Título: *Relaciones con el sector privado. Investigación de delitos tecnológicos. La recogida y tratamiento de la evidencia digital*

Ponente: José Manuel Colodrás. Inspector Jefe de Sección Técnica de la Brigada de Investigación Tecnológica. Dirección General de la Policía.

Mi lenguaje quizá no tenga la finura jurídica de las ponencias anteriores; tampoco utilizaré muchas palabras "chelis" para que no carezca de una base teórica o medianamente seria. Mi papel no es de un ingeniero informático o un juez o un letrado con mucha experiencia. Para ser policía en nuestra brigada hay que tener una pata en cada sitio, hay que ser un poco jurista, conocer los rudimentarios procedimientos jurídicos para ejercer nuestro trabajo, a veces no tan rudimentario en lo que se refiere al procedimiento penal, y, por otro lado, hace falta tener conocimientos técnicos. Cuantos más tengamos, mejor. Pero no somos ingenieros ni dedicamos todo nuestro trabajo a lo que es nuestra formación técnica. Nuestros jefes tampoco consideran que sea lo más importante; lo más importante, y en el fondo hay que estar de acuerdo con ellos, es hacer detenidos, prestar una labor de servicio publico y aumentar la sensación de seguridad ciudadana.

En ese sentido, hay que decir que nuestros jefes son magníficos gestores, ya que gastando poquísimos recursos en lo que es nuestra formación y nuestra especialidad, consiguen que tengamos una gran eficacia policial. Por ejemplo, en nuestra brigada, que voy a presentar a continuación, ahora mismo somos mucha gente. Somos más de 30 personas y llevamos, en lo que va de año, más de 340 detenidos. Esa es una cifra muy grande para una brigada especializada en investigación de delitos tecnológicos y creo que la experiencia en España de la Policía Nacional, la Guardia Civil, los Mossos d'Esquadra e, incluso, la Ertxaintxa, es de gran eficacia policial en comparación con otras policías del mundo en lo que se refiere a la investigación de delitos informáticos. Aprovecho ya que estoy aquí para decir que en esta sala también hay compañeros y colegas de la Guardia Civil y de la Policía Nacional.

Voy a presentar un poco mi brigada y la policía nacional en lo que se refiere a la investigación de delitos tecnológicos. Lo primero es decir que la Brigada de Investigación Tecnológica , la BIT, es una unidad central. Es decir, tenemos nuestra

sede en Madrid y competencia en todo el territorio nacional, somos como una especie -salvando las distancias para lo bueno y para lo malo- de FBI. Nos desplazamos a cualquier sitio para ayudar a nuestros compañeros del cuerpo nacional siempre que somos requeridos para ello o cuando la investigación sea una investigación que afecte a varias Comunidades Autónomas o jefaturas superiores en nuestra división territorial. Aparte de nuestra brigada central, en el último censo que hemos hecho hace tan sólo un mes, en España se dedican a la investigación de delitos tecnológicos de forma exclusiva o parcial, compartiéndolo con otras actividades como investigación de delincuencia económica o investigación de delitos contra la propiedad intelectual no por Internet, un total de 246 personas en diferentes grupos repartidos por el territorio. Eso quiere decir que, aunque nosotros no tengamos la pericia tecnológica que puedan tener determinadas empresas privadas como es Cybex o incluso otras policías del mundo, sí tenemos una capacidad que nosotros y otras policías y la Guardia Civil que quizá no la valoramos bastante, pero que es muy importante. Somos capaces de llegar al último pueblo, al último rincón de España simplemente levantando el teléfono y pidiéndole ayuda a los compañeros de Barcelona o de Lérida o de cualquier sitio. Esto nos permite tener una capacidad de gestión enorme y permite que, a pesar de tener (como ha dicho muy bien el Magistrado Maza) una escasez enorme en cuanto a formación y sobre todo de medios tanto humanos como materiales, tengamos una gran eficacia policial. Y eso es algo que no ocurre en muchas policías del mundo. Pensemos, por ejemplo, en Estados Unidos, donde hay cientos de agencias tanto federales como estatales o locales y donde no existe esa infraestructura que nosotros, como Fuerzas de Seguridad del Estado, sí tenemos.

Una vez dicho esto, decir que hay un equipo de 246, más nuestros 30 funcionarios que forman la unidad central. Voy a explicar brevemente a qué nos dedicamos y, de alguna forma, ofrecer nuestros servicios diciendo también que hay una unidad de la Guardia Civil que se dedica a lo mismo. Intentamos no solaparnos pero a veces llevamos las mismas investigaciones, incluso algunas son conjuntas cuando han empezado por las dos vías. Ahora mismo somos 7 grupos, más mi sección técnica. Estamos divididos en estas 3 áreas. Hay una sección operativa primera que se dedica a fraudes en Internet, (probablemente éstas son las modalidades delictivas más comunes) y abarca simplemente la utilización fraudulenta de números de tarjeta válidos de un usuario como su legítimo tenedor -las cartas nigerianas- que, digamos, es la actualización del

timo de la estampita. Recibimos esos correos que nos ofrecen ganancias por ayudar a una persona que está en Nigeria o en cualquier país del África subsahariana a sacar una cantidad, por ejemplo, de dinero de una cuenta que está intervenida. Esto que nos puede parecer que es algo que la gente no pica, que hay que ser muy ingenuo y que no debe ser un delito muy común, hay que decir que sí lo es. Es más común de lo que nos creemos y muchas veces la gente -por vergüenza- no lo denuncia a la policía. Pero no solamente hay que preocuparse por su trascendencia económica; está estudiado que la segunda fuente de riqueza de Nigeria, después de la exportación de crudo de petróleo, está precisamente en estos timos que se conocen como timos "nigerianos" o "cartas nigerianas". Estamos hablando de un país de 70 u 80 millones de habitantes. África no deja de tener su peso en el mundo y éste quizá sea el segundo país de África con más ingresos. Pero no solamente la incidencia económica es importante (sirva también como aviso a navegantes). Se han producido muertes, secuestros de personas que han caído en manos de estas mafias y es un delito bastante grave.

Más delitos que se dan en el ámbito de Internet, por ejemplo, están las subastas en ebay. Lo anterior era una especialidad de los nigerianos, esto es una especialidad de los rumanos. Cada país tiene su especialidad. Dos delitos que se están produciendo cada vez más y que nos preocupan muchísimo, sobre todo por su alta incidencia y por estar llevados a cabo por grupos del crimen organizado de toda la vida como por mafias rusas y organizaciones por el estilo, es el *fishing* y los chantajes a empresas. Se trata de chantajes de eliminación de servicios o de robo, de daños, o de robo de información. Por ejemplo, en el caso del chantaje sabemos que existen muchos más chantajes de los que nos denuncian y yo animo a las empresas a que pongan en conocimiento de las Fuerzas del Estado -en concreto de nuestra Brigada que nos abrimos a todos vosotros- esos hechos delictivos. El chantaje es una cosa que se produce con más habitualidad de la que somos conscientes. En cuanto al *fishing,* la cosa cambia. Tenemos conocimiento de muchos casos de *fishing*. Para los que no estén asociados con este tipo de terminología es básicamente el envío de SPAM o correo no deseado de una forma masiva a cientos de personas en los que se dice que actualicen sus datos de carácter personal para acceder a una página de banca electrónica y, para ello, da un enlace a una página que es una falsificación o una copia alojada en otro lugar de la página original. La entidad más atacada es Citybank porque

es una corporación de bastantes bancos y en España hemos tenido ejemplos desde hace dos años de este tipo de ataques. Una vez que se consiguen estos datos, el fraude consiste en que se utilizan estas informaciones para hacer transferencias no consentidas de fondos de las personas a otras entidades. Esto ha alcanzado tal volumen que incluso hay un protocolo en el que ha participado también la Guardia Civil o el Cuerpo Nacional de Policía para intentar evitarlo; entre otras funciones tiene la de filtrar o impedir que desde España (cuando se produce a una entidad financiera española) se acceda a servicios, a páginas web falsas, etc. que están alojados en el extranjero, en Estados Unidos, en servidor gratuito, en cualquier parte del mundo, en China etc. Esto previene o palia el posible perjuicio que se haga a los clientes de esa entidad financiera. Pero no lo lleva el grupo de fraudes en Internet, sino el de seguridad lógica, del que voy a hablar ahora mismo.

Ha salido en la prensa que el viernes pasado alguien colocó en una web de Estados Unidos una página que se dedica a cuestiones de tipo *gore*: una serie de imágenes, videos y fotografías de los atentados del 11- M en Madrid, imágenes realmente desagradables. El juez Del Olmo de la Audiencia Nacional se puso en contacto con nosotros y nos pidió que eliminaramos esa página, lo cual es imposible o muy difícil para nosotros. Tendríamos que pedírselo a las autoridades americanas o, en su defecto, lo que hicimos que fue utilizar el mismo protocolo utilizado para el *fishing* para impedir el acceso desde España a esa página. Problemas: realmente no se puede eliminar esa página porque, según los derechos recogidos en la Constitución de EE.UU., existe en la primera enmienda alusión a la libertad de expresión y esta página, en concreto, se acoge a este derecho fundamental. Aunque a los americanos tampoco les gusta mucho lo que están haciendo, realmente no pueden quitar ese contenido. Lo único que podemos hacer -como he dicho- es filtrar el contenido de los principales proveedores de servicio de Internet en España para que desde España, al menos, no se pueda acceder de una forma normal; por supuesto, se puede acceder seguramente a través de un proxy y por otras formas que evitan este filtrado.

Y llego al segundo grupo del que quiero hablar: la seguridad lógica. El *hacking* tiene una importancia grande para las empresas porque también se dedica a cuestiones de chantaje. Son cuestiones que, en principio, atañen a la seguridad pública o a la moral pública porque realmente no es un delito publicar esas imágenes, salvo que se

demuestre que han salido de datos policiales, en cuyo caso podría entenderse la revelación de un secreto sumarial o algo por el estilo. El equipo de seguridad lógica se dedica a incursiones, daños, usurpación de identidad, descubrimiento y revelación de secretos y tiene también una relación bastante estrecha con las empresas privadas. La propiedad intelectual en nuestra brigada solamente se refiere a lo que entendemos que son los fraudes a través de Internet, sobre todo, aplicaciones *peer to peer* y a la venta o el anuncio de software ilegal en la web, aunque también hemos realizado otras misiones que casi tienen más que ver con la propiedad intelectual, como es la falsificación de *coarses* por grupos organizados que se dedican a este tipo de delitos.

En cuanto a nuestra sección operativa segunda, hay dos grupos aunque aquí se está tratando como un área: la de protección al menor en las nuevas tecnologías. Es probablemente donde más hincapié hacemos porque es un tema muy sensible, lógicamente, y hay que decir que en este mismo mes de octubre ha entrado en vigor la nueva reforma del Código Penal y es la segunda ya en lo que se refiere a estos delitos. Por fin en España se pena la posesión de pornografía infantil. Hasta ahora solamente estaba tipificada la ejecución, lógicamente, porque estamos hablando de una violación o agresión sexual cuando hablamos de la producción y la distribución, pero no la posesión.

Por último, está el grupo de fraude en las telecomunicaciones, que tiene gran incidencia en el sector privado. Es el que se refiere a locutorios clandestinos, la utilización de la tecnología voz sobre IP para cometer determinados fraudes en la contratación de líneas y también todas las plataformas digitales, radio y demás fraudes que se producen a ese nivel.

Por último y de forma residual, nos queda casi lo que más trabajo da a la policía, que son las injurias, amenazas y calumnias. Esa cuestión intentamos que se quede a nivel de comisaría local, de distrito, como mucho que llegue a las jefaturas superiores pero también nos llega a nosotros en muchas ocasiones. Si bien en la mayoría de los casos este tipo de amenazas son como una simple falta, no llega a la consideración de delito. El típico caso es el (que es un caso real, por cierto) del vecino del 2º que está enfadado con su vecina del primero porque cuando llega ésta de trabajar a las 10 de la

noche pone la lavadora y no le deja descansar. Este señor pone un anuncio en un foro de Internet, en un foro de relaciones, anunciando “soy fulanita de tal, una mujer muy ardorosa y quiero mantener relaciones sexuales con chicos de 20 a 60 años”. Un juez quizá lo considere como una simple falta, pero la verdad es que para la señora que le hacían esto -que no sabia *a priori* de quién se podía tratar- es una faena. Hay que hacer todo un estudio técnico, hay que obtener las evidencias digitales como veremos más adelante y, a lo mejor, resulta ser una cosa poco grave.

Todas esas conductas que en muchos casos son particulares y en muchos casos son privadas tienen su relevancia penal y es frecuente que cuestiones laborales, mercantiles o civiles también estén relacionadas con el ámbito penal. Por eso yo considero que es importante que sepáis que existimos, tanto nosotros como la Guardia Civil. Trabajo no nos falta, y a ellos tampoco, me consta. Y, por supuesto, podéis elegir cualquiera de las dos vías. Existimos, somos un servicio público que en principio no cobramos nada por hacer un trabajo; lógicamente, tenemos algunas limitaciones pero intentamos superarlas con otras herramientas.

Esas son las funciones de nuestra brigada, como ya les he comentado y ahora comentaré otras, como es la labor de formación o relaciones internacionales institucionales. También tenemos una labor de autoformación, ya que muchas veces la formación externa está fuera de nuestro alcance por la falta de medios.

Digamos que hay dos momentos en que se puede hablar de evidencia, o de huella digital (que no dactilar) o de prueba digital, que aunque tienen la misma semántica y casi el mismo origen, no tienen nada que ver… Hay que decir que la policía tiene una larga tradición en lo que se refiere a la investigación desde el punto de vista pericial de policía científica de todas estas evidencias. El primer momento en que nos encontramos con lo que podría ser un prueba pericial es el momento de la denuncia, cuando nos presentan una denuncia. Normalmente las denuncias son testimonios que nosotros recogemos en un papel normalizado y pasamos a los juzgados. En el caso de los delitos tecnológicos, siempre intentamos empezar a aportar ya evidencias, que pueden ir desde la impresión en pantalla, los *logs* de una máquina, las cabeceras técnicas del mail, algo grabado, películas hasta filmaciones de lo que ocurre en un ordenador etc. Realmente esto es una copia del original. Esto es la representación de

este soporte físico. De todas formas -como ha dicho muy bien el juez- como existe la libre valoración de las pruebas por parte del juez, normalmente el testimonio escrito o una impresión en pantalla se admite como una evidencia digital y es en un primer momento cuando tenemos que ser cuidadosos a la hora de las evidencias digitales; es decir, no alterar cuando recojamos o cuando el denunciante nos aporte esta denuncia y no alterar las evidencias digitales porque quizás *a posteriori,* en el juicio oral, haya que contrastarla. La presentación magnífica de Matías Bevilacqua se refería a que fácilmente se alteran las pruebas digitales, por eso en el momento de recogida de la denuncia es importante que la empresa, el particular o la institución publica se ponga en contacto con la policía para, de alguna manera, intentar salvaguardar esta integridad de las pruebas digitales. Una recogida inadecuada, incluso en este momento cuando todavía no se ha empezado a hacer el análisis forense, puede alterar todo lo que sea *a posteriori.*

También cabe la posibilidad -a muchas empresas les ocurre pero a particulares no- de hacer un testimonio notarial de lo que está ocurriendo en ese momento en las máquinas. Es una cosa muy útil, tiene mucho valor añadido en el juicio y en algunos casos es casi necesario porque no quedan *logs* recogidos. Es otra posibilidad que hay que estudiar y que se puede plantear. En algunos casos, la policía puede actuar en perjuicio (la policía o los fiscales) ante el conocimiento de cualquier hecho investigado, salvo en el caso de las injurias, calumnias y amenazas a particulares. Ahora, con la reforma del Código Penal, siempre que sea autoridad o agente de la autoridad o funcionario público, se puede actuar de oficio. Pues esta necesidad es instrumental en el resto de los delitos; nosotros no podemos saber que le están haciendo chantaje a una gran corporación si ésta no nos lo cuenta. Necesitamos la colaboración de las instituciones y del sector privado para poder perseguir los delitos. También hay un pequeño cambio en el artículo 270 del Código Penal y ya no necesitamos la denuncia de parte para perseguir los delitos contra la propiedad intelectual, siempre que se den los demás elementos.

En cuanto a las relaciones con el sector privado institucional, que es algo en lo que me gustaría incidir pero quizá me he extendido demasiado presentando nuestra brigada, quisiera decir que no necesariamente están basadas en la denuncia. Por lo menos mi brigada -y me consta que en los grupos que están en jefaturas superiores- no es una

mera oficina de denuncias donde se van a denunciar unos hechos y se pasan a un juez. Sin ser una consultaría o algo por el estilo, también estamos abiertos a que vengáis a hablar con nosotros y a que nos contéis los problemas que tenéis; luego os diremos si es conveniente o no hacer la denuncia o en qué sentido atacar el problema. Pero, por supuesto, para este tipo de delitos -donde hay tantas relaciones con el sector privado- tener una relación fluida con el mismo es esencial. Por comentar un ejemplo: en el Reino Unido se crea hace unos años el Nacional High Technology Crime Unite, que es una unidad que tiene dos años de existencia, un presupuesto de más de 6 millones de euros para esos dos años y 50 policías, personal del Ejército, de la Administración, etc. Prácticamente el 70-80% de sus recursos no se dedican a la investigación, ni siquiera a la coordinación de las investigaciones, sino a las relaciones con el sector publico y privado y a las relaciones con los actores externos porque la información y el conocimiento de lo que pasa y el tener una relación fluida (de confianza) con el sector privado es fundamental para conocer los delitos y poder investigarlos correctamente. También a veces servimos de enlace con el extranjero, con otras policías, como una forma de facilitar la resolución de problemas que, para una empresa mediana e incluso grande, son difíciles de solventar. También es muy interesante esto para tener un conocimiento de la realidad, de lo que ocurre en la Red, de lo que ocurre en Internet.

En cuanto a la recogida de evidencias digitales o pruebas digitales, hay que hablar de tres momentos. En los orígenes, cuando no existían ni siquiera grupos de investigación de delitos informáticos, antes del año 1995 (cuando yo empecé se le llamaba grupo de delitos informáticos) había una total falta de especialización. Cuando había cualquier problemilla, cualquier cosa de informática, había que acudir inmediatamente a instituciones y empresas externas. Realmente eso de la informática no iba con el policía, era algo totalmente ajeno a él. A partir del año 1995 se crea el primer grupo de delitos informáticos de la policía en la comisaría general de policía judicial. Creo que en 1996 se crea un grupo análogo en la Guardia Civil y empieza a haber una especie de especialización. Se empieza a ver que hay que precintar el ordenador, de una forma muy lógica, tapando todos los dispositivos de entrada y salida del ordenador y que la secretaría judicial, además de recogerlo en su acta, también tiene que firmar para precintarlo adecuadamente. Saber cómo se recoge un

disquete y, por supuesto, saber recoger lo más precisamente posible todo lo que se hace en esa entrada de registro (aunque muchas plantillas todavía no han pasado de la segunda fase y, generalmente, no existen los medios ni los conocimientos para hacerlo).

Cada vez más se usa un sistema muy parecido al que ha explicado Matías Bevilacqua, que es la utilización de herramientas forenses y utilización de protocolos propiamente policiales en forma de actuación. Es precisamente lo que haría una empresa privada. Es muy parecido, por no decir que las herramientas son prácticamente las mismas y que los procedimientos son iguales.

Para solventar determinados problemas, cuando no llegamos más allá o cuando no nos interesa utilizar estas herramientas, también tenemos otros sistemas. Vamos a pensar que -como Matías muy bien ha dicho- para recoger cualquier evidencia digital lo primero que hay que hacer es una imagen, un clonado, una imagen *bit* a *bit* de estas evidencias porque si no se van a alterar. Sin embargo, esto implica tiempo y a veces la policía no tiene tiempo. Pensemos en los atentados del 11-M y vamos a suponer que llegamos al registro domiciliario de uno de los sospechosos. Hay que valorar, si el policía -o el experto policía- tiene tiempo para emplear dos horas, hacer un volcado de todo este ordenador y empezar a investigar realmente… o nos arriesgamos y, sabiendo que vamos a destruir muchísimas pruebas que pueden ser importantes, de todas formas nos vamos a meter directamente en el ordenador para sacar lo que está porque lo necesitamos para la investigación. O en otros casos: cuando un ordenador está conectado a Internet y está conectado a una partición de un disco duro remoto que está conectado en China (vamos a suponer), donde tiene muchas evidencias, si yo no conecto mi dispositivo USB a ese ordenador o un disquete y grabo la información que está en ese servidor de China, una vez que desconecte el ordenador para hacer la imagen forense, esa información la habré perdido. Eso es algo que hay que valorar y que hay que valorar desde el punto de vista policial. Entonces, en el futuro próximo no solamente habrá que tener expertos policiales para hacer todas estas imágenes, imágenes con todas las garantías técnicas utilizando la tecnología de la firma digital, por ejemplo, sino que los jueces y secretarios deberán conocer esta tecnología. Hace unos meses estuve presentando el protocolo que nosotros utilizamos en nuestra brigada para hacer todo ese tipo de entradas y registros a los secretarios

judiciales y cuando le hablé de la imagen o el clonado de los soportes digitales y la utilización para garantizar su integridad de la firma digital, todos los secretarios generales -o una buena parte de ellos- me dijeron "es que la utilización de esas herramientas es algo que deberíamos saber nosotros como fedatarios públicos". La ventaja que tenemos en España con respecto al resto de los países del mundo (si hay alguien que sepa que esto ocurre en otro país, que me lo diga que a mí) es que nosotros cuando hacemos una entrada de registro donde solamente va la policía, tenemos el secretario judicial y el secretario judicial no es ni más ni menos que un fedatario público. Es decir, como un notario. Si él levanta fe de que a tal hora se ha copiado aquel fichero, cuando vayamos a ver esa prueba sabemos que, efectivamente, la ha modificado pero es que está recogido en el acta de entrada de registro levantada por un secretario judicial. Sabemos que hemos modificado pero un letrado de la defensa no nos puede invalidar las pruebas porque nos acuse a nosotros de que lo hemos alterado. Todas las alteraciones están recogidas en el *log* del secretario general.

Esto puede plantear algunos problemas pero el trabajo policial a veces no puede ser tan fino y tan exhaustivo como nos gustaría. Yo sé que en el ámbito privado ocurre lo mismo: siempre hay lo deseable y lo posible. Pues aquí, igual, y nosotros tenemos la ventaja de que en la década de los 80, cuando se obligó a la policía a ir acompañada del secretario judicial, probablemente por la desconfianza en la alteración de pruebas que tuvieran en aquella época sobre la policía, casi todos los compañeros lo vieron como un insulto. Una ofensa a la policía. De hecho, hay que entender que es un poco así porque es algo que no existe en ningún país del mundo por lo que yo sé. Para nosotros ahora, en este campo de las evidencias digitales, es extremadamente útil. No me voy a extender más, por si alguien quiere hacerme alguna pregunta.

Me preguntan quién sufre el prejuicio económico en el caso del *fishing*: la empresa o el cliente. En primer lugar, el que sufre el prejuicio económico es el particular, que si es una cantidad pequeña puede que no se dé ni cuenta si lleva una contabilidad. Vamos a suponer que el grupo de crimen organizado ha conseguido gran número de números de cuenta y le han extraído 20 ó 30 euros a cada uno. Quizá no se dé cuenta. Me contaban una anécdota sobre un error bancario, sobre alguien que había cargado a todos los clientes una cantidad de dinero y ni el 60% de los implicados puso estos

hechos en conocimiento de la entidad bancaria. Es decir, si la cantidad no es muy grande, hay más de un 40% de gente que no se va a dar cuenta. Normalmente son cantidades grandes porque, ya que tienen los datos, para qué van a sacar sólo 30 euros. Suelen sacar 3.000 o 30.000 euros, o todo lo que haya en la cuenta, o bien el límite que pongan los bancos. Este tipo de delitos, en un primer momento, lo sufre la persona aunque nosotros estamos intentando que sean los bancos los que lo soporten, no por ninguna animadversión hacia ellos sino porque pensamos que lo que deben hacer ellos es mejorar sus medidas de seguridad. Si ha sido por un fallo en la custodia del password o del número, hay que entender que el que lo debe soportar es el particular; pero en estos casos en que las estafas están bastante bien diseñadas, yo entiendo que debe ser el banco. No tengo conocimientos de jurisprudencia, lo que estoy diciendo es una opinión un poco personal. Yo creo que son los bancos los que se harán cargo de estos fraudes, aunque sólo sea por defender su imagen corporativa.