COMPARECENCIA DEL INGENIERO INFORMÁTICO E INGENIERO EN ORGANIZACIÓN INDUSTRIAL, D. FÉLIX BREZO FERNÁNDEZ, EN LA SESIÓN DE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES EL DÍA 30 DE ENERO DE 2014.

El señor INGENIERO INFORMÁTICO E INGENIERO EN ORGANIZACIÓN INDUSTRIAL (Brezo Fernández): Lo primero de todo es agradecer la invitación y la posibilidad de exponer cuáles son los puntos de vista de una persona que trabaja en el día a día en el ámbito de la seguridad en la red en general y en el de los riesgos derivados de su uso en particular. Quiero agradecer también la preocupación de las instituciones acerca de un campo y de un ámbito que está cada vez más presente en la vida diaria de todos los españoles, de la sociedad europea en general y, particularmente, del sector de la ciudadanía que conforman los menores en un número cada vez mayor.

A continuación, les voy indicar cuáles van a ser los contenidos de mi intervención. En primer lugar, procederé a identificar algunas de las facilidades que ofrece la tecnología (lo voy a hacer también desde un punto de vista bastante práctico, bastante visual). Se hace necesario ver hasta qué punto las tecnologías, de las que otros ponentes también se habrán hecho eco, están a disposición de cualquier individuo que opere en las redes. Seguidamente, hablaré de las redes sociales y de qué tipo de información se puede obtener a través de ellas y del juego online y de las implicaciones que estas plataformas pueden tener para los menores. También me acercaré a otro tipo de divisas de fácil acceso, no solo bitcoin, tema bastante recurrente últimamente pero no necesariamente reciente, sino también en videojuegos y en plataformas de juego online, como Diablo II, World of Warcraft y similares, en los que existen auténticas economías sumergidas

en las que se pueden comprar y vender productos virtuales para luego extraer el dinero hacia el mundo real. Precisamente por esto último, estas plataformas han pasado a ser también nicho de otro tipo de actividades ilícitas que seguramente no vienen tan relacionadas con el tema concreto de la ponencia de hoy pero que no podemos dejar de tener en mente.

Como ya hemos avanzado, vamos a empezar por repasar algunas de las facilidades que ofrece la tecnología. No es extraño representar esta realidad comparando dos sucesos similares que han ocurrido en momentos diferentes pero relativamente cercanos. Algunos emplean la imagen de la investidura del Papa Francisco en 2013 para compararla con la imagen de la investidura de Benedicto XVI en 2005, apenas ocho años antes, pero lo cierto es que se podrían utilizar eventos deportivos o acontecimientos culturales para comprobar la penetración de los smartphones de un año a otro. ¿Qué subyace? El acceso a la tecnología y a los smartphones se ha democratizado a pasos agigantados. Hace nada era prácticamente impensable que un menor pudiera tener acceso a un dispositivo en el que pudiera sacarse fotos, compartirlas en la red y comunicarse con terceros sin prácticamente ningún tipo de control parental. La tecnología –afortunadamente, casi siempre para bien– nos amplía horizontes, pero si no tomamos las precauciones necesarias, si no educamos a nuestra gente sobre las implicaciones de su uso, estas nuevas funcionalidades inconscientemente utilizadas pueden ser explotadas por terceros.

Además, en el caso de la tecnología, de las redes y de Internet se da otra circunstancia que se convierte en un problema recurrente: las condiciones legales en unos países y en otros son diferentes. Si ya lo que en España es delito, podría no estar tipificado como tal en países culturalmente similares como Estados Unidos o Europa, la problemica se acrecenta cuando entran en juego estructuras legislativas similares de paíes

menos cercanos de otros continentes más alejados de nuestras costumbres y con otras problemáticas más acuciantes.

Pero, ¿hasta qué punto somos conscientes de lo sencillo que es conectarse desde otro país? Quería aprovechar para exponer a sus señorías en directo lo fácil que es utilizar, por ejemplo, la red TOR. Sin entrar en demasiado detalles, la red TOR es una plataforma que, a partir de una aplicación libre descargable y mediante apenas un par de clics, permite a los usuarios conectarse a la red empleando una dirección IP diferente a la propia, empleando un nodo de esta red como puente entre el destino final y ellos mismos. En esta demostración, para utilizar una nueva identidad bastaría con pincha en «Utilizar una nueva identidad» para conectarnos a través de otra dirección. Al intentar localizarla en este ejemplo, los servicios de localización aproximada indican que estamos intentando realizar una conexión desde Rumania. Lo que acabamos de ver pone de manifiesto que, en apenas dos clics y sin que sea necesario tener ningún tipo de conocimiento avanzado en materia de seguridad, sin ser un hacker o un gran experto se puede conseguir enmascarar la procedencia de una conexión. Estamos hablando de tareas que puede realizar cualquiera sin problemas y con unas herramientas que están a disposición de cualquiera, gratuitas, y accesibles y de una sencillez como la que se ha querido mostrar en esta pequeña demostración. De hecho, si estos mecanismos y otros similares fueran utilizados de una forma profesional, podrían hacer que el rastreo de un teórico delito llegara a ser extremadamente complicado, sobre todo si su seguimiento dependiera de países como los que hemos comentado anteriormente, países que no tienen desarrollada ningú tipo de legislación en temas de ciberseguridad.

De ahí el interés de realizar esta prueba en vivo: para ver con nuestros ojos que tenemos en el rastreo de los problemas de la red un problema serio y que su solución no pasa solamente por el desarrollo de

una sólida legislación española, sino por la formalización de acuerdos cada vez más estrechos a nivel europeo y a nivel internacional.

Esta problemática se han puesto de manifiesto en otros ámbitos. Los programas de espionaje masivo y de recolección indicriminada de información en cantidades ingentes también han copado numerosos titulares recientemente. Lo que es cierto es que existen aplicaciones y scripts con licencia de software libre y, por tanto, de uso, copia, modificación y distribución completamente gratuita que con 2.000 líneas de código Python que puede editar y configurar a su discreción cualquier programador para recabar de forma masiva la información pública sobre una entidad que opera en la red. Es el caso de Facebook Stalker (facebookstalker.py), que permite la conexión con Facebook para descargar y almacenar absolutamente toda la información a la que tenga acceso la cuenta de un usuario. Estas herramientas permiten, por ejemplo, recolectar desde fuera qué información pública tiene un determinado perfil. Huelga decir que entre la información que los usuarios facilitan gratuitamente hay datos de un carácter tan sensible como las afiliaciones políticas, las simpatías, los grupos favoritos, los eventos deportivos o musicales a los que va a acceder o ha accedido un contacto, los patrones de conexión a la red social en función de las horas en las que actualiza su muro o introduce comentarios en las fotos de conocidos, etc.

Sin embargo, la funcionalidad de estas herramientas no es lo sorprendente. Almacenar y obtener tus estadísticas de cara a construir un perfil virtual de una persona real es fácil y está al acceso de cualquiera. Se trata de miles de líneas de código que utilizadas de forma malintencionada pueden automatizar la obtención de información sobre cualquiera y que, por tanto, sobreexponen de una manera especial a nuestros menores.

Asimismo, de la globalización de los servicios web emanan otros problemas. ¿Qué ocurre si, estando en vía pública, es el satélite del

buscador de turno el que saca una fotografía? Esa información, ese derecho a la intimidad, ese derecho de acceso y rectificación, ¿lo podemos ejercer siempre desde España o dependemos de la ubicación de estos servidores pese a que la fotografía se obtiene sobre territorio español? ¿Existen mecanismos suficientes como para que los organismos públicos puedan presionar de forma efectiva cuando se atente contra la privacidad o se pongan en jaque cuestiones de seguridad? Estas problemáticas derivadas en parte del derecho a la intimidad y que se aplican a la totalidad de las personas son particularmente sensibles, como ya se pueden hacer una idea, en el caso de los menores.

El caso que comentaba la anterior ponente acerca de las Google glasses: pensar en un dispositivo como las Google glasses que permita un procesamiento de las imágenes en tiempo real para aplicar máscaras de reconocimiento facial y cotejar esa información con la disponible públicamente a través de las redes sociales. Las tecnologías, algunas más maduras que otras, para realizar este tipo de búsquedas no son ciencia ficción. Sin ir más lejos, y a modo de prueba, Google en su servicio de Google Images hace tiempo que cuenta con un buscador que permite identificar imágenes similares empleando como criterio de búsqueda el contenido de las mismas. sus colores y formas. Si se combinaran la información proveniente de diferentes herramientas se puede construir un perfil público (remarco esto) con información detallada sobre personas completamente anónimas como nunca antes se había pensado.

Estamos en un mundo en el que los ciberdelincuentes han encontrado más motivos que nunca para dedicarse a la ciberdelincuencia. La relativa facilidad de monetizar cualquier infección gracias a la masificación del uso de plataformas de pago, ha convertido en la sustraccióna en un negocio muy rentable. De hecho, diariamente se publican ofertas de compra-venta de números de tarjeta de crédito con CVV, fecha de caducidad y demás

datos personales. Esta información se vende en el mercado negro a precios variables a partir de los 3 USD. De la misma forma que se producen robos en las calles y en los bancos, y de la misma forma que hay gente que defrauda de una manera o de otra, existen delincuentes que robando credenciales bancarias y poniéndolas a disposición de terceros están haciendo negocio.

Para recuperar el tema de las redes sociales quería poner sobre la mesa una anlogía que ilustra lo paradójico de la situación cuando a los menores, a niños de 6, 7 u 8 años les hablamos sin tapujos de los reyes magos y les recordamos que no queremos que hablen con extraños o que no habran la puerta a nadie mientras ponemos en sus manos dispositivos que les permiten conectarse a todo tipo de contenidos, contar información sobre ellos y conectarles con completos desconocidos sin que los adultos muchas veces sepan qué pueden hacer para protegerlos.

Lo cierto es que en España tenemos mecanismos para empezar a hacer esto realidad. Y en el caso de las plataformas de juego online, que son plataformas para mayores de 18 años, se obliga a la identificación con nombre, apellidos y DNI entre otros datos personales. Si se quisiera implantarlos, hay tecnología para llevarlo a cabo. Ocurre lo de siempre: los mecanismos son más engorrosos: lleva más tiempo tener configurar un lector de tarjetas para poderte identificar ante una empresa y que esta pueda contrastar los datos. Pero mecanismos, existen. No podemos enrrocarnos en el: «no, es que no tenemos tecnología que nos permita garantizar la seguridad de los menores» porque esa tecnología existe.

Además, se dan otros problemas que también son inherentes a las redes sociales. Hace apenas unos días se detenía en Estados Unidos al administrador de una serie de páginas de contenido pornográfico en las que se difundían vídeos de contenido sexual. Pese a que los vídeos eran grabados de forma consentida por los propias parejas, eran colgados a en

internet a posteriori por uno de los dos miembros de la misma en el momento en que la pareja se rompía. Además de ser un evidente atentado contra la intimidad pareja, esta situación adquiere unos tintes más graves si los que protagonizan dichos contenidos son menores. La masificación del uso de la tecnología deja aún más expuestos a los menoreslo que debería derivarse en una sensibilización especial que no se ve reflejada en la realidad. De hecho, en abril de 2013 tuvo lugar la difusión masiva a través de Twitter de enlaces a un vídeo de contenido sexual entre los que aparecían diferentes menores. Como bien avisaba el CNP, la mera posesión (habría que revisar en este punto el concepto posesión, dado que si se visualiza online, técnicamente el vídeo también es descargado temporalmente al equipo del usuario) o distribución del vídeo es delito. Pese a ello, el vídeo alcanzó rápidamente un gran número de visitas y fue dado a conocer en dicha red social siendo tema del momento durante varias horas. El principal problema que subyace es que ni los usuarios son conscientes de que la distribución de dicho vídeo es pornografía infantil ni se han dispuesto elementos disuasorios aplicables al fenómeno de las redes sociales. ¿Es suficiente con perserguir a los productores y distribuidores originales del vídeo para concienciar a la sociedad de que lo que estamos haciendo es algo tan grave o se hace necesario desplegar iniciativas y/o normativas que adviertan de que la difusión de ese tipo de contenidos es un delito particularmente grave cuando los protagonsitas son menores? Desde luego, la naturaleza y cantidad de comentarios llevados a cabo no ponía de manifiesto la conciencia social en estas cuestiones.

Las redes sociales tienen también muchas ventajas. Evidentementem podemos conocer un montón de cosas sobre un montón de gente y adoptar nuevas ideas y jugar y perder el tiempo. Ese cambio de hábitos, ha dado paso también a nuevos modelos de negocio como el que explotan algunas compañías de desarrollo de videojuegos que han encontrado en los

micropagos un nuevo filón. Por un lado, los juegos de 60 euros de antaño mantienen su mercado, pero van dando paso poco a poco a otro tipo de soluciones de entretenimiento a las que se puede acceder por menos de tres o cuatro euros. Por otro, cada vez aparecen más aplicaciones grauitas que, a través de sencillos micropagos, permiten ampliar la experiencia de los jugadores. La ventaja es que estos créditos adicionales son más sencillos de pagar, incluso a través del teléfono móvil a la vez que, al tener un coste menor, se acercan también a públicos (como el infantil) con menos capacidades para realizar desembolsos superiores.

Además, existen entornos de realidad aumentada que no tienen por qué ser necesariamente juegos. El caso de Second Life es un caso muy claro. Se trata de una plataforma de realidad aumentada en la que el usuario ya no se crea un perfil sino un personaje con identidad propia que luego puede interactuar en 3D en un mundo tridimensional. Está destinado principalmente a las relaciones interpersonales y a conocer gente. La cuestión es que han emergido por debajo economías en las que se puede adquirir gorros, chaquetas y adornos para tu personaje, incluso de carácter sexual. Para ello, la plataforma cuenta con mecanismos que te permiten adquirir créditos de Second Life (*linden dollars*) que a posteriori también se pueden retirar y que, por tanto, podrían derivar en otro tipo de prácticas que también deberían ser investigadas en otro tipo de ponencias.

El juego *online* es un ámbito que hasta mayo de 2012 no disponía de una normativa legal específica en nuestro país. Por aquel entonces, las principales salas de juego online del momento operaban en España pese a estar afincadas en territorios de ultramar como Guernsey, la Isla de Man, Gibraltar o similares. De hecho, este era el caso de Full Tilt Poker sala de juego afincada en Guernsey, territorio de ultramar británico dependiente de la Corona de 78 kilómetros cuadrados y 1.900 habitantes y en el que estaba alojada la segunda mayor sala de póquer del mundo.

En este sentido, el 15 de abril de 2011 tuvo lugar el conocido como *black friday.* Se suspendió la actividad en Full Tilt Poker a raíz de una serie de problemáticas con las licencias y el bloqueo de las cuentas de juego y de dinero virtual de centenares de miles de jugadores a nivel mundial. Gracias precisamente a la legislación española hoy se dispone de garantías adicionales de transparencia y de mecanismos para perseguir en España aquellos sitios que, por ejemplo, no cumplan con los estándares de prevención de la ludopatía o no eviten que los menores puedan jugar en sitios de juego *online*, por ejemplo.

Sin embargo, aún habiendo desarrollado esta normativa los usuarios pueden seguir encontrando plataformas no están afincadas en España en las que registrarse es tan sencillo como rellenar una serie de campos de datos, insertar tu nombre y usuario y empezar a jugar. En casi todas ellas se ofrecen además reclamos en forma de bonos de primer depósito o bonos de fidelidad para atraer un mayor número de jugadores.

Es decir, independientemente de que sea fácil o difícil después extraer el dinero obtenido en esas cuentas, el problema es que nuestros menores están más expuestos a ellas por la publicidad y este tipo de salas no tienen la obligación de cumplir nuestra legislación. La solución es complicada: por un lado, se podría proponer el bloqueo del acceso a todas las páginas externas no reguladas en España en un ejercicio que podría ser entendido como una medida para coartar la libertad de expresión. Se podría sostener el argumento de la protección de los menores, pero habría que establecer claramente en qué casos está justificado y en qué casos no lo estaría. Seguramente, eso es cuestión para que el Pleno y el Senado y el conjunto de la ciudadanía en general lo consideren.

A este esecenario hay que añadir otra derivada: la de la persecución de los delitos relacionados con el blanqueo de capitales. Una legislación estricta pone a disposición de las FyCSE herramientas que obligan a las

empresas y a las plataformas a ofrecer información cuando nuestros estamentos consideren que puede existir algún tipo de delito pero.. ¿qué potestad tiene España para exigirle a un sitio web afincado en las Antillas Holandesas para que le dé información de las transacciones que están realizando sus jugadores? Acuerdos bilaterales aparte, no tiene ninguna potestad.

Lo cierto es que el sector del juego *online* ha experimentado un crecimiento sin parangón. Antes de la regulación existían aproximadamente 170.000 jugadores en España; seis meses después de la regulación, los expertos situaban la cifra en torno al millón de jugadores (997.000). Se ha acercado la publicidad y el hecho de que sea abiertamente legal seguramente ha alimentado este crecimiento. Pero las apuestas y los juegos han pasado a formar parte también de nuestro día a día. Si un usuario navegara por los principales sitios de noticias deportivas, se encontrará con que se habla de partidos de fútbol y coeficientes de apuestas prácticamente incrustados en las propias noticias, se habla de bonos gratis para apostar y se habla de jugar al póquer *online* gratis. A modo de demostración, si accedemos ahora mismo a los principales sitios deportivos de este país encontraremos por todos los lados *pop-ups* y ventanas (“bet” no sé cuánto, “apuesta” no sé cómo, el Madrid se paga más barato o más caro). Estos ganchos son también pecibidos por los menores, público especialmente sensible porque a menudo incluyen entre sus páginas de consulta diaria este tipo de plataformas no permaneciendo ajenos a las señales que les recuerdan que el tema de las apuestas sigue ahí.

Sin embargo, si vamos a la televisión los contenidos considerados para adultos se difunden a partir de una determinada hora como las líneas de contacto telefónico o la pornografía. De igual manera, se ponen avisos de contenidos no recomendados para menores de 18 años, de 13 años o de

7 años. Esa cultura de concienciación no la estamos viendo en los sitios *online* ni tan siquiera en los que operan en y desde España.

De la misma forma que ocurre en la red, ocurre en la radio. Al sintonizar cualquier emisora en horario de deportes de fin de semana se promocionan continuamente los sitios de apuestas, sin protección de ningún tipo hacia menor y con práctica impunidad en lo que respecta a los horarios. Este es un ámbito en el que creo sinceramente que se podría actuar de una forma prácticamente inmediata en términos legislativos que ya se mostró eficaz en el pasado. En el caso de la Fórmula 1, hasta hace 8 o 10 años la publicidad del tabaco era predominante y copaba gran parte de los espacios publicitarios de los grandes premios. Sin embargo, llegó un momento en que los diferentes países empezaron a retirar el tabaco de todos estos espacios desarrollando iniciativas legislativas locales, desapareciendo también los contenidos de bebidas alcohólicas.. En los casos del alcohol y del tabaco se pusieron los mecanismos que se estimó conveniente.

En otro orden de cosas, *bitcoin* es una emergente criptodivisa que necesita de la red para transferirse empleando ficheros. La complejidad de efectuar transferencias con *bitcoins* para gente que sabe manejarlo es trivial. Se trata de una economía plenamente especulativa que da cobertura a todo tipo de productos. La difusión de los *bitcoins* necesita de dos elementos para que tenga lugar. Por un lado, está la conexión a internet necesaria para que el resto de la red distribuida que gestiona la economía valide la transacción y, por otro lado, un ligero retardo que permita a esta verificar que el *bitcoin* pertenece a quien die hacerlo a partir de una serie de procesos matemáticos relacionados con la criptografía de clave pública.

Las características distribuidas de la red obligan a que las transacciones sean públicas para que cualquier nodo de la misma pueda realizar las verificaciones pertinentes. De hecho, el seguimiento de las

transacciones se puede realizar a partir de diferentes páginas que almacenan la cadena de bloques (nombre con el que se hace referencia al histórico de transacciones de bitcoins) comprobando así de qué cuenta a qué cuenta se han ido transfiriendo estos *bitcoins*. Pero, ¿tiene sentido que sean transacciones públicas y doten de una capa adicional de anonimato? Por un lado, se puede saber en todo momento cuántos *bitcoins* tiene cada cuenta mientras que, por otro, a diferencia de lo que ocurre en el mundo real, en *bitcoin* en cuestión de segundos se pueden crear decenas de miles de cuentas con un mismo propietario. Así, se facilita el camuflaje de las operaciones a partir de transferencias entre cuentas que en realidad son gestionadas por la misma idetnidad terminando por difuminar completamente cuál es el origen de las transacciones.

Esta realidad lleva consigo implícitos cuestiones de fiscalidad de fiscalidad de difícil solución dada que las trasnferencias económicas se realizan a través de *entidades* fuera del control de los estatales y ajenas a toda norma. Estamos hablando de una moneda cuyo curso no está oficializado por parte de ningún estamento, porque no se considera una divisa funcional. Pero la realidad nos demuestra que la gente está realizando pagos, está comprando servicios, está adquiriendo libros y películas y está contratando programadores. Aún así, sigue siendo muy difícil establecer criterios de fiscalidad robustos con divisas gestionadas de forma ajena a los bancos nacionales porque ni existe un mercado cambiario oficial ni tampoco es posible forzar el cumplimiento de las normativas fiscales nacionales.

Sabiendo esto, ¿por qué hablamos de los *bitcoins*? En noviembre de 2013 se producía un fenómeno que disparaba el *bitcoin* a prácticamente 250 dólares despegando desde los 2 dólares. Sin embargo, en un momento dado se dieron una serie de circunstancias que propiciaron su caída como la inesperada paralización (forzosa o premeditada) de la cotización en

algunos de losprincipales mercados de intercambio. El resultado fue una bajada que alcanzó un mínimo de 83 dólares poniendo de manifiesto quese trata de una economía globalizada sobre la que determinadas entidades podrían ejercer una influencia tal que cambiara el curso de la economía.

Las características que la configuran son los movimientos especulativos especialmente agresivos al margen de todo control europeo o nacional y la desprotección de los usuarios frente a las injerencias de poderes económicos asimétricos como, por ejemplo, las ventas masivas planificadas a precios más bajos de lo normal para lanzar el mercado a la baja y volverlos a comprar a continuación. Se trata por tanto de un producto volátil y complejo de gestionar con una penetración cada vez mayor.

La cuestión es: ¿estamos hablando de una economía que crece? Pues sí. En noviembre de 2013 el *bitcoin* se cambiaba a 246, como hemos visto; hoy se cotiza en torno a 1.000 dólares el *bitcoin* cuando hace apenas dos años se cotizaba a 2 dólares y hace cinco lo hacía a poco más de 0,06 dólares. Es decir, el que tenía un *bitcoin* hace dos años, ahora tiene quinientas veces más; y el que tenía un *bitcoin* hace cinco habría multiplicado su inversión por 15.000. Si a todo esto se suma la dudosa procedencia de algunas transacciones y el anonimato que proporcionaría una gestión efectiva, estamos hablando de economías en auge al margen de los esfuerzos que propone nuestra legislación.

Lo cierto es que *bitcoin* es solamente la punta del iceberg. Existen también otro tipo de criptodivisas y otro tipo de mercados cambiarios con los que puede interactuar el ciudadano. Criptodivisas y movimientos como los que van apareciendo en SecondLife o los que ya han aparecido en World of Warcraft. Precisamente ayer, en una conferencia de Iñaki Bernal del BBVA facilitaba el dato de que el mercado interno de Diablo II tenía una capitalización, solamente en China, mayor incluso que los *bitcoins*.

Esto que estamos contando no es nuevo ni necesariamente reciente, porque aunque son muchos los países que están empezando iniciativas legislativas para contener estas divisas, es cada vez el mayor número de servicios que las aceptan. No se escapa a los investigadores la existencia de mercados en los que se permite la compraventa de todo tipo de productos como drogas o medicamentos prohibidos (uno de los casos es Silk Road) y en los que incluso se han llegado a ofrecer ataques de denegación de servicio contra terceros o campañas publicitarias. Esta información está en la red a través de redes como TOR y es de acceso es trivial.

Se da además otra particularidad: precisamente para garantizar el anonimato de estas transacciones, los delincuentes utilizan herramientas de anonimización como las que hemos visto anteriormente para enmascarar actividades de tráfico de drogas, venta de armas y otros elementos que escapan al control estatal. Cualquiera, incluso los menores, podrían acceder a sitios de juego *online* y utilizar *bitcoins* con diversos fines. Registrarse en este tipo de sitios es incluso más fácil que en los sitios que utilizan transacciones tradicionales porque aquí lo único que necesitas es un nombre, un usuario, la contraseña, y repetir la contraseña. y con eso ya es suficiente para realizar las cuentas.

E insisto, lo más importante de esta cuestión es que no se trata de conceptos a desarrollar en la mente de alguien sino que son ya realidades que quedan hoy patentes. Hay casos de algunas salas de apuestas afincadas en las Antillas Holandesas que utilizan software que luego permite la interacción con cuentas de PayPal y de bancos europeos que aceptan también los *bitcoins*, y para cuyo registro no es necesario prácticamente suministrar ningún tipo de información.

Para ir terminando, quería extraer un par de conclusiones con respecto a estas temáticas. Por un lado, mis perspectivas para el futuro, no son en absoluto satisfactorias. La principal problemática de la persecución

de este tipo de delitos, tanto relacionados con pornografía infantil, como con el abuso de menores o los relacionados con el juego, va a depender mucho de cuáles sean las relaciones entre Estados y la convicción de estos a la hora de perseguirlos. Incluso desarrollando en España una legislación robusta aquí, al ser internet una red global, el establecimiento de protocolos de intercambio de información rápidos y eficaces con el resto de países de la Unión Europea, con Estados Unidos o con Rusia va a ser fundamental a la hora de perseguir con garantías a los ciberdelincuentes.

Por otro lado, no quería dejar pasar la burbuja de lo social, de estar disponible en todas las redes sociales el mayor tiempo posible. Una situación que ya de por sí deja expuestos a los adultos, expone sobremanerea a menores que no tienen por qué necesariamente comprender cuál es el sentido de la información que están suministrando ni los modelos de negocio que emanan de ellos, no deberían tener que preocuparse por el hecho de que los datos e su perfil están siendo utilizados para mostrarles publicidad a medida orientada a explotar sus intereses y a canalizar sus hábitos hacia determinados tipos de contenidos que son más susceptibles de consumir.

Y además, recuperar la existencia de nuevos escenarios. Los robos virtuales están a la orden del día como lo está la sustracción de credenciales bancarias o de credenciales de cuentas de correo y de activos tecnológicos corporativos. Nuevamente volvemos a exigir a los menores que comprendan aspectos que los mayores de edad no llegamos siquiera a dimensionar con garantías. Pese a que los menores pueden interactuar con completos desconocidos que pueden sacarle partido de muchísimas formas, lo cierto es que la red muchas veces no se concibe como algo externo seguramente porque el menor se mantiene dentro de nuestros hogares.

Para que nos hagamos a la idea, hace unos años una de las contratistas de los Estados Unidos recibía una oferta por parte del Gobierno

de los Estados Unidos para la generación de un software que permitiera el control de apenas una decena de identidades *online* diferentes. Se quedaron cortos, porque hace apenas unas semanas, la prensa hacía público que una de las personas detenidas en una operación contra la pornografía infantil podía haber mantenido contacto con hasta 500 menores. La gestión de diferentes identidades digitales ficticias es mucho más sencilla de llevar a cabo a través de la red y es una situación que no pasa desapercibida.

Por último, quería aprovechar para insistir en que se trata de competencias que no solamente pueden quedarse en el debate, que, por otro lado, es muy gratificante comprobar que se está manteniendo a nivel nacional, sino que deben ir muchísimo más allá para poder iniciar los mecanismos que establezcan un marco conjunto de colaboración a nivel internacional en el que se permita una persecución eficaz de los delitos y de quienes los cometen en pos de la preservación de los derechos y libertades de todos en general y de nuestros menores en particular.

Por mi parte, estoy a su disposición para cualquier tipo de pregunta que quieran formular.