Pedro Pacheco

Es licenciado en Derecho y también en Ciencias Policiales por la Universidad de Salamanca. Forma parte del Cuerpo Nacional de Policía desde hace 26 años, siempre en el área de Policía Judicial.

Entre los años 1996 y 1998, fue Inspector, Jefe del Grupo de Policía Judicial en la Comisaría de Tenerife. Después de esto y hasta el año 2009, fue Inspector, Jefe del Grupo de Crimen Organizado de Madrid. En el centro de Madrid, desde 2009 hasta 2015, fue Inspector Jefe, Jefe de la Sección de Policía Judicial. Durante los dos años siguientes, de 2015 a 2017, fue Inspector Jefe, Jefe de Homicidios de Madrid. Desde entonces y hasta la actualidad, es Comisario Jefe de la Brigada Central de Investigación Tecnológica.

Comisario Jefe de la Unidad Central de Ciberdelincuencia de la Policía Nacional.

Twitter: @policía

CIBERDELINCUENCIA EN ESPAÑA

Un desafío para el Cuerpo Nacional de Policía

Pedro Pacheco

La ciberdelincuencia, igual que ocurre con la ciberseguridad son conceptos que de un tiempo a esta parte han pasado de ser prácticamente desconocidos para la sociedad en general a adquirir una transcendencia que podría ser calificada de notoria.

Y si bien es cierto que ciberdelincuencia y ciberseguridad son cosas diferentes también lo es que tienen muchos aspectos en común, por ejemplo que el gran protagonismo que han venido adquiriendo está estrechamente ligado a la espectacular implantación que en los últimos años han tenido en nuestras vidas las nuevas tecnologías, especialmente las tecnologías de comunicación e información, comúnmente conocidas como TIC.

Y digo últimos años, porque por ejemplo Internet (sin duda la más conocida e implantada de las nuevas tecnologías) hace apenas cuatro décadas era un mero proyecto, que ha venido evolucionando a pasos agigantados hasta llegar al día de hoy, al presente, en el que estamos hablando de inteligencia artificial, 5G o del Internet de las cosas, es decir el Internet que se integra y lo domina todo, de manera tal que desde un simple teléfono móvil que todos llevamos encima somos capaces de controlar la mayoría de los aspectos de nuestras vidas, desde el correo electrónico, pasando por las alarmas de las casas, el contacto con los profesores de los hijos, la ubicación de nuestros coches, por no hablar de la adquisición de cualquier tipo de producto, etc.

Y si hablamos del ámbito físico o territorial, el auge de las nuevas tecnologías no se circunscribe a determinados lugares del planeta como por ejemplo las zonas más desarrolladas o ricas, sino que su implantación ha sido global, es decir afecta a todo el mundo. Sirva de ejemplo lo que a diario comprueban los policías de fronteras con los inmigrantes que tratan de acceder a España procedentes de zonas tremendamente pobres, y que carecen absolutamente de todo, y su única posesión se ciñe a la ropa que traen puesta y los terminales telefónicos que prácticamente todos ellos portan.

De la confluencia de estos dos ámbitos (temporal y territorial), y unido a la circunstancia que la implantación de las TIC afecta a todas los entornos que conforman el comportamiento humano: cultural, económico, social, laboral, doméstico, etc., podemos aseverar que se ha generado un cambio transcendental en la manera en que nos relacionamos y entendemos el mundo, a lo que coloquialmente se le define como la revolución tecnológica.

Esta revolución de las nuevas tecnologías nos está aportando mayoritariamente cosas buenas, nos está haciendo la vida más cómoda, y nos está generando una calidad de vida que hace unos años era impensable.

Aunque también estamos comprobando que no todo es positivo; también hay un lado negativo, que un número considerable de nuestros conciudadanos se

están valiendo del avance de la tecnología para llevar a cabo actividades delictivas, entrando en el campo de la ciberdelincuencia y los ciberdelincuentes.

En las próximas líneas voy a procurar dar una visión completa de la ciberdelincuencia en España, desde el punto de vista policial fundamentalmente, y para ello, en primer lugar se va a mostrar cuál es la situación real en cifras de la cibercriminalidad en España, es decir los delitos totales que se cometen en el país, para a continuación exponer la respuesta estratégica que ofrece el Cuerpo Nacional de Policía a esa ilícita actividad.

1 *La ciberdelincuencia en España. Cifras*

Antes, es preciso definir qué entendemos por ciberdelincuencia, y si bien es cierto que tradicionalmente se ha asimilado el ciberdelito a aquellos ilícitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos, tales como ataques o intrusiones informáticas, denegaciones de servicio, etc. (comúnmente conocidos como delitos de *hacker*), actualmente y debido al avance de esta modalidad delictiva, al hablar de ciberdelincuencia debemos entenderla en un sentido amplio, es decir, todos aquellos delitos que para su comisión el autor o autores se valen del empleo de las nuevas tecnologías.

Precisando, que si bien es cierto que en este concepto se incluye la comisión de delitos mediante el empleo de sistemas físicos o analógicos (lectores de tarjetas, microcámaras espía, grabadoras, etc.), la gran mayoría de estos hechos ilícitos en la actualidad son cometidos a través de Internet.

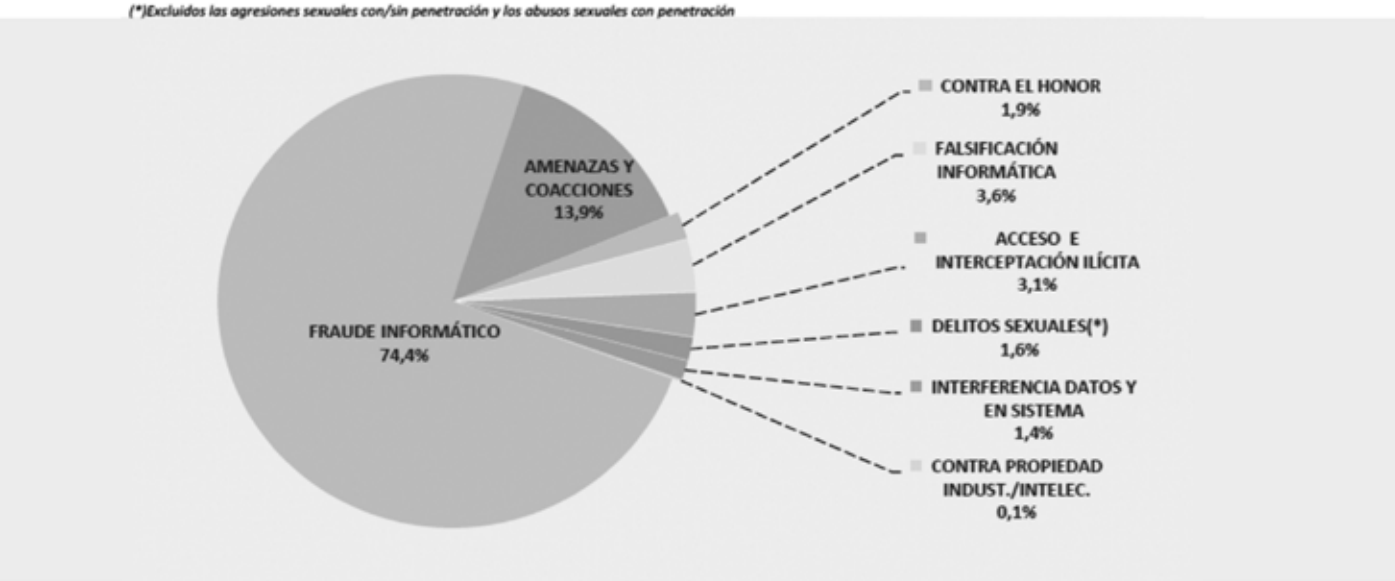
Partiendo de este concepto amplio, en la siguiente imagen se muestra la realidad de la ciberdelincuencia en España. Estos datos se han extraído del informe de cibercriminalidad elaborado anualmente por la Secretaría de Estado de Seguridad, dependiente del Ministerio del Interior, y muestra por años los hechos conocidos (denuncias de ciudadanos más la suma de las actuaciones policiales) en territorio de Policía Nacional y Guardia Civil desde el año 2014 al 2017, significando que el informe de el año 2018 al día de elaboración del presente aún no se había publicado.

La tabla inferior (circular) nos muestra los datos porcentuales sobre el total de cada uno de los diferentes delitos tecnológicos, siendo de destacar el fraude informático, que supone el 74,4 por ciento del total.

La primera tabla muestra tanto el número total de hechos de todos los delitos que pueden ser cometidos a través de las nuevas tecnologías como el cómputo global de todos ellos por años.

HECHOS CONOCIDOS	2014	2015	2016	2017
ACCESO E INTERCEPTACIÓN ILÍCITA	1.851	2.386	2.579	2.505
AMENAZAS Y COACCIONES	9.559	10.112	11.473	11.270
CONTRA EL HONOR	2.212	2.131	1.524	1.537
CONTRA PROPIEDAD INDUST./INTELEC.	183	167	121	109
DELITOS SEXUALES(*)	974	1.233	1.188	1.312
FALSIFICACIÓN INFORMÁTICA	1.874	2.361	2.697	2.961
FRAUDE INFORMÁTICO	32.842	40.864	45.894	60.511
INTERFERENCIA DATOS Y EN SISTEMA	440	900	1.110	1.102
Total HECHOS CONOCIDOS	49.935	60.154	66.586	81.307

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Lo más importante, desde el punto de vista policial, es observar las tendencias que se registran año tras año, pudiéndose comprobar cómo en los últimos años en España la delincuencia tecnológica viene aumentando en torno a un 14 por ciento anual, señalando que esta tendencia de incremento se ha mantenido durante todo el año 2018 y los cinco primeros meses de 2019.

Es preciso significar que los delitos que no requieren para su ejecución el empleo de tecnología, llamémoslos "tradicionales", especialmente los del orden socioeconómico, viene sucediendo todo lo contrario, en los últimos años tienden a mantenerse o disminuir, lo que significa que estamos siendo testigos de un cambio de tendencia en la criminalidad a favor de la delincuencia tecnológica.

2 *Estrategia del Cuerpo Nacional de Policía*

En base a los datos expuestos, nos podemos preguntar qué tipo de respuesta ofrece el Cuerpo Nacional de Policía a sus ciudadanos para hacer frente a este incremento de hechos y al desafío que empieza a suponer la ciberdelincuencia.

Para dar respuesta a esta cuestión se debe hacer mención al Plan Estratégico Institucional (PEI) elaborado por la Dirección General de la Policía para el periodo 2017-2021 en el que se definen cuáles son los grandes objetivos que se pretenden conseguir por la institución policial en ese periodo de tiempo.

Este PEI además de considerar la lucha contra la ciberdelincuencia como un área prioritaria de actuación, lo incluye como uno de los grandes objetivos estratégicos con la siguiente definición: "Prevenir y luchar contra la Ciberdelincuencia potenciando la ciberseguridad", que a su vez se concreta en tres objetivos específicos:

1. Detectar las amenazas y vulnerabilidades de los sistemas informáticos
2. Potenciar la atención al ciudadano, prestando especial atención a las redes sociales y a la lucha contra la explotación sexual infantil
3. Luchar contra el fraude en Internet

La Unidad encargada de hacer cumplir estos objetivos es la Unidad Central de Ciberdelincuencia, encuadrada dentro de la Comisaría General de Policía Judicial y que presenta la siguiente estructura:

Esta unidad, dentro del Cuerpo Nacional de Policía, es la competente para llevar a cabo la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y la comunicación (TIC) y el ciberdelito de ámbito nacional y transnacional, y está compuesta de tres brigadas:

1. Brigada de Seguridad Informática

Es la encargada de cumplir el primer objetivo: detectar las amenazas y vulnerabilidades de los sistemas informáticos.

Las investigaciones que desarrolla esta brigada están relacionadas con la ciberseguridad, ataques informáticos a sistemas de información y telecomunicaciones cometidos por personas u organizaciones criminales valiéndose de medios técnicos avanzados y que pretendan cualquier objetivo, fundamentalmente el patrimonial.

Tipología penal: ataques o daños informáticos, denegaciones de servicio distribuido (Ddos), malware, distribución ilícita de señal a través de sistemas de *Cardsharing*, IPTV, OTT streaming. También investigaciones relacionadas con divisas virtuales y criptomonedas: seguimiento de transferencias en *blockchain*, de *exchangers*, *mixers*, etc.; seguimiento de divisas virtuales usadas e interacción entre las mismas.

Es una brigada transcendental, pues esta actividad delictiva tiene la virtualidad que un único sujeto activo (autor) puede causar miles y miles de víctimas e incluso causar desestabilizaciones de instituciones.

Sirva como ejemplo de la actividad desarrollada por los componentes de esta brigada una investigación, la Operación Carbanak, culminada el año pasado, y en la que contamos con el apoyo operativo del FBI norteamericano, en la que fue detenido uno de los más importantes cibercriminales de la historia, Denis T., asentado en España, líder de una organización internacional, especializada en la creación de un tipo de *malware* que una vez introducido en los servidores informáticos de las entidades bancarias conseguían tomar el control de los sistemas críticos del banco. Esto les permitía alterar saldos de cuentas controladas por la organización; modificar cuentas destinatarias en transferencias de alto valor, o directamente gestionar de forma remota los cajeros automáticos para vaciarlos. La organización criminal consiguió a lo largo de su actividad tomar el control de la red de un número considerable de bancos de ubicados tanto en Rusia, como en las antiguas repúblicas de la

Unión Soviética, calculándose que los beneficios obtenidos por estas sustracciones pudieran superar los mil millones de dólares. Las ganancias de cada ataque, que superaban el millón y medio de dólares como media, eran convertidas inmediatamente en criptomonedas (especialmente *bitcoins*) para facilitar su movimiento en una red internacional de blanqueo de capitales.

Es preciso señalar, que esta práctica de convertir el dinero monetario en dinero virtual o criptomoneda se está convirtiendo en los últimos meses en algo habitual entre las organizaciones criminales dedicadas a estos sofisticados ilícitos, todo ello con el fin de dificultar el rastreo policial del dinero, pues a diferencia de lo que sucede en una cuenta corriente bancaria, que va asociada a una numeración, en las criptomonedas lo que ocurre es que cualquiera puede generarse su propio número de cuenta, con el hándicaps que estas cuentas son aleatorias y no se puede predecir de antemano, ni conocer a que persona están asociadas. Su funcionamiento se basa en un sistema criptográfico público/privado que garantiza el anonimato de la persona que tiene el acceso a esa dirección y que puede gestionar el monedero virtual.

2. Brigada de Investigación Tecnológica

Esta brigada es la competente para aplicar el segundo objetivo: potenciar la atención al ciudadano, prestando especial atención a las redes sociales y a la lucha contra la explotación sexual infantil.

Si el primer objetivo específico se refería a la ciberseguridad y al ciberespacio, este segundo está claramente orientado a los internautas, a la seguridad de las personas en sus interacciones más comunes y en la protección de los más débiles.

Tipología penal: delitos contra la libertad sexual de menores de edad a través de Internet, pornografía infantil, corrupción de menores, sextorsión, *sexting*, ciberengaño pederasta o *child grooming*, acoso, extorsiones, amenazas, coacciones, delitos de odio, tráfico de medicamentos, etc.

Uno de los cometidos prioritarios de esta brigada es la lucha contra la explotación sexual infantil a través de Internet, concretándose sus investigaciones tanto en tratar de localizar los centros de producción de pornografía infantil, como en tratar de detectar la distribución de pornografía a través de la red, cuyos autores por norma general no tienen conexión entre sí, sino que intercambian archivos a través de grupos privados en multitud de plataformas y canales privados en redes sociales o bien mediante programas de intercambio tipo *peer to peer*.

De la experiencia adquirida en el desarrollo de investigaciones en la que los sujetos pasivos o víctimas son menores de edad, se puede concluir que en esta nueva realidad que es Internet y la ciberdelincuencia, si hay un sector social vulnerable en el que se ceban las nuevas formas de comisión de delitos es el de los menores, muchos de ellos ya "nativos digitales", y a pesar de ello o quizás por ello son objetivo de los delincuentes que se esconden tras las redes sociales, en un porcentaje notable con intenciones de índole sexual.

Uno de los cometidos prioritarios de esta brigada es la lucha contra la explotación sexual infantil a través de Internet, concretándose sus investigaciones tanto en tratar de localizar los centros de producción de pornografía infantil, como en tratar de detectar la distribución de pornografía a través de la red

Ante lo expuesto, surge la pregunta ¿existe un perfil de depredador sexual pedófilo en Internet? A lo que cabe responder que en base a la información obtenida en las múltiples investigaciones desarrolladas a lo largo de los años, se puede afirmar que no existe un perfil psicológico específico del pedófilo que actúa en Internet. No existen tramos de edad, antecedentes penales previos, patologías psicológicas o cualquier otra característica que permita diferenciarlos de las demás personas.

Podríamos decir que, por regla general, se trata de personas normales, cuya única diferencia es que el objeto de su deseo sexual reside en los niños y cuya satisfacción se realiza en su ámbito más personal e íntimo, su casa, y a través de un medio que permite su separación respecto a las víctimas, Internet.

Otra de las funciones encomendadas a esta brigada es la continua navegación y presencia en la red para detectar nuevos *modus operandi* y monitorización de posibles actividades ilegales para su consiguiente investigación, así como el control, seguimiento y análisis preventivo de los contenidos publicados en Internet, especialmente en redes sociales.

Policialmente se conoce esta actividad como ciberpatrullaje. Los agentes la llevan a cabo tanto en la web pública como en la *Dark Web*. En la primera, quedan registrados nuestros datos de conexión a través de la IP que nos asignan las proveedoras. Por otro lado, la *Dark Web* es la red no pública en la que los usuarios pueden navegar de manera anónima, sin que se registren sus datos de conexión. Para acceder a esta se requiere de unos navegadores específicos, siendo el más utilizado el denominado Red TOR (The Onion Router) cuya característica principal es que cifra y encripta las comunicaciones y oculta los números IP de identificación de los terminales.

Este anonimato conlleva que sea utilizado por la delincuencia para llevar a cabo todo tipo de acciones delictivas y de ahí la transcendencia del control policial.

3. Brigada de Fraudes Informáticos

Es la competente para tratar de cumplir el tercer objetivo: luchar contra el fraude en Internet (intensificar la respuesta policial sobre las estafas cometidas a través de las TIC).

Este objetivo específico está orientado a la actividad económica y a la industria financiera; al mantenimiento y protección del patrimonio y la investigación de todos los delitos contra el orden socioeconómico cometidos tanto a través de Internet como a través de las nuevas tecnologías. Si bien es cierto, como se ha podido constatar, que el aumento de los delitos tecnológicos afecta absolutamente a todos los bienes jurídicos protegidos (que sean susceptibles de ejecución a través de las nuevas tecnologías), es especialmente significativo en los delitos contra el patrimonio, pues suponen aproximadamente el 75% de todos los delitos denunciados.

Con respecto a los mencionados delitos contra el patrimonio, los mismos mayoritariamente se corresponden con fraudes o estafas cometidos a través de Internet, de los que el 70 % aproximadamente de los hechos se corresponden con el delito de *carding*, así denominado al uso ilegítimo de las tarjetas de crédito o débito titularidad de otras personas con el fin de obtener productos o dinero fraudulentamente. Las víctimas o perjudicados denuncian los cargos no autorizados por ellos que, mayoritariamente, son compras realizadas a través de páginas webs ubicadas en países extranjeros.

Significa que para llevar a cabo este tipo de estafas los delincuentes necesitan tener los datos contenidos en las tarjetas de créditos, los cuales son obtenidos bien mediante clonaciones físicas de las tarjetas en cajeros automáticos (*skimming*) o establecimientos comerciales, bien mediante las clonaciones virtuales de las tarjetas cuando se realizan compras a través de Internet en páginas poco seguras, bien obtenidos mediante *phising* (suplantación de empresas o personas para conseguir los datos bancarios de la víctima), o bien mediante ciberataques a los servidores o bases de datos de empresas donde se guardan datos de los clientes.

El ciberpatrullaje se lleva a cabo tanto en la web pública como en la Dark Web. En la primera, quedan registrados nuestros datos de conexión a través de la IP que nos asignan las proveedoras. Por otro lado, la Dark Web *es la red no pública en la que los usuarios pueden navegar de manera anónima sin que se registren sus datos de conexión. Para acceder a esta se requiere de unos navegadores específicos.*

Otro 15 % aproximadamente de los hechos se correspondería con estafas en compras o ventas de todo tipo de productos en páginas especializadas, entre los que se incluyen entradas a conciertos o eventos deportivos a través de Internet, productos de segunda mano, etc.

Y el 15 % restante aproximadamente, se correspondería con un conglomerado de fraudes que tienen como eje común el engaño a las víctimas y entre las que cabe destacar las estafas en alquileres, normalmente vacacionales, de inmuebles anunciados en páginas web creadas por los estafadores con un diseño web similar a otras de reconocida solvencia que inducen a error a los usuarios. Destacan también los conocidos como *Fraudes del CEO,* en los que los ciberdelincuentes se hacen pasar por un alto cargo de la empresa que pretende estafar; contactan, generalmente vía correo electrónico, con un empleado cualificado de la organización con la capacidad necesaria para hacer trasferencias o pagos importantes, y lo engañan para efectuarlo.

3 *Implantación de una cultura de la ciberseguridad*

No me gustaría finalizar el presente artículo sin dejar de mencionar como desde Policía Nacional, ante el desafío que supone el auge de la ciberdelincuencia, no solamente se están adoptando medidas de carácter operativo, como las hasta aquí plasmadas, sino que también se están llevando a cabo otras de carácter preventivo, que consisten en tratar de aconsejar e incluso educar a los ciudadanos de los riesgos asociados al uso de las nuevas tecnologías, bien a través de los exitosos perfiles institucionales creados por Policía Nacional en las más conocidas redes sociales, bien a través de las charlas y seminarios en materia de ciberseguridad impartidos en todos y cada uno de los centros educativos de nuestra jurisdicción, bien a través de cualquier tipo de foro que nos haga llegar al más amplio espectro de la sociedad.

Todo ello con el fin de tratar de implantar en la ciudadanía una cultura de la ciberseguridad, asumiendo que es un problema que requiere de una respuesta integral por parte de todas las administraciones, no solo de carácter policial, desarrollando políticas de prevención, incluso desde el inicio de su periplo formativo en la escuela, ya que se está manifestando un uso generalizado, poco responsable, de las tecnologías de la información y la comunicación.

Concluir mencionando las excelentes relaciones que mantiene el Cuerpo Nacional de Policía con las diferentes agencias de investigación norteamericanas, especialmente con el FBI a través de sus enlaces de la embajada norteamericana en Madrid. Son diversas las áreas de ciberdelincuencia en la que colaboramos habitualmente, pero posiblemente por su transcendencia cabe mencionar dos, los delitos vinculados con la ciberseguridad y los relacionados con la pornografía infantil, significando que las más transcendentales compañías tecnológicas y proveedores de Internet son estadounidenses y se rigen por tanto por leyes de aquel país, resultando fundamental para poder culminar con éxito las investigaciones relacionadas con las nuevas tecnologías esta excelente armonía policial.