was that the crime committed on the Internet did not differ essentially from that executed in the terrestrial space, except perhaps in terms of the medium in which the criminal event takes place.

KEYWORDS: Cibercrime, Internet, routine activities, cyberspace, environmental criminology

FECHA DE RECEPCIÓN EN REC: 01/10/2019
FECHA DE PUBLICACIÓN EN REC: 31/12/2019
AUTOR/A DE CORRESPONDENCIA: macano@ugr.es

Nota previa

A lo largo de la historia de la comunicación humana han surgido una serie de descubrimientos trascendentales como la escritura, la imprenta, el teléfono o la televisión. Descubrimientos sin duda revolucionarios, los cuales marcaron un antes y un después no sólo en la evolución tecnológica, sino también en los contextos social, económico, político e incluso cultural, cambiando las costumbres y los estilos de vida de los ciudadanos.
Con todo, la aparición y posterior consolidación de Internet como mecanismo de comunicación ha supuesto una auténtica revolución tecnológica sin parangón, cuya dimensión y efectos son de un calibre tal que han dado lugar al comienzo de una nueva época y al nacimiento de una nueva sociedad: la sociedad de la información, también conocida como la «sociedad digital». A ello ha contribuido decisivamente la confluencia de dos variables en cierto modo interrelacionadas no sólo gramaticalmente: la red global de Internet y la globalización económica. Tal y como acertadamente indica Miró Llinares, Internet «ha transformado los mercados financieros en transfronterizos, ha multiplicado las opciones de acceso a información de todo tipo, ha permitido transacciones económicas o personales transfronterizas y en tiempo real, ha creado nuevas formas de comunicación personal y ha modificado los contextos y el sentido de cualquier forma de comunicación» (Miró Llinares, 2012: 143). De ahí lo acertado de hablar de la consolidación de una «sociedad digital» donde Internet es ya el más importante vehículo de comunicación personal y de información, así como un instrumento esencial para la vida social, política y económica. Y es que, como afirmaba Quintero Olivares hace casi dos décadas, «Internet no es una simple progresión en la evolución tecnológica, sino un cambio revolucionario en los modelos de relaciones sociales, que sirve a la fluidez de los intercambios comerciales y de todo tipo» (Quintero Olivares, 2001: 369-370).

Por otro lado, Internet ha creado una nueva dimensión en el espacio de trascendental importancia, a saber, el denominado «ciberespacio». En este sentido, el ciberespacio es un lugar, pero un lugar donde, como se verá a continuación, las dimensiones espacio/tiempo adquieren una significación radicalmente distinta a lo que sucede en el mundo terrestre. Acudiendo en este caso a las sabias reflexiones de Lessig, el ciberespacio es un lugar. Las personas viven en ese lugar, y «allí experimentan todos los tipos de cosas que experimentan en el mundo real. Además, las personas experimentan la vida en Internet en grupos, en comunidades, entre extraños y entre personas que incluso llegan a conocer y con quienes llegan a veces a congeniar» (Lessig, 2001: 348). Podría llegar a afirmarse que la vida diaria de las personas se desarrolla en mayor o menor medida en el ciberespacio.
Como se acaba indicar, el tiempo y el espacio en el ciberespacio adquieren una dimensión distinta, inabarcable e inaudita para el espacio físico. Internet ha hecho el mundo más pequeño, acercando a un mismo «lugar virtual» a personas que pueden estar separadas, en coordenadas espaciales, por miles de kilómetros. Por otro lado, el tiempo requerido para que dos personas separadas por un espacio físico puedan comunicarse se ha contraído también, ante la ausencia de la distancia y la aparición de un espacio virtual de intercomunicación inmediata.

Como a nadie escapa, la existencia de una sociedad digital que utiliza Internet no sólo como medio de comunicación interpersonal, sino también con finalidades económicas, culturales, políticas o de ocio, ha supuesto un auténtico reto para el legislador a la hora de regular todas estas actividades. Qué duda cabe que el enraizamiento de los medios tecnológicos es tan grande que impera en todos los órdenes sociales (Salom Clotet, 2006: 99). Pues bien, en el contexto descrito, el Derecho penal adquiere una especial significación, dado que Internet no sólo fomenta el desarrollo de actividades lícitas, sino también de aquellas otras con un carácter marcadamente delictivo, algunas de las cuales producen la lesión de bienes jurídicos, individuales y colectivos, de importancia. Hasta la década de 1990, el Derecho penal había tomado como referencia para seleccionar conductas delictivas la única dimensión espacial conocida: la del mundo físico o real, único espacio donde podía actuar el delincuente. No obstante, la irrupción de Internet ha dado lugar a que actualmente el mundo analógico conviva con otro mundo, con un espacio virtual también llamado «ciberespacio», con unas coordenadas de acción e interacción absolutamente distintas al mundo físico. Efectivamente, la ejecución delictiva a través de la tecnología informática cuestiona plenamente muchos de los axiomas hasta ahora vigentes para la detección, persecución y castigo del delito y, por ende, del delincuente (Fernández Teruelo, 2007: 13). Así, Internet determina una notable y especial dificultad para el descubrimiento del ofensor, debido al anonimato presente en ese espacio virtual. Por otro lado, el carácter transnacional de algunas conductas delictivas *online* entorpece la actuación de los organismos nacionales encargados de la persecución penal. Por último, el ciberespacio fomenta la vulnerabilidad de no pocos de sus usuarios, debido a su escasa conciencia con respecto a la necesidad de mantener una serie de medidas de seguridad para evitar convertirse en víctimas de un delito.

En definitiva, pese a que la mayoría de las conductas delictivas desarrolladas a través de Internet no son en puridad algo nuevo, «la extraordinaria peculiaridad del medio dota a las mismas de una especial estructura que obliga a actualizar los tipos delictivos» (Fernández

Teruelo, 2007: 13), y diríase incluso que a regular nuevas figuras típicas de exclusiva comisión en el ciberespacio.

Por otro lado, y entrando ya en la temática central de esta nota previa, Internet, la sociedad digital y el ciberespacio constituyen también sin duda un importante reto para la Criminología, acostumbrada a explicar las causas de la delincuencia y el evento delictivo a partir de coordenadas espacio-temporales de carácter físico. Si se tiene en cuenta que el ciberespacio presenta unas características meridianamente distintas al espacio físico, ello debería en principio conducir a que el denominado «cibercrimen», al realizarse en un nuevo ámbito o espacio digital completamente distinto al analógico, tendría en principio que ser analizado utilizando para ello unas coordenadas criminológicas de explicación del evento delictivo completamente distintas a las utilizadas hasta ahora.

Partiendo para ello de los enfoques criminológicos de la oportunidad, y teniendo en cuenta las características del ciberespacio esbozadas en los párrafos anteriores, las cuestiones que inmediatamente se plantean son las siguientes: ¿Constituye Internet un nuevo ámbito de oportunidad delictiva *distinto* al tradicional espacio físico? ¿O se trata, por el contrario, de un espacio que, en sus postulados o características fundamentales, resultado *idéntico* al espacio terrestre? ¿Son los tópicos de la Criminología clásica válidos para la explicación de un delito aparentemente nuevo como es el cometido en el ciberespacio? Pues bien, es precisamente en relación a estas cuestiones donde debe insertarse el trascendental trabajo de Peter Grabosky, Profesor Emérito de la Australian National University, el cual es aquí objeto de traducción por primera vez en lengua española, casi 20 años después de que el mismo viera la luz.

Utilizando para ello una metáfora que se ha convertido en legendaria para todos aquellos/as que desde la Criminología han estudiado la relación entre el evento delictivo y el ciberespacio, Grabosky se planteaba, a finales de la década de 1990, si el cibercrimen constituía realmente «*old wine in new bottles*». Pues bien, acudiendo para ello a los presupuestos establecidos años atrás por Cohen y Felson en su teoría de las actividades cotidianas, Grabosky argumentaba que, si bien la irrupción de Internet había constituido un cambio importante en el factor «oportunidad delictiva», al ser el medio donde transcurre el delito *online* distinto a aquél que caracteriza al espacio físico, los elementos del evento delictivo en el ciberespacio seguían siendo, en esencia, los mismos que en el espacio terrestre. Así, el autor motivado seguía actuando en el mundo virtual guiado por las mismas motivaciones que en el espacio físico, respaldando Grabosky dicha afirmación con la siguiente frase: «La emoción del engaño caracterizó la inserción del Caballo de Troya original, pero no menos que lo hizo la creación de sus descendientes digitales» (Grabosky, 2001: 248). Por otro lado, los sistemas de protección frente al evento delictivo (lo que Cohen y Felson denominaron en su día «guardián capaz») presentaban en Internet la misma importancia y características que en el espacio físico. Quizá la única excepción vendría protagonizada por el objetivo o víctima, la cual, en palabras de Grabosky, estaba expuesta en Internet a una mayor amenaza por parte del delincuente motivado. Y ello debido precisamente a las nuevas coordenadas espacio-temporales inherentes al ciberespacio.

Mucho ha transcurrido y pasado –en términos cibernéticos– desde que Grabosky publicase su influyente trabajo. Sin ir más lejos, el nacimiento de la Web 2.0, el aumento exponencial de terminales donde poder acceder a Internet desde cualquier lugar del mundo, así como la irrupción de los nuevos servicios de comunicación social, especialmente en el contexto de las redes sociales, era algo completamente desconocido para Grabosky en el momento de redactar su trabajo; lo cual, desde luego, no resta mérito a su sugerente análisis realizado de la criminalidad virtual.

Si, como hace ya cuatro décadas señalaron Cohen y Felson en su teoría de las actividades cotidianas, el delito se produce cuando confluyen en el espacio y en el tiempo un delincuente motivado, un objetivo adecuado y la ausencia de un guardián capaz de darle protección al segundo, es evidente que los especiales caracteres del ciberespacio, sobre todo en lo relativo a sus novedosos parámetros espacio-temporales, deben incidir necesariamente en el evento delictivo. Dicho de otro modo: el cibercrimen, como evento social, es necesariamente distinto al crimen en el espacio físico (Miró Llinares, 2011: 19); lo mismo que una relación amorosa es distinta en el espacio terrenal que en el virtual. Como consecuencia lógica, lo explicado conduce a que los elementos definitorios del evento criminal deben ser revisados con nuevos ojos al ser distinto el entorno o el contexto espacio-temporal en el que se comete el delito. Y todo ello sin restar validez a aquellas teorías que, a nivel macro o micro, han intentado explicar la conducta delictiva sobre la base de factores individuales o sociales que pueden afectar al agresor.

Por consiguiente, el cibercrimen, como evento social, sigue estando hoy en día conformado por los *mismos* elementos que el delito cometido en un espacio físico, con lo cual los postulados de Grabosky seguirían gozando de plena actualidad. No obstante, al producirse el ciberdelito en un ámbito tan distinto como es el espacio virtual, esos elementos confluyen de distinta manera a como lo hacen en el espacio terrestre.

Por tanto, la mítica frase «vino viejo en botellas nuevas», habría que interpretarla a día de hoy en el sentido siguiente: si bien el vino puede ser el mismo, la botella en la que el mismo se toma es distinta a la primigenia, por lo que es necesario beberlo y saborearlo de forma diferente a como se hacía antes (Miró Llinares, 2012: 144-145). No se trataría por tanto de botellas nuevas, sino más bien de botellas diferentes. Trasladando esta metáfora del mundo de la enología a la realidad delictiva, ello implica que, en Internet, el delincuente motivado se encuentra ante unas barreras temporales y espaciales distintas para la comisión del delito; a unas víctimas que, debido al anonimato y la dimensión trasnacional de la comunicación *online*, se encuentran más expuestas al riesgo de sufrir un ataque a sus bienes materiales o personales. Y, por último, a unos guardianes capaces con un ámbito de protección muy limitado debido precisamente a las amplias dimensiones del ciberespacio. El identificar estos cambios esenciales del evento criminal en el ciberespacio puede ayudar a la Criminología actual no sólo a explicar el ciberdelito, sino también a prevenirlo en el marco de la denominada prevención situacional.

Precisamente con respecto a la víctima como objetivo adecuado del cibercrimen, Grabosky hace especial hincapié, en la parte final de su trabajo, a la necesidad de impulsar el control social informal o, lo que es lo mismo, los mecanismos de autoprotección, debido precisamente a la probada ineficacia del control formal, y especialmente de las normas nacionales ante un tipo de delincuencia con un marcado ámbito transnacional. Con ello, Grabosky está insinuando que, en el contexto del cibercrimen, la víctima se convierte quizá en el único sujeto que puede incorporar un guardián capaz para su autoprotección o, como él mismo denomina, «autodefensa». Y esa autoprotección debe llevarse a cabo no sólo en el propio actuar cotidiano de los usuarios de Internet, sino también mediante la incorporación de sistemas de seguridad informática. Con lo que, aun de forma indirecta, el propio Grabosky estaba ya reconociendo que, aunque el cibercrimen es un crimen y no otra cosa, el elemento ambiental donde el primero se produce es distinto al terrestre en términos temporales y espaciales, por lo que su explicación se debería realizar usando coordenadas teóricas distintas a las tradicionalmente empleadas.

Bibliografía

Fernández Teruelo, Javier Gustavo (2007): *Cibercrimen. Los delitos cometidos a través de Internet*. Constitutio Criminalis Carolina: Oviedo.

Grabosky, Peter (2001): Virtual Criminality: Old Wine in New Bottles *Social&Legal Studies*, *10*(2), 243-249.

Lessig, Lawrence (2001): *El código y otras leyes del ciberespacio*, Madrid: Taurus.

Miró Llinares, Fernando (2011): La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen., *Revista Electrónica de Ciencia Penal y Criminología*, *13-07*, pp. 1-55.

Miró Llinares, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid: Marcial Pons.

Quintero Olivares, Gonzalo (2001): Internet y propiedad intelectual. En López Ortega, Juan José (Dir.), *Internet y Derecho penal*, Cuadernos de Derecho judicial *10* (pp. 367-398). Madrid: Consejo General del Poder Judicial.

Salom Clotet, Juan (2006): Delito informático y su investigación. En: Velasco Núñez, Eloy (Dir.), Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?, Cuadernos de Derecho Judicial, 3, (pp. 91-129). Madrid: Consejo General del Poder Judicial.

Criminalidad virtual: ¿Vino viejo en botellas nuevas?[1]

Peter N. Grabosky (*Australian Institute of Criminology)*

Introducción

Se ha convertido en algo trivial sugerir que la convergencia de la informática y las comunicaciones ha comenzado a cambiar la forma en la que vivimos y la forma en la que cometemos delitos. Si ello requerirá una revisión de nuestras premisas filosóficas, históricas y sociológicas es, sin embargo, otra cuestión distinta. Uno debe tener cuidado con realizar sobre-generalizaciones e hipérboles, algo que caracteriza a gran parte del discurso llevado a cabo en la era digital. En las páginas que siguen, sugiero que la «criminalidad virtual» es básicamente lo mismo que el crimen terrestre con el que estamos familiarizados. Sin duda, algunas de sus manifestaciones son nuevas. Pero una gran cantidad de los delitos cometidos con o contra ordenadores difieren únicamente en términos del medio. Mientras que la implementación tecnológica, y particularmente su eficiencia, pueden resultar sin precedentes, el delito es fundamentalmente familiar. No se trata por tanto de una cuestión completamente distinta, sino más bien de un delito reconocible cometido de una manera completamente diferente.

Quizá los desarrollos más notables relacionados con el crimen en la era digital son sus implicaciones transnacionales y las amenazas a la privacidad personal que plantean las nuevas tecnologías. La velocidad de las transacciones electrónicas permite a un delincuente infligir daño o pérdidas en el otro lado del mundo, dando un nuevo significado al término «control remoto». Asimismo, la tecnología digital facilita la vigilancia por parte de agencias públicas y el sector privado, y ello en un grado que es ciertamente revolucionario.

Motivación

Veamos primero las motivaciones de aquellos sujetos susceptibles de cometer delitos relacionados con la informática. Tal vez uno podría ser excusado por considerar el principio «*plus ça change, plus c'est la même chose*».[2] Los delincuentes informáticos están guiados por motivaciones tradicionales, las más obvias de las cuales son la codicia, la lujuria, el poder, la venganza, la aventura y el deseo de probar «el fruto prohibido». Mientras que muchos actos criminales fluyen de motivos mixtos, es la codicia la que principalmente subyace en los fraudes de transferencias electrónicas de fondos, y la lujuria la que impulsa el tráfico de pornografía infantil. La habilidad para tener un impacto en grandes sistemas puede, como un acto de poder, resultar gratificante por y en sí mismo. El deseo de infligir una pérdida o un daño a otro también puede surgir de la venganza, como cuando un empleado descontento desconecta el sistema informático de su empleador, o bien de la ideología, como cuando uno paraliza la página web de la Agencia Central de Inteligencia de los Estados Unidos. Mucha de la actividad que se desarrolla en la frontera electrónica contiene un elemento de aventura, la exploración de lo desconocido. El hecho mismo de que algunas actividades en el ciberespacio son susceptibles de provocar una condena oficial es suficiente para atraer a los desafiantes, o a los irresistiblemente curiosos. Dado el grado de competencia técnica requerida para cometer muchos delitos informáticos, hay otra dimensión motivacional que vale la pena señalar aquí. Esta es, por supuesto, el desafío intelectual para lograr dominar sistemas complejos.

Ninguna de las motivaciones señaladas *supra* es nueva. El elemento novedoso reside en la capacidad sin precedentes de la tecnología para facilitar la actuación a partir de estas motivaciones.

Las relaciones interpersonales en el ciberespacio

En cierta medida, la tecnología digital ha impactado en las relaciones interpersonales. La ilusión del anonimato parece haber provocado una mayor candidez en Internet de lo que cabría esperar en las comunicaciones cara a cara. Pero si el juego de roles que ocurre en algunas salas de chat constituye algo completamente distinto del buen teatro, en el cual los actores están inmersos en sus roles, eso sigue siendo un tema abierto. Sin duda, algunos de estos juegos de roles son extremadamente agresivos, o de otro modo antisociales. ¿Pero más que una actuación de la obra Hamlet?

De hecho, Internet ha provocado cambios significativos en la interacción humana. Los inversores ordinarios ahora pueden comprar y vender acciones *online* sin negociar a través de intermediarios como por ejemplo suscriptores, *brokers* o asesores de inversión. Si bien esto puede mejorar la eficiencia de los mercados de valores, también brinda oportunidades para su explotación criminal. Con todo, la criminalidad fundamental puede todavía ser reducida a lo básico: tergiversar el valor subyacente de una garantía en el momento de la oferta pública inicial, o manipular el mercado durante el comercio secundario de una garantía a través de la difusión de información falsa, o

[1] Título original: «Virtual Criminality: Old Wine in New Bottles?», publicado en *Social&Legal Studies*, Vol. 10(2), 2001, pp. 243-249.

[2] «Cuanto más cambia, más es lo mismo» (N. del T.).

diseñar un patrón engañoso de transacciones para atraer la atención del inversor involuntario.
Uno escucha anécdotas sobre niños que han sido atraídos por pedófilos desde la seguridad de sus hogares, después de un encuentro inicial en una sala de chat de Internet, o mujeres que, tras haber acordado una cita a través de la red, se topan con juego sucio a manos de un depredador. Pero ¿es esto algo realmente nuevo? El ciberespacio cumple la misma función que la parada de autobús, el patio de la escuela o la discoteca.

Hay otro aspecto en el que la criminalidad digital puede resultar similar a la criminalidad convencional. A riesgo de cometer una simplificación excesiva, uno puede dividir los delincuentes en dos clases: el competente y el incompetente. Tarde o temprano, la mayoría de la segunda categoría termina en prisión. Por su parte, el competente evita la detección, o al menos, el enjuiciamiento y la condena. Lo mismo sucede con los ciberdelincuentes. Los más expertos nunca se notan, y mucho menos son identificados. En el polo opuesto, el ciberdelincuente inepto deja sus huellas en todo el ciberespacio.

Nuevos desafíos para el Estado

La era digital ha comenzado a plantear nuevos desafíos para el Estado. Las comunicaciones blasfemas, sediciosas, salaces y de otra manera ofensivas han sido durante mucho tiempo un foco de preocupación gubernamental. En una era donde muchos gobiernos tratan de deshacerse de sus funciones y delegar poderes, la necesidad de controlar la tecnología digital sigue siendo intensa. Y, sin embargo, la capacidad de los gobiernos y los ordenamientos jurídicos para adaptarse a los nuevos medios en lo relativo a la transmisión de contenido ofensivo es todavía algo limitada. Por supuesto, uno podría siempre «tirar del enchufe» y restringir así severamente el acceso de los ciudadanos al ciberespacio. Pero aquellos gobiernos que buscan maximizar el bienestar económico de sus ciudadanos se dan cuenta de que es inútil intentar frenar la marea de la globalización, y que la imposibilidad de entrar en los fundamentos del comercio electrónico puede retrasar el desarrollo económico.

Los desafíos a los que se enfrentan los gobiernos no se limitan en absoluto a la regulación de contenido *online*. Al menos en las sociedades de habla inglesa, la capacidad de las fuerzas de seguridad se reconoce que es limitada. La mayoría de las víctimas de los robos residenciales son conscientes de que tienen pocas posibilidades de recuperar sus posesiones perdidas. Estas albergan pocas ilusiones de que «su» delincuente eventualmente será llevado ante la justicia. El papel de la policía a menudo se limita al de legitimar las reclamaciones a los seguros y a proporcionar unas palabras amables (y tal vez algunos consejos para la prevención del delito) a la víctima. Los individuos están en gran parte solos en lo que respecta a la prevención del delito, y ello en una medida que pocos desean reconocer abiertamente. Y, por ello, aquellos que se lo pueden permitir, adquieren sistemas de alarma sofisticados y viven en comunidades «cerradas». La necesidad de autosuficiencia en el control del delito no es menor en el ciberespacio que en el vecindario físico.

Paradojas de la era digital

Además de la tensión entre el Estado en reducción y el imperativo del tráfico directo en la autopista de la información, la era digital ha dado lugar a otras paradojas. Las tecnologías relativas al anonimato y al pseudónimo como son los *remailers*[3] y la criptografía pueden proporcionar un mínimo de cobertura para alguien que desea enmascarar su identidad y el contenido de su comunicación. Pero no todos se aprovechan de tales tecnologías, mientras que las capacidades de vigilancia exceden a todos menos a los usuarios más determinados.

La criptografía, considerada por la policía como una amenaza, es uno de los pilares fundamentales del comercio electrónico. Sin esta tecnología segura, los pagos electrónicos, y mucho menos la transmisión de los datos de la tarjeta de crédito, llevarían aparejados un riesgo mayor. La criptografía puede ser una bendición para los delincuentes, pero podría decirse que es una bendición aún mayor para los negocios legítimos.
Podría decirse que Internet constituye una mayor amenaza a la privacidad de lo que jamás se podría haber imaginado. La posibilidad de permanecer en el anonimato en el ciberespacio, lejos de ser interminable, aparece como significativamente limitada. Además, la amenaza a dicha privacidad puede provenir tanto de fuentes privadas como gubernamentales. Se da mucha importancia a las llamadas «páginas de *hackers*» y a aquellas salas de chat dedicadas al sexo con adolescentes, muchas de las cuales son accesibles sin dificultad para el gran público. El hecho es que estas páginas pueden ser maravillosas fuentes de inteligencia para las fuerzas del orden o para especialistas en seguridad de la información. Los anales de las fuerzas de seguridad están repletos de ejemplos de oficiales de policía haciéndose pasar por niñas de 13 años que organizan *online* encuentros con sujetos que alguna vez fueron descritos como «hombres viejos y sucios».

[3] Un «*remailer*» en un servidor que recibe correos electrónicos en un formato especial, los procesa eliminando las cabeceras, y los dirige hasta el destinatario del mensaje. Los correos normalmente están aplicados con criptografía (N. del T.).

La amenaza privada a la privacidad

Quizás de mayor importancia es la explotación de información personal por parte de intereses comerciales privados. La cantidad de información personal disponible sobre los patrones de gasto de las personas y las preferencias de los consumidores resulta sorprendente para muchos. En el pasado, la privacidad de la información estaba protegida por la dispersión de datos (Clarke, 1988). Es posible que se haya almacenado una gran cantidad de información personal aquí y allá en varios lugares (ya sean públicos o privados), pero aparte de las principales investigaciones, la engorrosa logística de clasificar habitaciones llenas de formularios en un lugar y otro impidió la recopilación en cualquier escala significativa. Las tecnologías de manipulación de datos que permiten la fusión de bases de datos y la coincidencia de identidades individuales ahora facilitan la agregación de datos de fuentes dispares (Clarke, 1988). El término «*data mining*» (extracción de datos) se usa comúnmente para referirse a tales prácticas. La vinculación de datos dispersos se ve facilitada por la existencia de números de identificación, los cuales son comunes en la mayoría de las sociedades industriales. Así, el número de nueve dígitos de la Seguridad Social en los Estados Unidos constituye un clásico ejemplo. A través de la recopilación de detalles personales dispares, el todo se vuelve más grande que la suma de sus partes.

Uno sospecha que la mayoría de las personas no están recurriendo cada vez más al anonimato, y que sus detalles personales son accesibles en abundancia. Además, estos detalles son comercializados libremente por las empresas de marketing.

Muchas personas que usan el correo electrónico lo hacen con una candidez inusual. En palabras de Bennahum (1999, 102) «el correo electrónico es un suero de la verdad». Pero a diferencia de una conversación cara a cara, las comunicaciones electrónicas no son efímeras. Los registros persisten y pueden volver a perseguir a uno o más participantes en la comunicación. Incluso cuando se borra un mensaje, éste puede haber sido retenido por la otra parte que participa en la comunicación, o puede haber sido «guardado en una copia de seguridad» [4] en uno o más archivos del sistema. Además, muchas comunicaciones resultan accesibles simplemente mediante el uso de tecnología de búsqueda fácilmente disponible. Así, un esposo separado buscó en Internet el nombre de la cuenta de su ex esposa, lo que le permitió recolectar 30 páginas de mensajes que ella había publicado en las salas de chat, y en los que no en todos se reflejaba claramente su condición de madre. Buscando mayores derechos de visita con respecto a sus hijos, el ex marido presentó sin éxito dichos mensajes al mediador en su audiencia de custodia (Glod, 1999).

La dimensión transnacional

Uno de los mayores desafíos planteados por la aparición de la criminalidad digital es el enorme potencial para la delincuencia transnacional. Muchos, si no la mayoría, de los delitos cibernéticos pueden ahora ser cometidos desde el otro lado del mundo tan fácilmente como desde el edificio de al lado. Esto no solo hará que la identificación del autor sea algo más difícil, sino que impedirá en gran medida el enjuiciamiento del delincuente.
A pesar de la trillada afirmación de que el mundo se está encogiendo, las leyes difieren. Algunas jurisdicciones prohíben el acceso no autorizado a un sistema informático, mientras que otras no lo hacen. Algunas consideran que es un delito alterar o borrar datos, mientras que otras no. Naciones como Alemania consideran delito difundir propaganda neonazi. Por muy desagradable que sea ese material, el derecho a hacerlo está protegido por la Constitución de los Estados Unidos de América. Algunas naciones criminalizan el juego *online*, mientras que otras lo ven como una fuente maravillosa de ingresos de exportación.

Se requiere una cierta base legal común para movilizar el ordenamiento de un estado extranjero en favor de alguien. Sin la «doble incriminación», la asistencia de la jurisdicción en la que se encuentra el delincuente es muy poco probable. Pero incluso si hay un cierto grado de consistencia, el cumplimiento de la ley por parte de las autoridades de la nación anfitriona de ninguna manera se producirá de forma automática. Y es que todas las agencias policiales tienen sus prioridades. Si yo, cómodamente situado en Australia, fuera tan tonto como para ser víctima de un fraude de inversión *online* originado en Albania, las autoridades australianas y/o sus contrapartes albanesas podrían tener prioridades más apremiantes. Es posible que «mi» asunto nunca reciba una seria consideración de investigación por parte de las autoridades de ninguna de las dos jurisdicciones.

Implicando a terceros

Las nuevas oportunidades para la delincuencia informática pueden crear nuevas responsabilidades para terceros. Considérese, por ejemplo, la responsabilidad de los empleadores por el mal uso de los ordenadores de oficina por parte de los empleados. Si yo decidiese enviar a un compañero de trabajo un

[4] El autor utiliza aquí la expresión «*backed up*» (N. del T.).

correo electrónico sexualmente ofensivo, mi empleador podría ser responsable por no proporcionar un ambiente de trabajo seguro. ¿Qué grado de respuesta preventiva o reactiva se requeriría por parte de mi empleador para evitar esa responsabilidad?

Aquellas compañías cuyas acciones se negocian en las principales bolsas de valores generalmente están obligadas por sus leyes nacionales a garantizar que la información divulgada sobre la compañía y sus actividades sea completa y precisa. Con el uso cada vez mayor de la *World Wide Web* como medio de relaciones públicas corporativas surgen nuevas responsabilidades de divulgación. Las páginas web de empresas pueden ser pirateadas o imitadas con un realismo asombroso. ¿Con qué frecuencia debería verificarse o actualizarse el sitio web de una empresa para garantizar que la información que contiene es correcta? ¿Qué debe considerarse como un retraso inaceptable cuando se rectifica información errónea? ¿Cuál es el curso de acción apropiado para una empresa que descubre que su sitio web está vinculado a otros sitios web que pueden contener imprecisiones sobre la empresa en cuestión? Sin duda, el futuro presentará varios de estos escenarios, y sería interesante observar cómo se resuelven. Para protegerse contra algunas de estas dificultades, muchas compañías han comenzado a contratar los servicios de consultores que escanean Internet para buscar referencias corporativas (Grabosky, Smith y Dempsey, 2001, cap. 6).

Conclusión

Uno de los principios básicos de la criminología sostiene que el delito puede explicarse por tres factores: motivación, oportunidad y la ausencia de un guardián capaz. Esta explicación puede aplicarse tanto a un incidente individual como a las tendencias a largo plazo. Desarrollado inicialmente para explicar la delincuencia «callejera» convencional, este principio resulta igualmente aplicable a la delincuencia en el ciberespacio. Como hemos visto, los motivos de la criminalidad relacionada con la informática no son nada nuevos. Las tecnologías pueden cambiar rápidamente, pero la naturaleza humana no lo hace así. Los Diez Mandamientos son tan relevantes hoy en día como lo fueron en los tiempos bíblicos. La emoción del engaño caracterizó la inserción del Caballo de Troya original, pero no menos que lo hizo la creación de sus descendientes digitales.

Por el contrario, la variedad y el número de oportunidades para el cibercrimen están proliferando. El crecimiento exponencial en la conectividad de la informática y las comunicaciones crea oportunidades paralelas para los delincuentes potenciales, así como riesgos paralelos para las posibles víctimas. A medida que Internet se va convirtiendo cada vez más en un instrumento para el comercio, se convertirá también cada vez más en un instrumento para el fraude.
El guardián capaz ha evolucionado a lo largo de la historia humana, desde el feudalismo, el surgimiento del estado y la proliferación de instituciones públicas de control social, hasta la era posmoderna en la que los empleados de los servicios de seguridad privada superan ampliamente a los oficiales de policía en muchas democracias industriales. La vigilancia del espacio terrestre es ahora en gran medida un esfuerzo pluralista. También lo es la vigilancia del ciberespacio. Las responsabilidades para el control del delito informático se compartirán de manera similar entre los agentes del estado, los especialistas en seguridad de la información en el sector privado y los usuarios individuales. Hoy en el ciberespacio, lo mismo que en el espacio terrestre hace dos milenios, la primera línea de defensa será la autodefensa.

Descargo de responsabilidad

Las opiniones expresadas en este ensayo son las propias del autor, y no necesariamente se corresponden con las del Instituto Australiano de Criminología o del Gobierno de Australia.

Bibliografía

Bennahum, D. (1999): Daemon Seed: Old Email Never Dies. *Wired* 7.05 (Mayo) 100–11.

Clarke, R. (1988): Information Technology and Dataveillance. *Commun. ACM 31*,5 (Mayo 1988) 498–512. Recuperado de http://www.anu.edu.au/people/Roger.Clarke-/DV/CAC M88.html (consultado el 30 de diciembre de 1999)

Glod, M. (1999): Spouses may delete their marriage, but e-mail lives on as evidence. *Seattle Times* 28/4/99. Recuperado de http: //archives.seattletimes.com/cgi-bin/texis.mummy/ web/vortex/display? StoryID = 3733259942 &query = internet+and+privacy (consultado el 13 de junio de 1999)

Grabosky, P., R. G. Smith y G. Dempsey (2001): *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge: Cambridge University Press.