FACULTAD DE COMUNICACIÓN

UNIVERSIDAD DE SEVILLA

Trabajo de Fin de Grado
“LA DEEP WEB: EL MERCADO NEGRO GLOBAL”

PERIODISMO

Alumno: José Gay Fernández
Tutor: Isaac López Redondo

ÍNDICE

RESUMEN:

La deep web es un espacio oculto de internet donde la primera garantía es el anonimato. En líneas generales, la deep web contiene todo aquello que los buscadores convencionales no pueden localizar. Esta garantía sirve para albergar una vasta red de servicios ilegales, como el narcotráfico, la trata de blancas, la contratación de sicarios, la compra-venta de pasaportes y cuentas bancarias, o la pornografía infantil, entre otros muchos. Pero el anonimato también posibilita que activistas políticos que viven en países dictatoriales puedan compartir información sensible con el resto del mundo. Para acceder a la deep web basta con descargar el programa Tor y acceder a un directorio -como TheHiddenWiki- para obtener los enlaces criptografiados que conectan con las páginas donde se ofrecen dichos servicios. Los pagos en la deep web se realizan mediante la moneda virtual, el bitcoin, y los envíos se realizan por correo ordinario. La mayoría de los movimientos que se realizan a través de la internet profunda tienen que ver con el menudeo de droga. Los dispositivos policiales que hay que organizar para localizar a quien se esconde en la deep web son muy costosos, ya que las conexiones se producen mediante saltos aleatorios entre los distintos nodos que hacen de servidores en la red.

- - - -

ABSTRACT:

The deep web is a hidden space where the first guarantee internet is to be anonymous. Overall, the deep web contains everything that conventional search engines can not locate. This guarantee serves to house a vast network of illegal services, such as drug trafficking, white slavery, hiring gunmen, the sale of passports and bank accounts, or child pornography, among others. But anonymity also enables political activists living in dictatorial countries to share sensitive information with the rest of the world. To access the deep web simply download the Tor program and access a directory -like TheHiddenWiki- for encrypted links that connect to pages where these services are offered. Payments in the deep web are made by virtual currency, bitcoin, and ships by regular mail. Most of the movements made by the deep web are related to the drug retail. The policing arrangements to be set up to track down who was hiding in the deep web are very expensive, because the connections are produced by random jumps between nodes that make servers on the network.

- - - -

PALABRAS CLAVE:

Deep web, internet, narcotráfico, mercado negro, crimen, anonimato.

- - - -

INTRODUCCIÓN

La deep web es un tema muy interesante por la cantidad de servicios que alberga. Partimos de que es uno de los mayores garantes de la libertad de expresión en el ciberespacio en la actualidad. Teniendo esto claro, también ofrece un amplio mercado de tráfico de estupefacientes, armas, personas, tarjetas bancarias, pasaportes, etcétera. Tal oferta despertó mi curiosidad desde un principio, así que le pregunté a algunos amigos que conocían este espacio. En un principio me disuadieron de hacer un reportaje sobre ello, alertándome de que en su mayoría se trataba de fantasía y superficialidades; pero una vez concluido el reportaje puedo asegurar que no. Es cierto que los servicios que se ofrecen pueden contener una gran parte de *scam* o estafa pura y dura; portales ficticios que aprovechan para quedarse con el dinero de aquellos compradores, con la garantía de que nadie va a reclamar una estafa por haber intentado comprar un esclavo o un kilo de cocaína. Tampoco he podido verificar la efectividad de muchos de estos servicios por mi propia cuenta, al no haberme atrevido a realizar la compra de alguno de sus productos. Sin embargo, esta investigación deja la puerta abierta a futuras comprobaciones que pueden desembocar en nuevos y más completos trabajos.

Antes de decidir el tema del reportaje, valoré otras opciones para realizar el trabajo, como una recopilación teórica relacionada con el periodismo y la literatura. No obstante yo quería hacer un trabajo práctico, aplicando los géneros periodísticos y los conocimientos que he adquirido durante los cuatro años de carrera. Así elegí elaborar un reportaje. Ya sabía que el tema sería la deep web antes del género. Esto es importante, porque es habitual encontrar artículos en los medios de comunicación sobre la deep web; cada cierto tiempo aparece uno nuevo, que no aporta prácticamente ninguna información actualizada pero alerta de su existencia y vuelve a ponerlo en el terreno de lo público. Realmente, escribir sobre la deep web y los servicios que alberga no es algo noticiable, por lo que lo más propicio era elaborar un reportaje, en el que pudiera escribirse en profundidad, con diversos apartados y que permitiera la interpretación. Mis palabras, en su mayoría, se acogen al lenguaje informativo, dejando la opinión para las citas de las fuentes entrevistadas e incluyendo la interpretación de manera indirecta en aquellas informaciones que me parecieron interesantes y a las que me sumaba, siempre evitando la opinión del periodista. Sólo al final del reportaje, y a modo de conclusión, me permito rebasar los límites de lo interpretativo para inducir al lector hacia mis opiniones personales, sin revelar éstas de manera explícita en ningún momento.

Para hablar de la deep web, era mejor utilizar un género mixto como el reportaje, que permitiera incluir las informaciones e integrar las opiniones de mis fuentes, así como cierta interpretación de lo que supone su existencia. No es un asunto que esté en las portadas de los periódicos, pero sí aparece eventualmente en revistas de divulgación o en suplementos. No es noticia, salvo que aparezca relacionada ante cualquier acontecimiento de actualidad, como por ejemplo la sentencia a cadena perpetua del creador de The Silk Road, que durante muchos años fue el mayor mercado de droga online del mundo. Por eso, el reportaje fue el género periodístico que me pareció más apropiado para su el tratamiento del tema. Alex Grijelmo escribía en su libro El Estilo del Periodista que “el reportaje es un texto informativo que incluye elementos noticiosos, declaraciones de diversos personajes, ambiente, color, y que, fundamentalmente, tiene carácter descriptivo. Se presta mucho más al estilo literario que la noticia. […] Normalmente, el reportaje parte de una recreación de algo que fue noticia y que en su momento no pudimos no quisimos abarcar por completo. Pero también pueden darse reportajes intemporales sobre hechos o costumbres que, sin ser noticia, forman parte de la vida cotidiana, la política, la economía, los espectáculos...”. El reputado periodista apunta también que “las variedades de reportaje son infinitas. Podremos hablar, entre los más habituales, de reportajes de interés humano (normalmente, centrados en una persona o en una colectividad), de interés social (en lo que afecte al funcionamiento de los servicios o a la cultura de una comunidad),

de interés noticioso (relacionado con un hecho concreto, ya sea ocurrido en el día o en fechas anteriores, ya fuera recogido en su momento como noticia o no), o de opiniones (basado en las consideraciones que un hecho merezca a determinadas personas), o de interés didáctico (se explica cómo funciona o cuál es el origen de determinado asunto o cosa). Incluso un mismo reportaje puede corresponder a dos o tres de estos apartados simultáneamente". Teniendo en cuenta este apunte sobre las variedades del reportaje, yo diría que el que se recoge en el presente trabajo se adapta al de interés social, opiniones y de interés didáctico.

Otro de los aspectos esenciales del reportaje es la entradilla. Había pensado ser bastante explícito y desagradable a este respecto -pues las siniestralidades que se encuentran en la deep web prestan facilidades para ello-, pero finalmente me disuadí y decidí optar por introducir el interés de una manera más sencilla y respetuosa con las sensibilidades del lector, simplemente planteando una pregunta y ofreciendo una respuesta. Alex Grijelmo indica que "el principal problema al plantearnos el reportaje consiste también, como en la noticia, en acertar con la entradilla. Pero aquí no dispondremos generalmente de un elemento noticioso que lleve la carga del interés y la actualidad. Por lo común, el reportaje parte de noticias conocidas días antes, que se desarrollan con una perspectiva diferente. Así que carecemos de un hecho noticioso como tal".

OBJETIVOS

No pasa desapercibido para nadie que las nuevas tecnologías han revolucionado la manera en que nos interconectamos, nos comunicamos y vivimos. Pero también el modo en que comerciamos. Antes había que buscar entre todas las tiendas deportivas de la ciudad para buscar el modelo de zapatillas deseado; ahora basta con buscarla en la web y encargar la compra, para tenerlas en casa a los pocos días. De igual modo, la venta de productos ilegales también ha modificado su *modus operandi.* Sabemos gracias a la literatura o al cine cómo se realizaban estos intercambios: los interesados se ponían en contacto con suma cautela para fechar un punto de encuentro y presentarse allí, a dos bandas, custodiados por sus hombres de confianza, para cambiar el dinero por la mercancía. Y estas mercancías pueden ser tanto estupefacientes, documentos, armas o personas.

Sabía desde hace tiempo que existía toda una red de conexiones secretas, ocultas bajo la capa del internet convencional, donde operaban las distintas organizaciones y que albergaba todo tipo de macabras ocurrencias. La deep web es donde lo macabro se vuelve realidad. Protegidos por el anonimato, estos grupos comercian y se lucran prácticamente con total impunidad. Mi curiosidad me llevó a indagar a este respecto y convení que sería un buen tema para mi reportaje final de grado. Los objetivos que al principio planteé resultaron ser demasiado ambiciosos, en palabras de mi propio tutor. Para hacer un análisis exhaustivo de los servicios y productos que se ofrecen en la deep web haría falta mucho dinero, equipo, conocimientos técnicos y valentía. Mis primeras preguntas eran referidas a la identidad de los grandes propietarios de los entramados ilegales, cosa harto improbable de revelar dada mi situación. Pero había otras cuestiones sobre las que sí podía arrojar cierta luz: ¿qué se vende exactamente en la deep web?, ¿quiénes son sus compradores?, ¿cómo se accede?, ¿por qué son anónimas las conexiones?, ¿cómo se crea y cuándo surge?, ¿quién la financia y a quién interesa que se mantenga?, ¿cuáles son, aproximadamente, los precios de ciertas mercancías?, ¿cómo opera la policía?, etcétera.

Son muchos los artículos que eventualmente aparecen en los medios hablando sobre la deep web, pero como se trata de un espacio que existe, es permanente y conocido; no suele escribirse como noticia. Sin embargo la mayoría de los artículos son pequeños y dejan muchas dudas abiertas, no profundizan, o se limitan a alertar de su existencia para alimentar el morbo del lector. Decidí hacer un reportaje más extenso para explicar en qué consiste la deep web, cómo se puede entrar en ella y lo que se puede encontrar.

Para realizar el trabajo y quedarme totalmente satisfecho debería haber comprado a través de la deep web y escribir sobre la experiencia. Sin embargo no he sido capaz. Sea por miedo a meterme en un lío con la policía, o bien que un hacker se apropiara de mi ordenador y fuera capaz de sustraer informaciones confidenciales, decidí que no lo haría con tal profundidad, conformándome con observar el fenómeno desde la superficie. Esto hubiera sido altamente interesante de haberlo realizado, pues me hubiera permitido comprobar cómo se lleva a cabo el intercambio efectivo entre mercancías. Tengo un conocimiento parcial del proceso: el comprador deposita el dinero en un depósito seguro de la deep web y a los pocos días recibe el producto en su casa, mediante correo ordinario, como si de una compra online más se tratara. Sin embargo no puedo confirmarlo personalmente y debo remitirme a las fuentes para creer que así sucede. Durante el desarrollo del reportaje comencé a ser consciente de la concepción errónea que la gente tiene sobre la deep web, y me propuse incluir en el trabajo la necesidad de garantizar el anonimato para preservar derechos humanos que en ciertos países son sistemáticamente violados. Eso sí, sin salirme de la línea marcada del trabajo (“el mercado negro global”), por lo que el grueso del reportaje es referido a estos servicios, dejando para las conclusiones los elementos positivos de que exista un espacio como éste.

METODOLOGÍA

Durante el desarrollo del presente trabajo he podido tomar contacto con las instituciones, en concreto con los cuerpos y fuerzas de seguridad del Estado, experiencia que nunca había tenido oportunidad de vivir a nivel profesional; he desestimado fuentes jugosas por no poder encontrar una fecha que nos satisficiera a ambos; y he aprendido una valiosa lección sobre el trato oportuno con que hay que cuidar a una fuente.

Desde un primer momento tenía claro que quería hacer un reportaje como trabajo de fin de grado, esto es, un trabajo práctico. Entre las varias opciones que se me presentaban, en su mayoría trabajos académicos o de recopilación teórica, me suscitaban poco o nulo interés; yo ya había tenido la oportunidad de escribir reportajes para las páginas de un periódico, y realmente me resulta mucho más gratificante la aplicación técnica del periodismo: llamar por teléfono, concertar citas, salir con la libreta, grabar y transcribir entrevistas, etc. El trabajo de redacción de hoy en día puede llegar a ser algo aburrido, sobre todo si dicho trabajo consiste en adaptar las múltiples notas de prensa para sacar páginas. Sin embargo, al tratarse de un reportaje para el trabajo de fin de grado, me daba la posibilidad de elegir un tema que resultase interesante y explorarlo con libertad. La gran traba que he tenido durante el tiempo que he realizado el trabajo ha sido precisamente ésa: el tiempo. Durante el segundo cuatrimestre de mi último curso en la Universidad, he tenido que hacerme cargo de las tareas y los trabajos regulares para las asignaturas en las que estaba matriculado; aparte la Semana Santa, la Feria y el viaje de estudios, así como una semana que pasé en Berlín recopilando información sobre los másters que ofertan sus universidades. Por ese motivo, muy pronto decidí que el trabajo no lo presentaría en junio, sino en septiembre. Aunque eso no significaba que no fuera a trabajar en este reportaje durante el curso. Me propuse dedicarme a la tarea documentativa durante los meses de marzo a junio, realizando entrevistas y organizando un dossier de prensa para guiarme durante el proyecto.

Necesitaba un ordenador para acceder a la deep web. La naturaleza singular de este ciberespacio oculto me hacía desconfiar de usar el mío personal para investigar, al estar expuesto a los eventuales vigilantes que rondan el internet profundo y tener unos conocimientos más bien básicos sobre informática y seguridad en la red. Pregunté en la Universidad si se me permitía utilizar uno de los suyos para tal fin, y me lo negaron aduciendo unos límites precisos en el tiempo de préstamo. Entonces comencé a investigar en base a páginas de internet y foros en los que se discutían sobre la deep web y resultó no ser demasiado peligroso acceder a ella, siempre y cuando se mantuviera un contacto superficial con sus contenidos y la exposición no fuera prolongada. Fue casi al final del trabajo cuando decidí descargar el programa Tor y entré a comprobar algunos enlaces relacionados y los servicios que se ofertan, sin registros ni descargas.

Tiempo atrás, había leído un libro del profesor Ramon Reig en el que refería un trabajo de investigación sobre películas *snuff*, realizado por los alumnos Cármen Pérez Domínguez, Rocío Troncoso Muñoz y Francisco J. Poyato Pino, quienes habían localizado a un hombre llamado Manuel Lorenzo, residente en Sevilla y experto en esta especialidad fílmica. Consideré que sería una buena fuente e intenté seguir sus pistas para ver si estos alumnos podían ponerme en contacto con él. Pero al profesor Reig le resultó imposible localizar a estos antiguos alumnos. Eran de la promoción 1992-1997. Descarté la fuente.

La deep web es un territorio al margen de la legalidad, donde operan tanto criminales refugiados en el anonimato como defensores de la libertad de expresión; pero también la policía, quien está al tanto de los movimientos que en ella se producen y es la encargada de vigilar y escudriñar sus parcelas. Por tanto, la primera fuente que iba a necesitar sería una policial, preferiblemente de

alguna brigada como la de investigación tecnológica, o el cuerpo de delitos telemáticos de la Guardia Civil. Así, me puse en contacto con el periodista Antonio López Hidalgo, profesor de la Universidad de Sevilla, para que me proporcionase algún número de teléfono o me acercara a alguna fuente policial para comenzar el reportaje. Sin más dilación, Antonio López concertó una reunión con un inspector de policía en un bar frente al Rectorado de la US, donde haría de enlace y nos presentaría para una futura entrevista. Allí conocí a Joaquín Pérez, del Cuerpo Nacional de Policía, quien resultó estar trabajando en asuntos de menores y conocía los movimientos de la deep web. Le expuse brevemente el tema de mi reportaje y la información que necesitaba y accedió a proporcionármela; quedamos para una semana más tarde en su despacho, me indicó la dirección y allí nos reunimos, donde mantuvimos una conversación de aproximadamente una hora que recojo literalmente en el apartado correspondiente del presente trabajo. Una vez hube recogido las palabras del inspector de policía, consideré que igualmente sería valioso para el reportaje el testimonio de un guardia civil de delitos telemáticos. Comencé preguntando a amigos, concretamente a uno cuyo abuelo había servido en el cuerpo hacía tiempo, pero le fue imposible a éste ayudarme, alegando que no conocía a nadie que se adaptara al perfil buscado. Luego consulté a un familiar residente en Almería, que trabaja como abogado y por su oficio se relaciona con la benemérita. Éste me consiguió un apellido -Gabón- y un número de teléfono. El procedimiento fue el siguiente: mi familiar le preguntó a una compañera con quien comparte bufete, ésta habló con su padre, guardia civil ya jubilado, quien habló con el señor Gabón y accedió a que su número de teléfono me fuera facilitado. Yo le llamé, desde Sevilla, y le comenté lo que necesitaba. Desde un primer momento, el señor Gabón se mostró reticente a facilitarme cualquier tipo de información sensible. "Comprenderás", me dijo, "que no puedo darte información sobre nuestras investigaciones". Como mucho me explicaría los procedimientos, pero no parecía especialmente entusiasmado por mantener una entrevista con un estudiante de periodismo. En Semana Santa, aprovechando que estaría pasando unos días en Almería, lo volví a llamar; accedió a reunirse conmigo, pero con margen de una semana más y sin la certeza de comprometerse a una fecha concreta. La principal inconveniencia era que si esperaba hasta entonces, perdería una semana entera, o dos quizá, de clase; teniendo además muy cerca la feria, el viaje de fin de carrera y los exámenes. Valoré mis opciones y finalmente decidí volver a Sevilla y posponer en lo posible la entrevista. Otra vez telefoneé al señor Gabón para disculparme e intentar buscar otra fecha alternativa; sin embargo nos fue difícil encontrarla y yo no quería realizar la entrevista por correo electrónico o teléfono, por suponer que sería poco productiva. Así, descarté esta fuente y me contenté con la sustanciosa información que me había proporcionado el inspector Pérez de la Policía Nacional.

Consideré que, por otra parte, mi reportaje necesitaba el testimonio esencial de un informático, así que me puse a buscar nombres de profesores de informática en la Universidad de Sevilla. Primero observé las asignaturas que impartían y me decanté por el doctor Pablo Neira Ayuso, en parte porque su especialidad eran los sistemas de seguridad en la internet, y por otra porque el título de doctor le confería una especial distinción. Contacté con él mediante correo electrónico y accedió a entrevistarse conmigo en su despacho en la Escuela Superior de Informática, en horario de tutorías, donde mantuvimos una animada conversación de una hora, en la que me explicó bastantes términos y principios teóricos de la informática. Al terminar esta entrevista, el profesor me pidió que le pasara una copia del reportaje cuando éste estuviera completo, y así le prometí que haría.

Cuando ya tenía la información operativa del policía y la información técnica del informático, quise terminar las entrevistas incluyendo las palabras de un hacker, especialmente uno que hubiese operado a través de la deep web. Esta tarea me resultó muy complicada al principio, pues no se me ocurría manera alguna de llegar a estos y menos de conseguir que accediesen a revelarme información. La ocasión me llegó cuando, hablando con un amigo, éste me comentó que tenía ciertos estupefacientes poco habituales. Yo le pregunté cómo los había conseguido y él me lo dijo:

un amigo suyo los había comprado a través de la deep web. Enseguida le pedí que me lo presentara, en una reunión estrictamente profesional donde su amigo podía confiar en mi discreción y la confidencialidad de sus palabras. Pasó el tiempo y la cita no se producía, hasta que una mañana de domingo, después de haber trasnochado, vino mi amigo corriendo y me dijo "allí está el chico de la deep web, ven que te lo voy a presentar". Yo me acerqué encantado, con muchas ganas de conocerlo, y quizá estas ganas fueron lo que me hizo comportarme con excesiva extroversión y confianza, ante una persona que de nada conocía y que no era un amigo, sino una fuente en potencia. Yo le expliqué cómo era el procedimiento con un periodista, que necesitaba su testimonio, que sus datos personales no serían revelados y que, en definitiva, podía estar tranquilo. Este chico en cuestión parecía bastante reservado, aunque al final accedió no muy convencido a enseñarme cómo funcionaba la deep web. Algunos días después, al preguntarle a mi amigo por la fuente, éste me confirmó mis peores sospechas: había perdido a la fuente. Decía que ya no quería reunirse conmigo porque le parecí excesivamente amistoso sin conocernos de nada. Y es cierto que así fue. Mi error fue confundir a un amigo con una fuente; lo conocí por medio de un amigo que ya me había presentado varias personas con las que en la actualidad mantengo una buena amistad, y yo actué con la fuente como si de un nuevo amigo más se tratara. Aprendí una valiosa lección: hay que saber separar lo social de lo profesional, aunque más adelante ambos ámbitos puedan converger.

Por último, decidí que sería bueno incluir las palabras de profesionales en otras parcelas como la economía o el derecho. Del mismo modo que había hecho para contactar con el profesor Neira, busqué en el directorio de la facultad de empresariales y económicas de la Universidad de Sevilla y localicé a la profesora Concha Morejón, a quien le envié un correo solicitando audiencia. Ésta me contestó al poco refiriendome a otro profesor, Francisco Zabala, alegando su reconocida formación en Finanzas Internacionales, aspecto más relacionado con mis intereses sobre el impacto de los negocios en la deep web para la economía internacional. Le mandé el mismo correo al profesor Zabala, sin obtener respuesta por su parte. Localicé a otro, perito en materia de derecho internacional y fiscal, el profesor Nicolás Diaz Ravn, quien amablemente me invitó a visitarlo en su despacho los miércoles a partir de las 13:00 horas, aunque él mismo me confió que no creía poder ayudarme mucho. Al barajar las opciones, y estando en aquella fecha ocupado con otros trabajos para la carrera, le respondí disculpándome por no poder reunirme con él y descarté otra fuente.

CONCLUSIONES DEL TRABAJO

Buscar en la deep web resulta muy fácil una vez que se conoce el método. Basta con descargar el servidor Tor, buscar un directorio de enlaces como puede ser The Hidden Wiki, y darle clic a los enlaces para que te reconduzcan a sus páginas. El problema es la seguridad, hacen falta más conocimientos que los de un usuario normal para navegar protegido. Otro de los problemas es la fiabilidad; es muy posible que al comprar por la deep web quedemos esperando un producto que no llega porque hemos picado el anzuelo de la estafa. Pero sí es verdad que bajo el internet convencional, allá donde los buscadores como Google o Bing no llegan, se oculta una vasta red de narcotráfico internacional, donde se ofrecen todo tipo de productos imaginables. La droga o las armas es quizá lo más habitual, pero también se esconden misteriosas corporaciones y grupos con un acceso sumamente restringido, documentos que portan verdades incómodas, fabricación de productos que pondrían en peligro a toda la humanidad, o revelaciones científicas que costarían la reputación de más de uno. Sin embargo esto no es nada nuevo. Lo que realmente resulta novedoso es la posibilidad que cualquiera tiene de acceder a ellos, siempre que se esfuerce lo suficiente.

Pero hay algo más importante que aprendí mientras investigaba. Durante la realización del trabajo acabé descubriendo que la deep web no era el pozo negro de los trapicheos ni la ciudad sin ley del mafioso. Lo que principalmente albergaba era la posibilidad real de comunicar con las garantías del anonimato. Quizá un estudiante universitario en España no alcance a ver las posibilidades de esta red más allá del negocio fraudulento, pero resulta sustancialmente distinto cuando la red posibilita que la opinión pública conozca ciertos secretos que deberían conocer. Hablo aquí de países dictatoriales donde los gobiernos ejercen un férreo control sobre las informaciones divulgadas, pero también de países democráticos que han mantenido ocultos documentos que prueban su responsabilidad en ciertos sucesos acaecidos. Por ejemplo, cuando en 2003 se abrió fuego contra el Hotel Palestine en Irak, donde se hospedaban los periodistas enviados a cubrir la guerra, primero se culpó a los talibanes, pero poco después pudo saberse a través de los documentos que se filtraron en la deep web que los verdaderos responsables eran unos oficiales del ejército estadounidense, y que la administración Bush había silenciado este acontecimiento para preservar su credibilidad internacional. El caso fue ampliamente seguido a través de los medios de comunicación, pero fue a través de WikiLeaks que se fueron ofreciendo nuevos documentos sobre las diligencias tomadas por parte de los gobiernos afectados y la solución diplomática al conflicto. Los servicios de inteligencia norteamericana se apresuraron a buscar al responsable de estas filtraciones y culparlo por un delito de revelación de secretos oficiales de Estado. Pero esta información que fue filtrada era veraz y de gran interés público, ¿acaso no merecían conocerla los familiares de los periodistas asesinados en Irak? Esto es, la existencia de la deep web sólo garantiza el anonimato, de base. Pero cuando se ofrece un servicio de estas características, también se presta a ser utilizado para otros asuntos más escabrosos y menos dignos. Así pues, el internet oculto no es más que una plataforma, una posibilidad de ejercer la libertad de expresión con todas las garantías. Una espada de doble filo, en toda regla, ya que pese a garantizar derechos humanos fundamentales, en su interior aflora la nueva realidad virtual del mercado negro global.

FUENTES

1. FUENTES DOCUMENTALES

- CASO Laura, *Hay vida más allá del porno, las drogas y las armas en la 'deep web'*, El Mundo, 03/06/2015 (http://www.elmundo.es/enredados/2015/06/30/55915d40e2704e361d8b4577.html)

- Geekland, *Acceder a la web de forma segura* (http://geekland.eu/acceder-a-la-deep-web/)

- GRIJELMO, Alex (2008), *El estilo del periodista*, Madrid, Taurus.

- HANRAHAN Jake, *Hablamos con uno de los mayores narcotraficantes de la deep web* 30/07/2015 (https://news.vice.com/es/article/hablamos-mayores-narcotraficantes-deep-web)

- MUÑOZ Alberto, *Viaje al lado oscuro de internet*, El Mundo, 05/03/2015 (http://www.elmundo.es/espana/2015/03/05/54f7513cca47413e0f8b4570.html)

- REIG, Ramón (2000), *Periodismo de investigación y pseudoperiodismo*, Madrid, Ediciones Libertarias.

- Trend Micro (2005), Informe '*Deep web: below the surface*', (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf)

-Xataca, *Una semana en la deep web*, 11/02/2015 (http://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado)

2. FUENTES ORALES

- Inspector Joaquín Pérez, del Cuerpo Nacional de Policía, en Sevilla

- Doctor Pablo Neira Ayuso, profesor de informática en la Universidad de Sevilla

REPORTAJE

LA DEEP WEB: EL MERCADO NEGRO GLOBAL

Es habitual escuchar comentarios como “la matrícula de la universidad es tan cara que voy a tener que vender un riñón para pagarla”, igual que es sabido que alguien puede obtener un pasaporte legal de los Estados Unidos de América sin pasar por el trámite burocrático establecido. Sí, ¿pero cómo se comercia con un órgano? ¿cómo se puede obtener un visado sin un contacto físico que lo proporcione? Todo este tipo de actividades y muchas más pueden realizarse a través de la deep web, aquella parte del internet que se mantiene invisible por razones obvias.

La deep web, o internet profundo como se conoce en español, es un espacio prácticamente infinito donde las posibilidades se amplían más allá de los límites de lo racional y lo sensato. En líneas generales, la deep web procura el anonimato de los usuarios, con las implicaciones que ello conlleva. Aproximadamente entre el 85% y el 90% del contenido de Internet -aunque es muy complicado dar un porcentaje exacto- no es accesible a través de los motores de búsqueda estándar, como Google, Bing o Yahoo. Eso no quiere decir que todo el contenido del internet profundo sea un espacio para realizar actividades ilegales; dentro de ese porcentaje se encuentra una gran cantidad de páginas dinámicas que se generan al consultar una base de datos concreta y temporal, como el saldo bancario o el tráfico de una carretera en ese momento, o simplemente una página que solicite un código de confirmación Captcha para acceder.

Los contenidos que se encuentran en las profundidades de la deep web son de lo más escabrosos, por eso es común hallar un halo de misticismo al hablar de sus recovecos. Y no es para menos. Entre otros, la deep web alberga servicios de venta de drogas, venta de armas, blanqueo de dinero, contratación de mercenarios, documentos científicos, venta de objetos robados y billetes falsos, información bursátil confidencial, turismo sexual y prostitución, pornografía infantil y bizarra, vídeos gore y de violencia extrema, manuales de terrorismo, instrucciones para fabricar artefactos explosivos, tráfico de animales exóticos, claves de identificación para sitios como PayPal, eBay o Skype, literatura conspiranoica, documentos de secreto de Estado, y un largo etcétera. Una plataforma que garantiza el anonimato de sus usuarios puede generar todo tipo de servicios. Ilegales o no.

Básicamente la deep web integra todas esas páginas de internet que no pueden ser indexadas por las arañas de los buscadores tradicionales. El Dr. Pablo Neira, profesor de informática de la Universidad de Sevilla, explica el funcionamiento de estos robots a la hora de localizar y clasificar la información. “Los buscadores tienen un software, que es un robot, que se suelen llamar arañas (spiders, en inglés), que lo que hacen es conectarse a una web y seguir sus enlaces, y cuando sigue esos enlaces va construyendo lo que viene siendo la telaraña de la web, todo el entramado de conexiones y enlaces que hay de una web a otra”, asegura. La forma de actuar no resulta demasiado complicada si se entiende el funcionamiento de los servidores de internet. Los contenidos de la web están alojados en servidores, máquinas que permanecen encendidas las 24 horas del día. Estos servidores generalmente tienen un nombre asociado, como 'elmundo.es' o 'infolibre.com', pero no tienen por qué tener un nombre, pues con la dirección IP basta. En esa máquina puede instalarse un servidor web y alojar allí los contenidos que se deseen; pero, alerta el profesor Neira, “si ese servidor ofreciera un contenido y nadie lo referencia, va a ser más difícil de encontrar”. Es decir, son muchas las páginas de internet que dependen del volumen de sus visitas diarias, por lo que las arañas realizan un ranking de relevancia. “Es sabido que uno de los criterios es la cantidad de referencias que hay a una web, luego los robots tienen su forma de canalizar, porque a menudo se inventan enlaces superfluos a una web para aumentar en el ranking; así los navegadores también

tienen un robot que evalúan si esos enlaces son falsos o no, y penalizan a los falsos enlaces", explica el profesor Neira.

Si el propietario de una web de apuestas o de información deportiva depende de la relevancia de su página, hará todo lo posible para aumentar la visibilización de ésta en los motores de búsqueda. En la deep web ocurre todo lo contrario: basta con hacerla invisible a las arañas de los buscadores. Existen varias formas de esconder los contenidos de la web convencional, por ejemplo, poniendo un servidor web en un puerto no estándar. El profesor Neira explica que "las arañas suelen seguir enlaces o tantear todas las máquinas que hay en internet en el puerto 80 o en el puerto 443", que son los puertos más frecuentes, así que basta con alojarlo en otro puerto menos convencional. Pero también puede ocultarse esta información de una manera mucho más sencilla: mediante un usuario y una contraseña. Esto son contenidos que no son indexables y a los que cualquier otra persona no puede acceder. El profesor Neira asegura que "hay mecanismos técnicos muy sencillos para hacer que algo no sea alcanzable, como puede ser ocultar el contenido, poner usuario y contraseña, o cifrar con criptografía de claves".

LA RED TOR

Para acceder a la deep web basta con descargar un software libre específico que no revele la identidad de los usuarios. Las tres redes anónimas de mayor relevancia en la actualidad son Tor (The Onion Router), I2P y Freenet; siendo la primera de ellas la más popular. Cuando un usuario utiliza internet, lo normal es que el ordenador se conecte al servidor de la página que se visita. El servidor anota la dirección IP que identifica y localiza al usuario, y envía de vuelta la página buscada. Para una agencia del gobierno o para un hacker resulta muy sencillo observar este tráfico, pero Tor lo dificulta mediante la introducción de intermediarios.

El funcionamiento de Tor se basa en un sistema de saltos entre el tráfico de datos. Cuando un cliente se conecta, solicita a un servidor los nodos disponibles. Su petición va rebotando de un nodo a otro y saltando de país en país de manera aleatoria. La información del ordenador es sucesivamente cifrada y modificada en cada eslabón hasta que llega al destino final. Un espía podría interceptar el mensaje, pero le resultaría imposible saber quién lo escribe ni desde dónde. Al acceder a la red Tor, lo primero que llama la atención es su aspecto retro, parecido a los primeros portales de los noventa, y el elevado tiempo de espera a la hora de cargar las páginas. Esta estética se debe a un aumento de la funcionalidad a costa de una apariencia más simple, pues de por sí es lento establecer las conexiones -debido a los saltos entre servidores intermedios- como para invertir en recargar innecesariamente el portal.

La historia del proyecto Tor se remonta al año 2003, cuando unos técnicos del Laboratorio de Investigación Naval de los Estados Unidos anunciaron que habían desarrollado un sistema de comunicaciones que garantizaba el anonimato, cuyo funcionamiento era similar a las capas de una cebolla -de ahí el nombre-, dificultando progresivamente el acceso por cada nivel que se desciende. Estos investigadores fueron Roger Dingledine, Nick Mathewson y Paul Syverson. Desde 2005 hasta la actualidad, este sistema es propiedad de Tor Project, una organización sin ánimo de lucro encaminada a la investigación y a la educación, con sede en Massachusetts, y que ha sido financiada por distintas entidades desde su creación, entre las que se encuentran Google, Human Right Watch, la Fundación por la Libertad de Prensa, SRI International y los gobiernos de Alemania, Suecia o, curiosamente, los Estados Unidos. Actualmente el proyecto Tor está dirigido por un equipo liderado por su creador, Roger Dingledine.

Obtener TOR es tan sencillo como dirigirse a su página web (thetorproject.org) y descargarlo. No

obstante, la propia página alerta del funcionamiento de este software tan particular y ofrece una serie de indicaciones a tener en cuenta antes de realizar la descarga. Así, avisa que es recomendable usar el navegador TOR ya que está configurado para proteger su privacidad y el anonimato en la web; avisa también de que no es recomendable intercambiar archivos torrent, porque estos ignoran la configuración de su proxy y puede ser potencialmente destructivo para su computadora. El sistema TOR inhabilita por defecto los pluggins instalados en su navegador, tales como Flash, RealPlayer o Quicktime, ya que estos pueden ser manipulados para revelar la dirección IP desde la que se realiza la conexión. No se recomienda la instalación de complementos adicionales en el navegador Tor, ya que estos pueden dañar su anonimato y privacidad. Para asegurar el cifrado privado a sitios web, el navegador TOR incluye por defecto el complemento HTTPS Everywhere, que fuerza el uso de cifrado HTTPS -esto es, de navegación segura-, en los principales sitios web a los que se conecte. Por otro lado, Tor advierte al usuario antes de abrir automáticamente cualquier documento que sea manejado por una aplicación externa. Esta advertencia no debe ser ignorada y se debe tener mucho cuidado a la hora de descargar documentos a través de Tor, especialmente los archivos en formato DOC y PDF, ya que estos documentos pueden contener recursos de internet que se descargarán desde un servidor externo a Tor y podría revelar la dirección IP, comprometiendo seriamente el anonimato y convirtiendo al usuario en un potencial objetivo de los hackers que merodean tras la deep web.

En la actualidad, no hay ninguna legislación en España que impida acceder a la red Tor. Pero el anonimato comienza una vez se navega dentro de esta red. El profesor Neira advierte que “en la época dígital en la que estamos hoy día, si estás desde tu casa accediendo a la red Tor, te estás visibilizando dentro de la montaña de datos”. Porque no todo el mundo accede a Tor, sin embargo “con los mecanismos de visibilización que existen puedes ver que hay una persona que está accediendo a Tor y la metes dentro de un mismo saco”, aclara.

Hay que ser especialmente cuidadoso a la hora de acceder a la deep web, porque en ella abundan los hackers. Pero eso no quiere decir que el peligro se limite a estos márgenes. El profesor Neira relaciona la instalación de Tor con cualquier otro software que sea descargado en un ordenador. “Cada vez que uno instala un software está realizando un acto de confianza. Si el software que te descargas viene ya con puerta trasera o con software para utilizar tu ordenador como un bot, o para poder emplearlo en ataques orquestados para negación de servicios, o para espiarte, o robarte información, eso puede suceder con cualquier software”, explica, pero añade que “es más probable que te lo instales con un juego, que hay millones en internet, a que te instales un cliente de Tor manipulado”. El profesor Neira recuerda un caso que sucedió hace algunos años: “hubo un cliente de Tor, que la web estaba traducida en persa, y el objetivo era atraer a los activistas iraníes, que accedieran a la red Tor y divulgaran la información... periodistas, activistas, políticos”, pero finalmente se descubrió que este cliente estaba vinculado con el estado iraní, una trampa en la que muchos activistas habían caído confiando en que su anonimato estaba garantizado. “El Estado Iraní tenía un software de puerta trasera para monitorizar la actividad” explica Neira, “y eso lo puedes hacer con el software de Tor o con cualquier otro”.

PORNOGRAFÍA INFANTIL

Uno de los contenidos que más abundan por la deep web son los de pornografía infantil. En sus profundidades se alojan vastas redes de pederastia que operan por todo el globo intercambiando todo tipo de documentos, fotografías, vídeos, en los que se observa a menores de edad desnudos o practicando sexo. La etiqueta con la que se denominan los contenidos de pornografía infantil en la deep web es 'Cheese Pizza' -pizza de queso- o simplemente CP, un sútil acrónimo que hace referencia a 'Child Pornography' por sus siglas.

Este tipo de material no sólo se encuentra alojado en la deep web, sino que también puede encontrarse en páginas del internet convencional, aunque es prácticamente imposible localizarla a través de los buscadores habituales porque aquellos que lo divulgan se cuidan mucho de hacerlo visible. “De todas formas”, advierte el profesor Neira, “los robots son capaces de detectar cierto contenido e incluso apartarlo de manera automática, aunque a veces se cuela contenido que no es. Basta con buscar en Google Imágenes, en la sección de imágenes intentan no poner pornografía, pero siempre se cuela algo”.

El asunto de la pornografía infantil es un tema muy delicado y también una preocupación muy fuerte desde el punto de vista de las fuerzas de seguridad del Estado. El inspector del Cuerpo Nacional de Policía de Sevilla, Joaquín Pérez, explica que la legislación ha cambiado mucho en los últimos años. “Antes había que comprobar que se había realizado un traslado de documentos, ahora basta con demostrar que hay en un ordenador imágenes de menores con contenido pornográfico, ahora la simple posesión de imágenes de menores es constitutiva de delito”, aclara. No obstante, al estar la mayoría de los archivos de la deep web nombrados mediante criptografía, resulta muy complicado conocer a ciencia cierta qué tipo de archivos son los que se están descargando. El inspector Pérez acota los procedimientos que deben ponerse en marcha a la hora de cerciorarse que se ha descargado material ilegal. “Hay quien descarga una película y resulta que es una película pornográfica de menores”, explica, “si avisas a la policía asumes que tienes que pagar una multa por piratería pero nada más. Otra cosa es que descargues pornografía infantil y te lo calles”. Además, ilustra con un caso que le ocurrió mientras trabajaba en Málaga. “Una vez me llamó un hombre diciendo que su hijo se había descargado una película y apareció una fotografía de menores, nosotros fuimos a ver el ordenador, vimos los puntos desde los que se ha conectado y trabajamos en base a ello”, aclara. Sin embargo, los tiempos han cambiado y los mecanismos de encriptación han mejorado, ampliando el abanico de posibilidades que tienen los criminales para ocultar este tipo de material. El inspector Pérez señala que “antiguamente tú podías descargarte una película de vídeo que si la metías en un programa, esa película tenía detrás, enmascarada, una serie de imágenes o un procesador de texto que te lo convertía en una imagen encubierta en segundo plano”. “Y eso era antiguamente, así que imagínate lo que puede haber hoy”, apostilla.

Los casos de pornografía infantil son muy abundantes pero apenas se conocen, puesto que no son mediáticos. Y esto es debido a la especial sensibilidad que tienen estos asuntos para con los menores y sus familias. Explica el inspector Pérez que “el tema de los menores no sale en la televisión por el tema de la protección. Claro que detenemos menores que le pegan a los padres, o tenemos menores que han sido víctimas de abusos sexuales dentro de la familia; pero eso no sale, y si sale es porque el menor aparece gravemente maltratado en un hospital. Eso es algo mediático y se dispara”.

SERVICIOS EN LA DEEP WEB

La posibilidad de encontrar drogas ilegales varía mucho en el internet profundo. Se puede encontrar desde tabaco de contrabando o cannabis hasta heroína, psicodélicos, cocaína, éxtasis y otros. Además de las tiendas especializadas y los foros, existe un buscador muy popular en la deep web llamado Grams, con un logo y un formato muy similar al utilizado por el buscador de Google, que permite localizar fácilmente aquellas páginas relacionadas en las que puede encontrarse la droga en cuestión. El mercado de drogas de mayor relevancia en la deep web se llama Agora, que se ha configurado como el primero y más completo desde la caída de Silk Road en 2013, saldado con la detención de su líder Ross Ulbricht, recientemente condenado a dos cadenas perpetuas. No obstante, son muchas las páginas que se dedican a comercializar estupefacientes, y el estado de sus servidores

es variable, igual que los enlaces de conexión cifrados que a menudo cambian para evitar la sobreexposición. Otro mercado relativamente nuevo es Oxygen, del que resulta especialmente curioso el mensaje en inglés que utilizan de eslogan: “Nuestra misión es hacer tan sencillo como seguro sea posible para todo adulto comprar y vender drogas”. En esta página puede encontrarse, por ejemplo, 3,5 gramos de Cubensis Orgánica, una seta altamente alucinógena, por unos 15$.

El método de compra es similar en todas. El vendedor expone su producto y, en función de la confianza de negocios previos, el comprador puede valorar el nivel de fiabilidad observando su *feedback*. Con cinco estrellas, se considera un vendedor fiable y pueden leerse comentarios como “Excelente producto, buena calidad, como siempre”. La mayoría de las guías para comprar en la deep web recomiendan no adquirir ningún producto de vendedores tengan pocos o ningún comentario anterior, porque existe el riesgo de que tal vendedor se trate simplemente de *scam*, el término con el que se conoce en la jerga informática a la publicidad falsa y los estafadores.

La venta de cuentas robadas el otro de los servicios que ofrecen los distintos portales de la deep web, sin embargo es una práctica criminal que también puede encontrarse en la web convencional, aunque de manera mucho más discreta. Números de tarjetas de crédito, números de cuenta bancaria, y credenciales de cuentas de videojuego son probablemente los bienes más comercializados en estos sitios. Como en la web convencional, los precios varían según la naturaleza de las ofertas. Pueden encontrarse cuentas robadas de PayPal, con un balance de 700$ y correo electrónico verificado por 250$. También puede adquirirse por 90$ una réplica real de una tarjeta de crédito Visa americana con un balance de 2.000$.

Los pasaportes y documentos nacionales de identidad falsificados pueden obtenerse mediante la deep web para abrir cuentas bancarias, cruzar fronteras y solicitar préstamos. Los precios son muy variados en función de los países y los vendedores. La validez de estos documentos es difícil de comprobar sin haber adquirido previamente los bienes, especialmente en el caso de la ciudadanía. Estos servicios pueden ser simple *scam* aprovechándose de las vulnerabilidades de aquellos que esperan obtener la nacionalidad de los países en los que residen. En el portal FakeID aparece una gran lista de precios en función del paquete elegido. Por ejemplo, el pasaporte español se facilita por 550€, que pueden ampliarse hasta 800€ si se compra un *pack* que incluye, además, el DNI español y el permiso de conducir. El pasaporte más caro en este sitio es el americano, que cuesta 700€ el simple y 900€ el completo, que incluye DNI y licencia de conducción. El más barato, por contra, es el pasaporte brasileño que puede obtenerse por 400€, sin posibilidad de obtener el carnet de conducir ni el documento nacional de identidad.

Uno de los más escabrosos servicios que se ofrecen a través de la deep web son los del sicariato. Si los mercados de venta de droga o de pornografía infantil son cautelosos con su identidad, en los servicios de asesinato por encargo se aumenta la naturaleza secreta del negocio. Hay un sitio en la web llamado C'thulhu, en honor a la deidad de los horrores creada por Lovecraft, que facilita una detallada lista de precios en función del servicio que quiera obtenerse. Estos precios varían desde una paliza simple por 3.000$, dejar paralítico al objetivo por 30.000$ o provocar una muerte por accidente por 75.000$. A su vez, estos precios aumentan según el rango y la posición del objetivo. Por ejemplo, dejar paralítico a un político cuesta 120.000$. Pero este portal no sólo facilita eliminar a una persona, también ofrecen secuestros. El rapto de una persona adulta sin posición relevante cuesta unos 7.000$, mientras que secuestrar al retoño menor de edad de alguna *celebrity* asciende a 84.000$. En este sitio no pueden encontrarse referencias a servicios prestados en el pasado por la extrema cautela con que protegen su identidad. Así mismo lo hacen constar en su página: “Todo contrato es privado, y todo los datos son borrados tras enviar la prueba de eliminación al comprador. Es necesario para nuestra seguridad y la del comprador”. De igual modo es difícil establecer un

grado de confianza suficiente. El portal informa que el pago se realiza una vez finalizado el encargo, pero curiosamente sí hay que depositar el dinero antes, en manos del llamado *escrow* o intermediario, por lo que también existe un alto riesgo de estafa.

BÚSQUEDAS EN LA WEB

La deep web alberga manuales que son retirados del internet convencional por su potencial peligrosidad. Por ejemplo, puede encontrarse cómo fabricar ciertos venenos o artefactos explosivos, como falsificar documentos oficiales o tarjetas de crédito, e incluso documentos de valor científico que han sido silenciados. “La búsqueda en internet no conlleva ningún delito”, explica el inspector Pérez. Se trata del paso del campo virtual al campo real. “Yo puedo saber, y de hecho lo sé, cómo se falsifica una tarjeta de crédito o cómo se roba un vehículo. Otra cosa es que lo ejecute”, comenta. Si alguien busca en las profundidades de la deep web, por ejemplo, cómo fabricar una mina antipersona, va a encontrar todo tipo de explicaciones y cronogramas, “otra cosa es que tú lo coloques y le explote a alguien”, subraya el inspector Pérez. A la hora de cometer un delito por utilizar la deep web es importante tener en cuenta el paso de la virtualidad a la realidad.

HACKERS EN LA DEEP WEB

Un espacio que garantiza el anonimato casi total como la deep web resulta un territorio idóneo para que los hackers de todo el mundo realicen su labor. El profesor Neira se esfuerza particularmente en explicar que un hacker no es algo negativo, a pesar de que a menudo este término aparezca vinculado a unas connotaciones más siniestras, relacionadas con el espionaje o la apropiación indebida de datos ajenos. “La definición que yo tengo de hacker es aquel que tiene interés por conocer cómo funcionan las cosas a nivel tecnológico, llegar a la raíz de cómo funcionan las cosas”, aclara.

Según el profesor Neira, se pueden establecer dos tipos de hackers: el 'black hat' y el 'white hat'; esto es, hackers de sombrero negro y de sombrero blanco. La diferencia entre ambos es que el hacker de sombrero blanco es aquel que generalmente trabaja al servicio de otras partes, mientras que el del sombrero negro es aquel que trabaja en actividades delictivas. Pero el white hat hacker realiza otro tipo de labores más allá de combatir las injusticias o ayudar a los cuerpos de seguridad del Estado a desempeñar su labor, explica Neira, por ejemplo “estudiando softwares, descubriendo problemas de seguridad y divulgándolo al resto de la comunidad”, pero también puede trabajar como consultor a sueldo. Aclara también el profesor Neira que “el término hacker siempre acaba predominando con sentido negativo”. “También se ha hablado mucho del término cracker, que es que se intenta asignar a alguien que se relaciona con actividades delictivas, lo que pasa es que en prensa es un término que no termina de calar, el que cala es el término hacker”, y resulta que al hablar de hackers “tiene unas connotaciones asociadas negativas”.

BITCOIN: LA MONEDA DIGITAL

Para llevar a cabo las transacciones comerciales que se realizan a través de la deep web se ha creado una criptodivisa descentralizada que facilita estos intercambios. Las posibilidades de anonimato del euro, el dólar o el yen quedaron desplazadas en 2009 cuando el señor Satoshi Nakamoto anunció la creación de esta nueva moneda, el bitcoin. Hasta que apareció, todos los pagos en el comercio electrónico se canalizaban a través de entidades centralizadas de confianza. Sin embargo, el bitcoin no está respaldado por ningún gobierno ni depende de la confianza de una entidad emisora. En el momento de su primera emisión, el bitcoin tenía un valor parejo con el Dólar norteamericano de uno a uno. En la actualidad, un bitcoin equivale a 263 $.

La exagerada inflación de la divisa digital podría despertar las suspicacias de aquel que explora las profundidades de la deep web. Pero el profesor Pablo Neira no cree que esto tenga que ver sólo con la criminalidad. “El aspecto especulativo del bitcoin tiene que ver con la naturaleza especulativa de la economía; la economía ya de por sí es especulativa”, subraya. “El bitcoin no tiene una autoridad central que regule el valor de esa moneda, por lo que los ataques especulativos se vuelven más fuertes, pero ha habido ya ataques especulativos en Europa”, apunta el profesor, quien explica que hace algunos años “hubo uno contra la libra orquestada por una gran corporación, y el banco central británico no fue capaz de luchar contra ella”. En este panorama, con una autoridad central incapaz de defender su divisa ante ataques especulativos organizados, se torna especialmente difícil hacerlo con el bitcoin, ya que éste se mueve en un espacio completamente desregulado. El profesor Neira cree que el aumento del valor de esta divisa “está asociado también a que hay personas poniendo dinero ahí porque a nivel especulativo es rentable”. “El valor del bitcoin era X, y en tres años se ha disparado. El que tuviera su dinero invertido en bitcoins ha pegado un pelotazo”, señala. No obstante, este fenómeno no se aleja de la realidad económica más básica e inmediata: la oferta y la demanda. “Hay un interés por parte de inversionistas. Si todos quieren comprar bitcoins, pues su precio se dispara. El cambio de una moneda, de euro a dólar, viene controlado por una autoridad central que emite más o emite menos”, advierte, “en el caso del bitcoin, la emisión es continuada por parte de toda la infraestructura de *mainer*”, esto es, softwares que generan monedas. Asimismo, existen páginas especializadas en la deep web que cobran pequeñas tasas por convertir los bitcoins en otras monedas. Páginas como, por ejemplo, EasyCoin o WeBuyBitcoin, que envían directamente el dinero a cuentas de PayPal, a través de la Western Union o incluso mediante correo ordinario.

El nombre del creador de la divisa, Satoshi Nakamoto, no es más que un seudónimo bajo el que se oculta el grupo de personas que desarrollaron tanto el bitcoin como su software de referencia, Bitcoin Core. A día de hoy, la identidad de Nakamoto sigue siendo una incógnita y el objeto de múltiples especulaciones, sin que ninguna de las investigaciones llevadas a cabo hayan reportado resultados convincentes.

El bitcoin es la moneda virtual que se ha generado a través de internet, pero tiene un inconveniente principal, según el inspector Joaquín Pérez del CNP. “Muchos países son todavía reacios a utilizarlo. En Sudamérica, por ejemplo, que es donde están algunos de los países más exportadores de droga, rechazan los bitcoins porque ellos quieren el dólar encima de la mesa”, apunta, “y si lo tienen que esconder, lo van a esconder en un sótano, como ocurrió en los inicios de los grandes cárteles colombianos”. Pero el inspector Pérez va más allá, y apunta que “como se genera tanto dinero, lo que se crea es un campo virtual de tráfico societario inventado para poder justificar el trasiego de dinero de un país a otro”. Es entonces cuando actúan los organismos estatales, tanto la Policía como la Agencia Tributaria, porque “hay una ley específica que obliga, por el blanqueo de capitales, a distintos organismos, instituciones o personas, a comunicar a las autoridades cualquier movimiento sospechoso”. Quiere esto decir, que aunque el individuo no comunique a las autoridades el trasiego de dinero superior a tres mil euros, sí lo va a hacer el banco, porque la cuenta ha dado el aviso. Así es como trabaja la policía, explica el inspector Pérez, “eso es un elemento legal que permite un control para ver qué es lo que está sucediendo, a nivel vigilativo, porque tú no puedes prevenir eso, pero si pones más posibilidades para cogerlos, ellos tendrán que inventar otras estructuras, y de hecho las montan”.

El inspector Pérez profundiza sobre el aspecto de las estructuras que desarrollan las organizaciones criminales para salvar estos controles. Por ejemplo, “si tú tienes que pasar de una cuenta a otra 500 millones de euros, porque has hecho una compra de dos aviones que vas a vender en Libia, está claro que no vas a hacerlo de forma normal: un recibo de 200 millones de euros a cambio de dos

Mig-21”, explica con cierta ironía. “Entonces necesitan un entramado societario, un entramado de conocimientos legales a nivel internacional y, sobre todo, se necesitan contactos en los dos sitios, no en los países de entrada y salida de dinero, sino en otros países, que ahí es donde juega una gran baza la virtualidad”.

ACTUACIÓN POLICIAL CONTRA EL CIBERCRIMEN EN LA DEEP WEB

En las esferas de la deep web se ocultan múltiples organizaciones criminales que obtienen elevados beneficios como resultado de su actividad ilegal. Los servicios de seguridad de los diferentes Estados se empeñan en neutralizar estas redes, pero la actuación policial resulta especialmente compleja dado que estas organizaciones se mueven en un espacio donde la primera garantía es el anonimato. Para rastrear las conexiones aleatorias entre los distintos nodos intermediarios es necesario montar un dispositivo policial muy costoso y complicado que, en la mayoría de los casos, suele revelar pequeñas transacciones de menudeo de drogas. De hecho, el 31'60% de las ventas son de cannabis; seguida por un 21'05% de productos farmacéuticos como Ritalín y Xanax; que, junto al 10'53% de MDMA, constituyen más de la mitad de los productos que se comercian a través de la deep web.

“Con independencia de que podamos fijarnos en lo que ocurre en Internet, los hechos delictivos en algún momento tienen que hacerse efectivos, pasan de la virtualidad al campo real”, apunta el inspector Pérez. Los movimientos de bienes a través de la deep web pueden parecer imposibles de rastrear, pero el anonimato sólo dura lo que esas transacciones tardan en gestionarse. “Tiene que haber un sitio donde haya una trata de mujeres, un sitio donde esté la droga... la virtualidad podemos establecerla en un campo intermedio, el campo de la gestión, información que cruce o no, citas que se produzcan y, sobre todo, traslado económico a través de cuentas bancarias”, explica Pérez.

Los intercambios de mercancías en la deep web funcionan con una estructura muy similar a la de plataformas de compra-venta online como eBay o Aliexpress. Con productos no demasiado voluminosos, el vendedor envía el paquete y llega directamente a casa. Cuando se trata de materiales más evidentes suelen establecerse otro tipo de medidas para asegurar la entrega, como las citas en persona a través de intermediarios o el establecimiento de códigos secretos para su recogida. Principalmente, la Policía trabaja a través de las aduanas para detectar los envíos de mercancías ilegales. Pero eso también tiene inconvenientes. “En España y en la mayoría de países Europeos”, apunta el inspector Pérez, “cuando existe la libertad de comercio y existe la libertad de movimiento y de mercancías, tenemos unas fronteras exteriores, no interiores”. La cantidad de movimientos diarios limita enormemente las posibilidades de actuación de la policía. “No hay que ser muy listo para saber que en el puerto de Algeciras entran, por ejemplo, 30.000 contenedores diarios, que yo creo que serán más”, explica Pérez, “la capacidad de aduanas para abrir contenedores y ver lo que hay es de un 1%. Al día se pueden abrir 100, por decir un número”. En este aspecto, el comercio es declarativo; es decir, las empresas declaran una compra y una venta, y la policía hace un ejercicio de confianza creyendo que lo declarado es lo que va en el contenedor. “Ese es el gran handicap”, advierte Pérez, “porque si no existiese esa libertad de movimiento las mercancías no se moverían con tanta celeridad”. Por eso es tan importante el trabajo previo de investigación, tanto en España como en las embajadas principalmente de países productores, que se coordinan mediante oficinas de enlace para que esas informaciones lleguen. “Nosotros somos países receptores o de tránsito, por tanto nuestras investigaciones estarán fijadas en si llega la mercancía o no”, subraya Pérez, “los países productores son lo que tienen que estar pendientes de si sale o no, porque salir va a salir”.

La única forma de controlar las transacciones de mercancías ilegales es a la entrada y la salida de éstas. La Brigada de Investigación Tecnológica (BIT) de la Policía Nacional se encarga de escudriñar la web para localizar las posibles actividades ilegales, pero es muy complejo. El inspector Pérez explica que "la BIT se fija en los delitos que estadísticamente hablando se producen más a menudo, como la pornografía infantil", pero resulta muy complicado vigilar todo el trasiego de información que se mueve a través de la deep web. "Puede que pase un perro al lado del contenedor y salte la liebre, pero si yo voy y abro un contenedor concreto es porque tengo ya información previa que hemos podido obtener a través de nuestras fuentes, pero que esa información se haya obtenido en la red es muy complicado, porque tienes que tenerlo localizado en la entrada o en la salida", continúa explicando el inspector, "salvo grandes poderes estatales que sean capaces de interceptar las comunicaciones en internet, y no creo que en España haya muchos". Resulta difícil hacer un seguimiento exhaustivo de los paquetes de información que circulan por la red, "a no ser que tengas unos equipos potentes para hacer una desviación de información a unos servidores que tendrían que ser monstruosos", subraya.

A nivel policial existen diferentes agencias encargadas de detectar y neutralizar el crimen organizado. En España hay tres oficinas centrales de comunicación a nivel internacional, que son Interpol, Sirene y Europol. La Interpol es la oficina policial por excelencia, lleva fundada desde 1923 y son 190 países los que en la actualidad están adheridos a su programa, por tanto "deben seguir unos cánones de estructura, cumplir una serie de documentos para participar en los intercambios de información, y tienen la posibilidad de solicitar o demandar determinada información a otros países, siempre desde el punto de vista policial", informa el inspector Pérez, de la Policía Nacional. Además, el inspector Pérez ilustra con un ejemplo cómo funciona la policía internacional según su grado de jerarquía. "Imagina que la Interpol desde Alemania está haciendo una investigación, que en la mayor parte de los casos está judicializada, y necesita información operativa de la zona de Sevilla, entonces la Interpol de Alemania, a través de sus grupos correspondientes, comunica a Interpol Madrid, que deriva esa información a la localidad competente para gestionarla. Es decir, a última instancia, podemos decir que la inmensa mayoría de la policía judicial en España es Interpol, porque trabaja a petición". La Unión Europea tiene su propia agencia de investigación, la Europol, que se encarga de coordinar todas las investigaciones de crimen organizado en Europa. De este modo, todo está interconectado. Para garantizar que se persigue el crimen sea en el país que sea, existen comisiones rogatorias internacionales y equipos conjuntos de investigación que permiten el acceso, con determinadas normas y bajo control judicial, a la policía de otros países en España, para trabajar un hecho delictivo concreto y guiada por las pautas que marca la Ley de Enjuiciamiento Criminal.

DELITOS SOCIETARIOS

A la hora de vender y comprar productos mediante la deep web, son muchos los delitos en que puede incurrirse. Delitos normales, como el blanqueo de capitales o la organización criminal; delitos más enrevesados como el cohecho activo o pasivo -explica el inspector Pérez que los criminales "van a intentar aplicar dinero a determinadas estructuras del estado para acceder a la posibilidad de que echemos la vista a un lado o no se revisen"-; pero sin duda los más complicados son los delitos societarios, derivados de la fuerte actividad económica que realizan. Los asesores de estas empresas no buscan cometer delitos, sino que se valen de las lagunas legales que puedan existir tanto en las leyes nacionales como internacionales. "Por ejemplo, hace poco se descubrió que Luxemburgo tenía acuerdos con grandes empresas internacionales para que tributasen allí al 1%, entonces las empresas montan sus sedes principales en Luxemburgo para que declaren allí", apunta Pérez, "todo son transferencias que se hacen a su sede principal en base a sus estatutos y a su organización;,y eso no está regulado al estar dentro de la Unión Europea; no se hace control del

IVA, y estás viendo que en vez de computar aquí los ingresos, lo vas a hacer allí al 1%".

Las organizaciones que se benefician del tráfico de mercancías ilegales necesitan tener una infraestructura societaria "que genere credibilidad hacia los países para que piensen que compran y venden cosas, y así conseguiguen tener un tráfico de dinero. Montar un artificio de dinero societario internacional cuesta una millonada, pero los beneficios que genera son muchísimo más grandes", indica el inspector de la Policía Nacional. "En esta materia, la hipocresía internacional es importante", advierte, "los paraísos fiscales son como las válvulas de escape para que la economía normal siga funcionando. Si no tuviéramos esos paraísos fiscales habría empresas que no pondrían en juego determinado dinero porque los beneficios iban a ser menores que los que ellos quieren tener". Y la verdad es que hay lugares que se presentan como especialmente idóneos para asentar un entramado societario, por las facilidades con las que acogen a estas sociedades. Por ejemplo, las Islas Caimán, "que tiene una tributación exenta de impuestos y ningunas condiciones de identificación de los titulares de las empresas, y encima no van a responder a ninguno de los requisitos internacionales que se les pueda hacer en materia de justicia", afirma Pérez. Pero el inspector va más allá. "Gibraltar es un paraíso fiscal", afirma contundente, "allí hay creadas numerosísimas empresas ficticias, sin movimiento, empresas creadas ex proceso, para tapar un verdadero negocio que se está produciendo en otro sitio y para que los nombres reales de los propietarios de ese negocio no se sepan. Y como hay un secreto, evidentemente, no van a revelarlo".

DEEP WEB Y LIBERTAD DE EXPRESIÓN

A menudo se relaciona la deep web como un espacio propicio para alojar a las organizaciones criminales que operan en todo el mundo y para facilitar el narcotráfico y las actividades ilegales. Pero sería un grave error limitar las posibilidades que ofrece este lugar al cibercrimen, obviando el infinito valor que tienen los sistemas de comunicación cifrada para los periodistas o los activistas. Inmediatamente, pensar en la deep web como herramienta de disidencia política remite a países como China, donde el gobierno tiene instalado un gran cortafuegos que recoge en sus redes toda la información que circula y un equipo inmenso de burócratas vigila constantemente que no se filtren datos perjudiciales para el Partido. Pero no hay que irse tan lejos. Recientemente la deep web ha emergido del subterfugio de las oscuras orillas de la informática especializada para poner su existencia en conocimiento público gracias al mediático y polémico caso Wikileaks. Cuando Julian Assange y su equipo decidieron hacer públicos una serie de documentos de secretos oficiales de Estado que comprometían seriamente a la Administración norteamericana, la opinión pública comenzó a tomar consciencia del potencial que radica en la internet profunda.

Julian Assange o Ridley Manney son nombres muy sonados por los múltiples documentos filtrados. El inspector de policía Joaquín Pérez explica que al revelar estas informaciones confidenciales, ambos incurrieron en revelación de secretos oficiales de Estado. "Somos nosotros y tenemos unos códigos de información, todos los sistemas están auditados y con contraseñas, y yo soy el responsable de mis accesos, si entran con mis datos y se produce cualquier tipo de intrusismo es a mí a quien van a pedir responsabilidades, que soy un inspector de policía. Imagínate un tío que está a otros niveles", subraya. Pero la realidad va más allá, y es que el acceso a bases de datos y la posibilidad de obtener informaciones privadas es un asunto que puede ser delincuencial, sin embargo en los últimos años se ha tenido conocimiento de que los propios Estados, como el alemán o el norteamericano por citar algunos, han estado ejerciendo este tipo de prácticas que a otra persona le costarían la cárcel. ¿Estamos, pues, ante otro ejercicio más de hipocresía gubernamental?

Cada vez con mayor intensidad, la esfera globalizadora de la red está dejando de ser materia aislada, reservada a unos pocos reconocedores de su potencial latente, para integrar a todos los eslabones de

la sociedad contemporánea. Existe un fuerte movimiento de activismo social a través de internet. Son muchos los nombres con los que se han popularizado las distintas asociaciones dedicadas a la lucha contra las opresiones gubernamentales y los intereses macroempresariales, como la archiconocida red Anonymous, pero lo cierto es que a nivel global el activismo organizado se ha formulado como un método efectivo de lucha, sirviéndose de las ilimitadas herramientas que ofrece internet. El *cypherpunk* es tanto el movimiento como el método. Está formado por personas anónimas que consideran que la privacidad es un elemento fundamental y que debe ser garantizada por los medios tecnológicos. Tor, por su parte, es una red que garantiza el anonimato, y eso tiene unas connotaciones de libertad muy fuertes. El profesor Pablo Neira considera que "el anonimato garantiza una serie de aspectos relacionados con los derechos humanos y con la libertad, que son fundamentales, pero también recoge otro tipo de actividades que no nos gustan tanto"; y es que cuando se genera un espacio de libertad absoluto, que auspicia la libertad para todo tipo de movimientos y situaciones, puede salirse de madre. Lo que sí parece claro, como apunta Neira, es que estas actividades ilegales "no son un reflejo de la tecnología, son un reflejo de la sociedad en la que vivimos". Se hace evidente entonces la magnitud del alcance de la deep web. Un espacio que permite a unos lucrarse de actividades ilegales, obtener beneficio del sufrimiento ajeno, y comerciar con todo tipo de oscuridades; mientras que a otros les permite ejercer libremente, con la seguridad del que se esconde tras sus sombras, un derecho fundamental como es la libertad de expresión. Porque en esta era tecnológica todavía existen personas que deben refugiarse para denunciar las prácticas cuestionables de sus gobiernos, bien sean dictatoriales o democráticos.

ANEXO 1:

TRANSCRIPCIÓN LITERAL DE ENTREVISTA CON INSPECTOR PÉREZ DEL CNP

P- En primer lugar quería saber cómo trabaja la Policía para dar caza a las redes delictivas a nivel internacional de todo este movimiento de tráfico de personas, armas, drogas… los organismos que están implicados y su grado de jerarquización.

R- A nivel de policía, para el tema de crimen organizado ya sea a nivel nacional o internacional, tienen diferentes escalones. Tenemos 3 oficinas centrales de comunicación que a nivel internacional son Interpol, Sirene y Europol. La Interpol es la oficina policial por excelencia, lleva fundada desde hace ochenta años y hay más de 100 países que están adheridos, esto es, que deben seguir unos cánones de estructura, cumplir una serie de documentos para participar en los intercambios de información, y que tienen la posibilidad de solicitar o demandar determinada información a otros países, siempre desde el punto de vista policial). Imagina que la Interpol desde Alemania está haciendo una investigación, que en la mayor parte de los casos está judicializada, y necesita información operativa de la zona de Sevilla, entonces la Interpol de Alemania, a través de sus grupos correspondientes, comunica, a través de su central en Berlín, a Interpol Madrid, que deriva esa información a la localidad competente para gestionarla. Es decir, que a ultima instancia podemos decir que la inmensa mayoría de la policía judicial en España es Interpol porque trabaja a petición. Eso a nivel internacional, para cuestiones derivadas de un país a otro, para averiguar y poder aportar información. Luego investigaciones a nivel internacional, en España existe la Europol, que es la que coordina todas las investigaciones en Europa a nivel de crimen organizado. De hecho se cumplen diversos requisitos para el tema de bases de datos, de intercambio de información... hay accesos a determinados niveles, hay información que otros países vuelcan en esas bases de datos. Es decir, imaginate que tu tienes una persona buscada internacionalmente y francia pone una orden de detección que figura en los ordenadores españoles. Así está todo interconectado. Con independencia de que luego se lancen determinados avisos puntuales que llegan a la oficina por una persona concreta con un hecho concreto para realizar determinadas gestiones. Y por último, a nivel de investigación existen los niveles de coordinación. En Madrid a nivel de policía nacional, guardia civil y secretaría de estado hay una serie de organismos que lo que hacen es coordinar las investigaciones para que no se dupliquen actuaciones. La guardia civil y policía nacional que podrían entrar en una investigación por dos vías para que a su vez esos organismos sean los receptores y emisores de informaciones que sean necesarias para otros países. Un país cualquiera no se puede dirigir a la policía de Sevilla a pedir información, lo tienen que hacer a través de la Interpol, pasar el filtro de esos organismos de coordinación, para establecer los niveles de la investigación y ya entraríamos en los mecanismos legales: comisiones rogatorias internacionales, equipos conjuntos de investigación... pueden acceder con determinadas normas y bajo control judicial la policía de otros países en España para trabajar un hecho delictivo concreto con una serie de pautas que te marca la ley de enjuiciamiento criminal y nosotros podemos participar en investigaciones de otros países también mediante esos requisitos legales

P- Y para ordenar una investigación judicial en este sentido, de tráfico de armas, drogas y personas... qué hace falta para que se organice? Tengo entendido que es bastante costosa a nivel económico y que cuesta mucho tener pruebas reales de los movimientos que se realizan a través de internet.

R- Con independencia de que podamos fijarnos en lo que ocurre en Internet, lo cierto es que los hechos delictivos a los que te refieres en algún momento tienen que hacerse efectivos, pasan de la virtualidad al campo real... tiene que haber un sitio donde haya una trata de mujeres, un sitio donde

esté la droga... la virtualidad podemos establecerla en un campo intermedio, el campo de la gestión, información que cruce o que no, citas que se produzcan... y sobre todo, traslado económico a través de cuentas bancarias. Aunque parezca que no, se producen porque si tu vas a comprar droga en kilos, puedes llevar 60.000 euros encima para hacer la compra, pero si estamos hablando de transacciones de cientos de millones de euros, los malos no llevan tanto dinero encima.

P- ¿Se hace a través de bitcoins?

R- El bitcoin es la moneda virtual que se ha creado a través de internet, pero tiene un inconveniente. Muchos países son todavía reacios a utilizarlo. En sudamérica, por ejemplo, que es donde están algunos de los países más exportadores de droga, rechazan los bitcoins porque ellos quieren ver "martín, martín", es decir, el dólar o el euro, encima de la mesa, y si lo tienen que esconder, lo van a esconder en un sótano, que eso fueron los inicios de los grandes inicios de los cárteles colombianos. Como se genera tanto dinero, lo que se crea es un campo virtual de tráfico societario inventado para poder justificar el trasiego de dinero de un país a otro.

P- Ahí es donde actúa la policía a nivel preventivo.

R- Ya no la policía, también otros elementos dentro de los organismos estatales, es decir, Hacienda o la Agencia Tributaria, porque ten en cuenta que hay una ley específica que obliga, por el blanqueo de capitales, a distintos organismos, instituciones o personas, a comunicar a las autoridades cualquier movimiento sospechoso. Los notarios, por supuesto los bancos, los primeros; las comunicaciones que tu tienes que dar cuando haces un trasiego de dinero superior a 3000 euros, aunque tu no lo hagas el banco lo va a hacer por ti, porque en tu cuenta ha dado el aviso. Entonces, eso es un elemento legal que lo que permite es un control para ver qué es lo que está sucediendo, ya no preventivo pero sí vigilativo, porque tu no puedes prevenir eso, pero si pones más posibilidades para cogerlos, ellos tendrán que inventar otras estructuras, y de hecho las montan. Porque si tu tienes que pasar de una cuenta a otra 500 millones de euros, porque has hecho una compra de dos aviones que vas a vender en Libia o en cualquier otro sitio, que se está produciendo, lo que está claro es que no lo vas a hacer de una forma normal: recibo por 200 millones de euros a cambio de dos Mig-21. Entonces necesitan un entramado societario, un entramado de conocimientos legales a nivel internacional y sobre todo se necesitan contactos en los dos sitios, no en los países de entrada y salida de dinero, sino en otros países, que ahi es donde juega una gran baza la virtualidad.

P- Con respecto a esto que has dicho me interesan fundamentalmente dos cosas: Por la deep web funcionan los intercambios de mercancias con una estructura muy similar a la de plataformas de compra-venta como eBay o Aliexpress, que desde China o el país que sea meten el producto en un avión y llega directamente a tu casa. Qué tipo de controles hacen en aduanas para evitar esto?

R- En España y en la mayoría de países europeos, cuando existe libertad de comercio, y existe la libertad de movimiento y de mercancías, dentro de lo que es la Unión Europea, tenemos unas fronteras exteriores, no interiores, pero sí exteriores. No hay que ser muy listo para saber que en el Puerto de Algeciras entran, por ejemplo, 30.000 contenedores diarios, que yo creo que serán más; capacidad de aduanas para abrir contenedores y ver lo que hay: un 1%. Al día se pueden abrir 100, por decir un número. Ten en cuenta que el comercio es declarativo, tú declaras una compra y una venta, la policía tiene que creerse que eso es lo que va en el contenedor. Ese es el gran handicap porque si no existiese esa libertad de movimiento las mercancías no se moverían con tanta celeridad. Esa libertad de movimiento es la que ha permitido que exista esa posibilidad de engaño y de camuflaje, por eso cuando tu abres un contenedor y las tres primeras filas son pantalones vaqueros y las 15 de atrás son bolsas de cocaína. Ahí está el trabajo de investigación que no

solamente investiga en España, ten en cuenta que España tiene embajadas en otros países y otros países las tienen aquí, y ahí hay unas oficinas de enlace a nivel interior en todas esas embajadas para las informaciones que lleguen. El hecho de que se compren 400 toneladas de coca en Colombia, los colombianos saben que eso se va a producir y si no lo saben sus oficinas de información van a estar intentando averiguarlo porque son países productores, nosotros somos países receptores o de tránsito, por tanto nuestras investigaciones estarán fijadas en ver si llega o no, ellos tienen que estar pendientes de si sale o no sale (porque salir va a salir), por tanto eso es otro trabajo a nivel informativo previo.

P- Has dicho que esas sociedades tienen una asesoría legal muy grande. Quería preguntarte cuáles son los delitos más frecuentes que se cometen a la hora de realizar estas transacciones. Tengo intención de ver después a algún jurista para que me explique mejor estos delitos.

R- Podemos hablar de delitos normales como el blanqueo de capitales, la organización criminal -que es un delito concreto-, cohecho activo o pasivo -porque van a intentar aplicar dinero a determinadas estructuras del estado para acceder a la posibilidad de que echemos la vista a un lado o no se revisen-; también el tema más complicado de los delitos societarios, administración desleal no porque no es una administración real. En este sentido los asesores de estas empresas no van a cometer delitos, sino que se van a valer de las lagunas legales que puedan existir tanto en las leyes nacionales como internacionales para intentar acceder. Por ponerte un ejemplo, ahora se descubrió hace poco que Luxemburgo tenía acuerdos con grandes empresas internacionales para que tributasen allí al 1%, entonces las empresas montan sus sedes principales en Luxemburgo para que declaren allí, todo son transferencias que se hacen a su sede principal en base a sus estatutos y su organización, y eso no está regulado al estar dentro de la Unión Europea, no se hace el control del IVA, y estás viendo que en vez de computar aquí los ingresos lo vas a hacer allí al 1%. Eso no es ilegal, sino alegal, porque no está regulado y porque dentro de la libre competencia lo que habría que hacer es decirle a Luxemburgo y a otros países que hicieran una normativa tributaria homogénea. Esta gente necesitan tener una infraestructura societaria que genere credibilidad hacia los países para que piensen que compramos y vendemos cosas y así conseguimos tener un tráfico de dinero. Montar un artificio de dinero societario internacional cuesta una millonada, pero los beneficios que genera son muchísimo más grandes. Entonces uno crea una serie de empresas o sociedades en las Islas Caimán porque tiene una tributación exenta de impuestos y unas condiciones de identificación de los titulares de las empresas cero, y porque encima no van a responder a ninguno de los requisitos internacionales que se les pueda hacer en materia de justicia. Blanco y en botella. Los paraísos fiscales, aunque digan lo contrario, y esto es una opinión personal mía, existen porque quieren que existan. Son como las válvulas de escape para que la economía normal siga funcionando. Si no tuviéramos esos paraísos fiscales habría empresas que no pondrían en juego determinado dinero porque los beneficios iban a ser menores que los que ellos quieren tener. Entonces esos paraísos fiscales es la válvula de escape para que si ganan 1000, tributen sólo 200 y los 800 restantes para la jarilla. Si esos paraísos no estuvieran no les compensaría tributar por los 1000. En esta materia, la hipocresía internacional es importante. Nos rasgamos las vestiduras porque Gibraltar es un paraíso fiscal, porque es lo que es, allí hay creadas numerosísimas empresas ficticias, sin movimiento, una empresa creada ex proceso, creadas para tapar un verdadero negocio que se está produciendo en otro sitio y para que los nombres reales de los propietarios de ese negocio no se sepan. Y como hay un secreto, evidentemente, no van a revelarlo.

P- Si aplicamos esto a delitos menores, por ejemplo a los llamados TIPS (manuales de falsificación de documentos de identidad, de tarjetas bancarias) o los manuales de fabricación de artefactos explosivos o venenos. Esto está dentro de la deep web, pero son delitos?

R- La búsqueda en internet no conlleva ningún delito. Es lo que te digo, pasamos del campo virtual al campo real. Yo puedo saber, y de hecho lo sé, cómo se falsifica una tarjeta de crédito, yo puedo saber cómo se roba un vehículo, otra cosa es que lo ejecute. Salvo la reforma que pueda haber ahora a nivel de terrorismo, que se contemple en el código penal el acceso a esas páginas. Yo no lo sé, pero a lo mejor se pone una serie de cotos para que quien visite esas páginas o descargue ciertas cosas, pues no sé, que podamos catalogarlas como páginas prohibidas. Si buscamos... no sé...

P- Por ejemplo, ¿cómo fabricar una mina antipersona?

R- Te lo va a poner, y con dibujitos y cronogramas, otra cosa es que tú lo coloques y explote a alguien. Es decir, el paso de la virtualidad a la realidad. Pero esto te pediría que se lo preguntases a un abogado. La gente busca en internet y hoy en día se busca practicamente todo. Pero de ahí a que sepamos... La pornografía de mayores, todo lo que tu quieras, porque no está prohibida. Ahora, pornografía de menores está prohibida, por tanto empiezan a enmascarar las actuaciones dentro de internet para intentar que no se detecte sus actuaciones con pornografía de menores... mediante servidores exteriores, anonimizadores de cuentas, encriptamiento de las imágenes, para establecer una dificultad de acceso, porque la policía está rasteando diariamente la red porque es un sitio donde se están produciendo delitos. ¿Por qué pasa un coche patrulla por aquí? Porque tiene que estar vigilando. Pues lo mismo en la red... y ya nosotros no te digo, pero los yankis no es que vigilen la red, es que la escudriñan a diario.

P- Me llama mucho la atención los papeles de Wikileaks, de Julian Assange y Ridley Manney, que filtraron documentos sobre la guerra de Irak y las maniobras de Estados Unidos a través de la Deep Web.

R- Ahí estaríamos incurriendo en una revelación de secretos oficiales de estado. Si yo, como funcionario, que tengo acceso a unas bases de datos donde hay datos de personas y tal, si eso lo filtro estoy cometiendo una revelación de secretos y en España me pueden condenar por delito. Otra cosa es lo que está ocurriendo con este hombre que habrá sacado esa información como sea, habrá tenido acceso a una serie de filtros pero no deja de ser un delito. Otra cosa es la repercusión a nivel internacional y que haya una serie de países que quieran intervenir, eso no lo voy a discutir, ya se entenderán ellos. Pero cuando tú entras en una empresa tú tienes unos contratos de confidencia y no digamos ya a nivel de estado. Somos nosotros y tenemos unos códigos de información, todos los sistemas están auditados y con contraseñas y soy yo el responsable de mis accesos, si entran con mis datos y se produce cualquier tipo de intrusismo es a mí a quien van a pedir responsabilidades, que soy un inspector de policía. Imaginate un tío que esté a otros niveles. Partiendo de la base de que este tío haya podido cometer ese delito, el resto es bombo. Es como lo que ocurre con el fulano este... Falciani, que ha llevado la lista del HSBC. Centrémonos. Algunos habrán evadido, pero este hombre cuando se llevó la lista estaba cometiendo un delito porque se estaba apropiando de una información secreta y su contrato se lo impedía. Es que aquí no todo vale, porque un policía necesita una orden de registro para entrar en tu casa, no puedo entrar porque sí. Entonces es fascinante el tema de internet en el sentido... ¿qué fue antes, el huevo o la gallina? Ahí yo te pediría que el tema de accesos a bases de datos y posibilidad de información que puede ser delincuencial y que pueden estar ejerciéndolo los propios Estados, por supuesto, nos ha jodido, pero ¿qué es? ¿el hecho de que yo revele que el Estado está haciendo algo mal? ¿o que yo para revelar esa información he entrado en sus bases y cometido un delito? Pues ambos, en realidad.

P- Aparte, el tema del estrecho que estábamos hablando. Ya fuera de entrevista. Yo tengo un amigo que trabaja en el SIVE y quería preguntarle... porque quería usar a este hombre como fuente, pero no tengo muy claro como relacionarlo con la deep web. Yo creo que este tipo de movimientos se

producen a través de los puertos y luego hay muchas organizaciones que se dedican a distribuirlo.

R- A ver, el mercado negro internacional y la influencia que tienen las nuevas tecnologías en ese mercado negro. Al fin y al cabo, el SIVE y el tema de los contenedores no deja de ser el traslado de lo virtual a lo real. O sea, ¿cómo lo encajas? Si tu quieres hablar de lo que es el internet profundo y cómo se usa la red para ejecutar alguna tipología delictiva... yo no lo veo ahí. Pero tú eres el dueño del trabajo. El SIVE es al fin y al cabo como un Gran Hermano en el Estrecho, como los radares de los aeropuertos: tenemos 15 aviones y cuantos hay, 16, hostia, ¿eso qué es lo que es? Entonces, a partir de ahí.... si tu detectas una entrada de droga en un contenedor. Puede ser que pase un perro al lado del contenedor y salte la liebre, pero si yo voy y abro un contenedor es porque tengo ya información previa, y esa información es la que hemos podido obtener a través de nuestras fuentes, que se haya obtenido información en la red, que es muy complicado porque tienes que tenerlo localizado en la entrada o en la salida (de información), salvo grandes poderes estatales -que no creo que en España haya muchos- que sean capaces de interceptar las comunicaciones en internet. Los paquetes de información que van en la red, a no ser que tengas unos equipos potentes para hacer una desviación de información a unos servidores que tendrían que ser monstruosos. Si no, mirando por internet, ¿en qué te fijas? ¿dónde pones tu foco?

P- Pero la Brigada de Investigación Tecnológica tendrá esos servidores para interceptarlos.

R- Pero mira lo que te digo, la BIT se fija en los delitos que estadísticamente hablando se producen más a menudo. Por ejemplo la pornografía infantil. Se trabaja a nivel internacional porque hay una serie de información que está volcada en la red y que no son nuevas. Los archivos en internet tienen una 'matrícula'. A nivel internacional se crean bases de datos con las 'matrículas' de esas imágenes y esos vídeos, y eso es lo que se rastrea para saber si se han movido o no se han movido.

P- Ese es uno de los principales problemas de la deep web. Por ejemplo entramos desde tu ordenador al servidor de EL MUNDO, y la conexión es directa de tu servidor al del medio; pero sí hacemos eso a través de la deep web hacia una página de pornografía infantil no es una conexión de servidor a servidor, sino que accedes desde un servidor a otro mediante saltos aleatorios entre otros servidores. Por eso cuesta tanto localizarlo.

R- Ahí está lo que te digo, ¿dónde se puede controlar? A la entrada y la salida, me lo has dicho tú mismo. Yo no soy ningún experto en informática. Cuando tu trabajas lo que intentas es que nadie sepa que eres tú quien está ahí, y si hace veinte años había programitas que te borraban tu IP de conexión, no me imagino ahora lo que puede haber. Si antes tenías que hacer virguerías para conectarte a un servidor y derivarla a otros sitios, ahora me imagino que habrá aplicaciones que lo hacen con sólo darle a un botón. Y la segunda parte, si eres capaz de tener varios ordenadores zombi, que son los que se utilizan mientras estás tú detrás, pues ya está.

(LLAMADA TELEFÓNICA. MIN 31'10" // 33'25")

R- Bueno por donde íbamos

P- Estábamos en las entradas y las salidas, pero esa parte ya la tengo bastante clara. Te voy a hacer un par de preguntillas más: ¿Tú estabas trabajando en algo relacionado con la pedofilia?

R- No, yo trabajo el tema de los delitos contra los menores. El grupo que se encarga de todos los delitos tecnológicos es otro grupo de la brigada. Lo que pasa es que en su momento sí tocamos, cuando estábamos destinados en Málaga, el inicio del tema de las imágenes, el traslado de

documentos... ha cambiado mucho desde entonces. Ahora la simple posesión de imágenes de menores es constitutiva de delito. Antes había que comprobar que se había realizado un traslado. Ahora basta con demostrar que hay en un ordenador imágenes de menores con contenido pornográfico.

P- ¿Cómo funcionan las personas que captan a los menores? Ya no sólo para la pornografía, sobre todo a nivel de venta de esclavos o de venta de órganos.

R- Que yo sepa, aquí en España no se han captado menores para el tema de venta de órganos. A nivel de policía judicial si me suena un poco más. Se trabaja con el tema de la trata de seres, la pornografía, la prostitución... pero el tráfico de órganos, puedo decir que he conocido algún caso en España, pero no puedo decirte a nivel de investigación cómo se actúa. No deja de ser una investigación normal. Se me ocurre pensar una recepción en un hospital, que llega una persona en estado grave y se dan cuenta de que le han extirpado un riñón y no ha sido en el hospital, entonces la investigación empieza a trabajarse ahí. Porque sino no te llega la información. Seguramente tú puedes ver que se venden órganos a través de la web, pero que aquí se hayan dado esos casos, no me suena. Que yo sepa, eh. El tema de los menores es un tema que no sale por la televisión por el tema de la protección. Claro que detenemos menores que le pegan a los padres, o tenemos menores que han sido víctimas de abusos sexuales dentro de la familia. Pero eso no sale, y si sale es porque el menor aparece gravemente maltratado en un hospital. Eso es algo mediático y se dispara.

P- Tengo intención de hacer una especie de inmersión en la deep web. Ponerme en contacto con algún conocido que me ayude a entrar y pueda verlo a través de mi propio ojo. ¿Puedo meterme en un lío por entrar en la deep web?

R- Si una persona hace una entrada en un servidor y para ello ha tenido que romper algunas claves de acceso, evidentemente es un delito. Es un acceso ilegal. Has tenido que hacer una entrada con fuerza, según el código penal, porque se considera llave los códigos de entrada. Si tu los revientas con un programa concreto has usado una herramienta adecuada para romper un seguro de entrada. Otra cosa es que tú entres en los sitios que no tienen un nivel de seguridad, si no hay ningún cortafuego que te lo impida, no estás haciendo nada ilegal.

P- Tengo entendido que tienes que tener un disco duro externo para acceder a la deep web para ver las imágenes.

R- Ahí ya me pillas fuera de juego.

P- Las imágenes no se ven, tienes que descargarlas de la deep web. Cada archivo puede tener muchos nombres, a lo mejor descargo alguno y resulta que es un vídeo en el que están violando a un niño. ¿El simple hecho de ver eso, almacenarlo aunque luego lo borre inmediatamente, es delito?
R- Evidentemente. Nosotros vemos que se ha descargado un archivo en ese ordenador... o hagamos al revés, quien se descarga una película y resulta que es una película pornográfica de menores. Si avisas a la policía asumes que tienes que pagar una multa por piratería pero nada más. Otra cosa es que descargues pornografía infantil y te lo calles. A mí en Málaga me ha ocurrido, me llamó un hombre diciendo “mire usted, que mi hijo se ha descargado una película y apareció una fotografía de menores”, fuimos a ver el ordenador, vemos los puntos desde los que se ha conectado y se trabaja. Antiguamente tu podías descargarte una película de vídeo que si la metías en un programa, esa película tenía detrás enmascarada una serie de imágenes o un procesador de texto que te lo convertía en una imagen encubierta en segundo plano. Y eso era antiguamente, así que imagínate lo que puede haber hoy.

ANEXO 2:

TRANSCRIPCIÓN LITERAL DE LA ENTREVISTA AL PROFESOR PABLO NEIRA DE LA US

Breve presentación

P- El reportaje que estoy haciendo trata sobre la Deep Web y me está costando bastante encontrar fuentes específicas. He de decirte que, a día de hoy, yo no he entrado en la Deep Web. ¿Tú has entrado alguna vez?

R- Es que la deep web son muchas cosas. ¿Tú qué entiendes por la deep web?

P- Pues, por lo que yo tengo entendido, se accede a través del servidor TOR...

R- Cualquier contenido que no esté indexado, esto es, que no sea fácil de encontrar, ya es de por sí la deep web. Se habla mucho de TOR, pero deep web es cualquier cosa que no está visible, al alcance del navegador convencional.

P- ¿Existen otros navegadores para entrar a ella, a parte de TOR?

R- A ver, TOR no es un navegador. TOR es una estructura concreta de la red, un protocolo de capas de cebolla. Lo que hace es que por cada paquete va abriendo capas con mayor dificultad de acceso. Más que nada está pensado para el tema del anonimato. Lo principal: hay unos puntos de acceso, tú instalas un cliente de TOR en tu ordenador, y con ese cliente de TOR te conectas a un punto de entrada de la red de TOR. Y a partir de ahí tienes acceso.

P- ¿Y según el nivel de profundidad, te garantiza un mayor nivel de anonimato?

R- No, el anonimato viene dado por la cantidad de saltos que da el tráfico a la hora de circular por el acceso.

P- Algo así tenía entendido. Va saltando de servidor a servidor, ¿podrías explicármelo un poco mejor? Porque no lo entiendo. "Por ejemplo, para meterme desde mi servidor personal -que yo no soy un experto en informática, pero bueno, a nivel usuario, yo quiero entrar desde mi casa, desde mi servidor particular quiero conectarme al servidor de... digamos, por ejemplo, el periódico El Mundo. Desde mi servidor a su servidor, hay una conexión bidireccional.

R- Sí, la estructura es cliente-servidor. Tú en casa tienes un navegador, el navegador hace de cliente. El navegador habla una serie de protocolos, en el caso de una navegación convencional, tu navegador habla HTTP, que es un protocolo... es como si... Para ponerlo más sencillo, es como si yo soy el cliente y tu eres el servidor, tenemos que ponernos de acuerdo en la manera en la que hablamos. Por ejemplo el idioma, hablamos en castellano, español, y nos podemos comunicar. Lo que sucede con un servidor y un cliente es que el servidor es como si fuera el chico que está detrás del mostrador de un hotel pendiente de recibir peticiones, y van llegando clientes que son la gente que va a solicitar cosas. Detrás de la barra del hotel va recibiendo peticiones de clientes. "Pues dame una llave", "¿de qué, de la habitación?" "Pues sí", "que quieres dejar una maleta, pues vale". Son una serie de servicios, el servidor tiene un rol pasivo... están pendientes de recibir peticiones de los clientes, y los clientes lo que hacen es que solicitan cosas. Cuando es una navegación normal, tu tienes un navegador web que habla el protocolo HTTP y se conecta a los servidores http. Cuando tu pones tres uves doble y cualquier nombre, lo que sucede es que el navegador primero resuelve ese

nombre mediante DNS -otro protocolo- a una dirección IP, y nada más que tienes la dirección IP se conecta al puerto estándar (los servidores, para permitir comunicación simultánea de diferentes servicios, tiene una multiple facción) Es decir, que hay una serie de puertos y cada puerto tiene unos servicios diferentes. Estos servicios... por ejemplo, en el puerto 80 está el protocolo HTTP, entonces cuando tu te conectas a un navegador, cuando tú pones la dirección, lo que hace el navegador es que se dirige a esa máquina, a ese nombre, en internet y va a ese puerto 80. Si pones HTTPS se va al puerto 443, que es el puerto de comunicación segura. Y se va a ese otro puerto. O sea, depende de lo que tú hagas con el navegador se va a una máquina y accede a los dos puertos que generalmente soportan los navegadores. También soportan FTP, que es otro servicio, lo que pasa es que lo que consigue el navegador es homogeneizar de cara al usuario los diferentes servicios que parecen todos lo mismo porque es la web.

P- Luego están los otros protocolos que serían los anónimos, que están indexados, son los de la deep web, que ahí donde hablamos de los saltos de servidores.

R- Vamos a ver, tú tienes contenidos de internet. Este contenido está alojado en un servidor. Un servidor es una máquina que está encendida 24 horas al día. Generalmente tiene un nombre asociado pero no tiene porque tener un nombre, porque con la dirección IP basta. Yo, en esta máquina sin un nombre, podría instalar un servidor web y poner contenidos ahí. ¿Qué pasa? Que si ese servidor ofreciera un contenido y nadie lo referencia, va a ser más dificil de encontrar. Porque los buscadores lo que tienen es un software, que es un robot, que se suelen llamar "arañas" (spiders), y la araña lo que hace es que se conecta a una web y va siguiendo los enlaces, y cuando sigue esos enlaces va construyendo lo que viene siendo la telaraña de la web, todo el entramado de conexiones y enlaces que hay de una web a otra. Luego ellos hacen su ranking de relevancia, es sabido que uno de los criterios que hay es la cantidad de referencias que hay a una web, luego ellos tienen su forma de canalizar, porque ya la gente se da cuenta y se inventan enlaces superfluos a una web y aumento el ranking, pero los navegadores también tienen un robot que evalúan si esos enlaces son falsos o no y penalizan a los falsos enlaces. Tu piensa que hay mucha gente que depende de que sus contenidos aparezcan en primer lugar en el ranking. Aquí la historia es que hay una serie de buscadores que tienen estas arañas que además aparecen, si eres técnico y tienes un servidor web, puedes ver quién te visita y además te dicen quienes son. "Soy la araña de Bing, soy la araña de Google...", y ellas seguramente vienen de otro enlace que han hecho que llegues ahí. Eso es lo que sería la web convencional. ¿Qué sucede? Que yo puedo esconder contenidos de la web convencional. ¿Cómo lo escondo? Pues haciendo que nadie me referencie. O poniendo un servidor web en un puerto no estándar. Las arañas suelen seguir enlaces o tantear todas las máquinas que hay en internet en el puerto 80 o en el puerto 443, que son puertos frecuentes. 8080, que es menos frecuente... Puertos más o menos frecuentes que son los que te vas a encontrar en una web. Te vas a encontrar un software que habla HTTP, lo que el navegador puede hablar. Si yo lo cambio a un puerto en el que no se ve, hay más probabilidad de que no se vea. Y si esa información... Ahora yo tengo buscar la manera de divulgar esa información porque si quiero que haya gente que acuda ahí a ese contenido, también lo puedo hacer simplemente poniendo un usuario y una contraseña y dándole a mis amigos un usuario y una contraseña. Eso son contenidos que no son indexables y que cualquier otra persona no puede acceder. Eso sería la manera más sencilla de ocultar información visible a los navegadores, porque el concepto de deep web, tal y como yo lo tengo interpretado es, simplemente, lo que no se ve, lo que no es fácilmente alcanzable. Hay mecanismos técnicos muy sencillos para hacer que algo no sea alcanzable, como puede ser ocultar el contenido, poner usuario y contraseña, o cifrar con criptografía de claves...

P- Estamos hablando de cualquier información que alguien quiera ocultar.

R- Luego está la red TOR, que es una red sobre la red de internet.

P- Realmente la red TOR es casi lo que más me interesa, porque en realidad lo que más me ha llamado la atención sobre este tema es la cantidad de dinero que se mueve a través de internet, sobre todo a nivel de organizaciones criminales, venta de armas, de droga, tráfico de personas...

R- En TOR hay mucha información de todo, pero hay mucho SCAM también, que es publicidad falsa. Por ejemplo, compra unos matones a sueldo, tu pagas y crees que contratas un matón, pero luego resulta que tú pagas y no pasa nada. Entonces hay mucho contenido que es SCAM, que también está en el internet normal. Los scammer están en todas partes, lo que pasa es que si uno se refugia en TOR pues lo va a tener más complicado. Ve tú a la policía a decir que te han robado 20.000 euros porque te has ido a una página de TOR, y te van a decir "¿TOR? Espérate que vamos a hablar con la Guardia Civil, con la Brigada de Delitos Telemáticos, mira, que este tiene un problema con la red de TOR".

P- Eso es otra leyenda que no sé cuánto tiene de verdad. Si un usuario entra en la red TOR o en el Internet Profundo, y la Guardia Civil descubre que ese usuario ha entrado, ¿está cometiendo una infracción?

R- No, a día de hoy, que yo sepa no hay ninguna legislación en España que impida acceder a la red TOR. Lo que sí claramente es que en la época digital que estamos hoy día, si estás desde tu casa accediendo a la red TOR te estás visibilizando dentro de la montaña de datos. Porque dentro de la montaña de datos, la mayor parte de la humanidad no accede a la red TOR; y si tu accedes, con los mecanismos de visibilización puedes ver que hay una persona que está accediendo a la red TOR. Entonces metes en un saco a la gente que está accediendo a la red TOR. A la red TOR no necesariamente hay que acceder para ... la red TOR trasciende de lo delictivo, lo que hace es garantizar el anonimato. Y eso tienes que tener en cuenta también que, desde el punto de vista de los derechos humanos, hay muchos países en los que la libertad de prensa está muy cuestionada y donde sacar información de allí es muy complicado. Y este tipo de soluciones tecnológicas permiten que estas informaciones puedan circular.

P- También quería orientar el debate sobre ese punto, porque no es solo tráfico de armas o trata de personas, sino que también las revelaciones de secreto de Estado, que también puede ser muy importante desde el punto de vista de los derechos humanos. Por ejemplo, Wikileaks. Todo salió a través de la red TOR, porque Julian Assange tenían conocimientos de sobra para saber que eso podían ocultarlo... y sin embargo el gobierno federal de los Estados Unidos acabó sabiendo quienes eran los responsables.

R- Obviamente, el aparato de un estado tiene muchos recursos para dedicar a la búsqueda de esos datos. ¿Cuánta gente hay en un país con la cualificación suficiente para realizar ese trabajo a nivel tecnológico? Seguro que se puede restringir la búsqueda.

P- Los hackers abundan en la deep web. Siempre me han hecho advertencias sobre estos términos. Me han dicho un par de cosas que quería confirmar. Primero que a la hora de acceder es muy fácil que los hackers localicen que tú has entrado y te revienten; o sea, que entrar a la red TOR sin unos sistemas de seguridad específicos puede ser peligroso. Y luego también, que por lo visto necesitas un disco duro externo para almacenar lo que sería el caché -corrígeme si me equivoco- del navegador normal.

R- Cualquier software que tú te instales, que no sepas cómo funciona, ni lo que hace... Hay mucha

gente que se instala softwares de páginas como Softonic, o páginas que ofrecen software gratis. Cada vez que uno instala un software está realizando un acto de confianza. Si el software que te descargas viene ya con puerta trasera o con software para utilizar tu ordenador como un bot, o para poder emplearlo en ataques orquestados para negación de servicios, o para espiarte, robarte información... es decir, si viene con funcionalidad de puerta trasera, para utilizarlo como un zombi, eso puede suceder con cualquier software. Es más, yo creo que es más probable que te lo instales con un juego, que hay millones en internet, a que te instales un cliente de TOR manipulado. Como sucedió, yo no se si tu recuerdas que hubo un cliente de TOR, que la web estaba traducida al persa y te ponía como para que los activista de Irán accedieran a la web, instalaran ese cliente y jugaban con que la web estaba en persa. El objetivo era atraer a los activistas iraníes, que accedieran a la red TOR y divulgaran la información... periodistas, activistas, políticos. Se descubrió que al final estaba vinculado al estado iraní. Que el estado iraní tenía un software de puerta trasera para monitorizar la actividad. Eso lo puedes hacer con el software de Tor o con otro. Hay información reciente de que el estado alemán ha utilizado software con puerta trasera que ha permitido que... además, el software enviaba información a Estados Unidos, lo cual complica aún más la cosa, a nivel legal, el frameware que es internet, tú te acoges a las leyes del lugar donde se encuentre esa máquina físicamente. Si tú estás generando información con un equipo que está en Boston, se aplican las leyes del estado de Massachuset. Y si en Massachuset se aplica que se puede utilizar información privada para hacer minería y hacer perfilados... cosas que están haciendo grandes corporaciones como Google, Facebook y demás, pues ahí no puedes hacer nada. Son batallas perdidas que desde la Unión Europea se está diciendo: "esto, desde el punto de vista legislativo europeo, no se están cumpliendo unos requisitos de privacidad". Pero aplica la ley del estado en cuestión. Esto aumenta aún más la complejidad.

P- ¿Qué protocolos de seguridad debería activar yo para acceder a la deep web? Dicen que si entras a la deep web una vez ya sales perturbado de por vida.

R- Hombre claro que no. Depende del sitio que tu quieras visitar, pro vamos, que en internet hay multitud de cosas que no están en la deep web y son perturbadores. Fotos de crímenes terribles que habían sucedido, personas con la cabeza cortada...

P- ¿Y la pornografía infantil? Eso no se encuentra en el internet normal.

Con los buscadores no, porque ellos se cuidan mucho. Yo creo que en cuanto hay algo visible ellos lo eliminan de sus buscadores. De todas formas los robots son capaces de detectar cierto contenido e incluso apartarlo de manera automática, aunque a veces se cuela contenido que no es. Basta con que busques en Google Imágenes, en la sección de imágenes intentan no poner pornografía, pero siempre se cuela algo. Pero con el tema de la pornografía infantil es mucho más delicado, y yo la información que tengo es que es una preocupación muy fuerte desde el punto de vista de las fuerzas de seguridad del estado. También la violencia machista, se está muy pendiente, y hay unos protocolos que se activan inmediatamente. En temas de pedofilia igual. Yo tengo amigos que son administradores de sistemas y tienen que bregar con este tipo de cosas. Ofrecen servicios a terceras partes y estas terceras partes no tienen por qué ser de confianza, y utilizan su infraestructura para hacer actividades ilegales.

P- Claro, pero el tema es que la mayor parte de la pornografía infantil se encuentra a través de la deep web, y ya no sólo este tipo de pornografía, sino venta de menores como esclavos y ese tipo de cosas. Lo que me pregunto es si estas personas -no sé como llamar a las personas que se mueven a través de la deep web, ¿son hackers también?- que cuelgan este tipo de contenidos son criminales.

R- No, hombre, no. Un hacker no...la definición que yo tengo de hacker es una definición... que comparten pues otras actividades de relevancia dentro del mundo de las tecnologías. La definición que yo tengo de hacker es aquel que tiene interés por conocer cómo funcionan las cosas a nivel tecnológico. Entonces, por conocer... llegar a la raíz de cómo funcionan las cosas. Luego dentro de la vertiente del hacker generalmente se habla de dos tipos de hackes: el black hat y el white hat, "el sombrero negro" y "el sombrero blanco". Y estamos hablando de hackers desde el punto de vista de la seguridad. A mí la definición de hacker que me gusta es la de aquella persona que tiene un interés de llegar a los conocimientos tecnológicos.

P- ¿Y qué diferencias hay entre los dos tipos de hackers que mencionas?

R- Pues el hacker del sombrero blanco es un hacker que generalmente trabaja al servicio de otras partes... y el hacker del sombrero negro es el que trabaja en actividades delictivas.

P- El hacker de sombrero blanco es entonces, por ejemplo, aquel que ayuda con su trabajo a la policía.

R- Puede, pero también simplemente divulgando problemas de seguridad, estudiando softwares... descubrir el problema de seguridad. Y decir "aquí hay un problema de seguridad, lo he descubierto yo, y al resto de la comunidad pues quiero hacer ver que está este problema. Y luego a lo mejor pues trabaja como consultor a sueldo. Y el del sombrero negro pues es un tipo que está orientado a las actividades delictivas. Dentro también de estas definiciones, el término hacker siempre acaba predominando con el sentido negativo. También se ha hablado mucho del término cracker, que es el que se intenta asignar a alquien que se relaciona con actividades delictivas, lo que pasa es que en prensa es un término que no termina de calar, el que cala es el término hacker, lo que pasa es que el término hacker tiene unas connotaciones asociadas negativas.

P- Volviendo a lo que hablábamos sobre pornografía infantil y todo este tipo de actividades. Los llamados hackers de sombrero negro realizan...

R- No creo que tengan que ser hackers, los hackers son aquellos que tienen conocimientos técnicos, pero cualquier persona puede subir imágenes y no tener los conocimientos técnicos para utilizar esa infraestructura.

P- Bueno, pero también hay quien usa los portales web a través de la deep web para generar dinero. Por ejemplo hay portales de venta de menores que son exclusivamente para ganar dinero a través de los bitcoins. Los portales se dedican a generar beneficios mediante el uso de esta moneda. Había un portal, que ya lo cerraron, que era SilkRoad, el portal más grande de venta de droga del mundo; y Agora, el mercado por excelencia de venta de armas, entre otros muchos. O sea, que en realidad no son sólo hackers, sino organizaciones criminales. ¿Es imposible neutralizar a estas organizaciones? ¿No puede hacer nada la policía?

R- Sí, son organizaciones criminales. Al chaval este que estaba detrás de SilkRoad, o al menos a uno de ellos, que es norteamericano, lo han pillado.

P- ¿Cómo se organiza una investigación así? ¿Qué mecanismos se emplean para romper sus defensas?

R- Pues con muchos recursos y mucha dedicación, igual que para investigar cualquier tipo de delito informático... muchos recursos para seguir la pista a quien está cometiendo este tipo de delitos.

P- Sí, ¿pero cómo se sigue la pista?

R- Simplemente que se equivoque y envíe información de lo que está haciendo a través de un correo convencional y ya están encima de él. Que cometa algún tipo de error.

P- Los correos electrónicos también se envían a través de la deep web.

R- No sé si hay infraestructuras de correos en TOR, la verdad.

P- Para acceder a la deep web, ¿qué infraestructura técnica necesitaría?

R- Para acceder a la red TOR te basta simplemente con un ordenador e instalarte un cliente de TOR. Puedes probar y... ya está.

P- ¿No necesito utilizar un antivirus muy potente? Yo uso Avast gratuito.

R- No, lo que puedes hacer es, justo cuando hayas acabado de informarte pues reinstalar el sistema operativo completamente, si quieres alcanzar el nivel de paranoia máximo y reinstalar todas las aplicaciones desde cero y destruir todo el software que tengas instalado, si te quieres asegurar. Lo mejor que puedes hacer es entrar y sacar toda esta información de primera mano.

P- Voy a hacer un par de preguntas más. ¿Qué es el cypherpunk?

R- Bueno, son simplemente activistas que opinan que la información debe garantizar la privacidad. Gente que considera que la privacidad es fundamental y que hay que garantizarla con los medios tecnológicos. Los niveles de criptografía que se emplean hoy día en internet eran ilegales hace quince años en los Estados Unidos. Las leyes estadounidenses tenían unas rectricciones muy fuertes con respecto a los niveles de seguridad que se podían utilizar con criptografía, y luego también las restricciones desde el punto de vista de exportación de tecnología criptográfica, y las siguen teniendo. Son muchas cosas.

P- Esto enlaza con otra duda. ¿Estamos viviendo una especie de nuevo orden mundial o de guerra virtual a través de los servidores? Siempre que veo que cosas de ciberataques, de Anonymous, el Estado Islámico, los Rusos, los Chinos... me parece sacado de la Guerra de las Galaxias.

R- (Se ríe). Tu piensa que la infraestructura básica de un país cada vez se sustenta más en los pilares de la información. A todos los niveles. Tu piensa que la logística de muchas empresas, o la Administración Pública, depende completamente de la infraestructura de la red hoy día. Y que incluso hay experimentos, por ejemplo aquí en la Universidad, para desarrollar la telefonía IP. O sea que tanto los servicios de datos, de voz, de televisión... convergen hacia internet. De televisión, de streaming... de todo. En este escenario... Esto no ha pasado todavía pero es cuestión de tiempo, tu piensa que tocando la infraestructura básica de un Estado podrías paralizar la actividad de éste durante días, con las consiguientes consecuencias y problemas que eso puede ocasionar ¿no?

P- Sí, ya imagino... si un sólo día de huelga general bloquea completamente la producción de un Estado...

R- Y pensémoslo a menor escala. Bloquea los sistemas logísticos de distribución de un supermercado, o de correos... Si es navidad y la gente protesta porque llegan los paquetes con

retraso, pues imagínate. La tendencia es... hacia que esta infraestructura crítica de base, que está ahí expuesta, y...

P- Con este panorama que me planteas cualquiera podría paralizar un país con conocimientos tecnicos y mucho tiempo.

R- Hombre, hace falta más que eso. Conocimientos, equipamientos, recursos... Claro que sí. Dependiendo de como se construya esa infraestructura, y si no han considerado unos requisitos de seguridad están mucho más expuestos. Esto obviamente tiene que derivar en una toma de conciencia de que se está gestionando muchas cantidades de información y ya no hay una persona al otro lado esperando a que llamen de un número de teléfono para apuntar en un papel lo que la otra persona le pide. Los tiempos han cambiado y ahora la infraestructura es crítica, igual que la infraestructura de los aeropuertos es crítica o la portuaria, o de carretera... que son infraestructuras físicas, y que de lo físico sí hay una conciencia de definir bien los perímetros y de poner los medios para protegerlo. En lo virtual eso está tardando más en llegar, pero va a ser cuestión de tiempo. Va a ser más evidente, en el momento en que haya una parálisis de internet, que no sea propiciada por un Estado. Porque tu piensa que China tiene un cortafuegos enorme para filtrar y monitorizar la actividad de sus ciudadanos, y que por ejemplo, estados como el de Turquía, que está solicitando la entrada a la Unión Europea, con la cantidad de problemas que ha habido como lo del 'Getnick' y ese tipo de cosas, bloqueó el acceso a Twitter y a Facebook, para desmantelar a nivel organizativo...

P- A través de la deep web, de los contenidos cifrados de internet, ¿se podría pasar cortafuegos gigantes como los de China?

R- Claro, ese es uno de los grandes objetivos. TOR nace como una red para garantizar el anonimato, eso tiene unas connotaciones de libertad muy fuertes. ¿Qué sucede?, que en este tipo de cosas se auspicia un espacio de libertad absoluto y se auspicia todo tipo de cosas. El anonimato garantiza una serie de aspectos relacionados con los derechos humanos y con la libertad, que son fundamentales, pero también recoge otro tipo de actividades que no nos gustan tanto. Pero esas actividades no son un reflejo de la tecnología, son un reflejo de la sociedad en la que vivimos. Y eso sucede porque esta sociedad permite este tipo de cosas.

P- Y además las apoya, como con la creación del Bitcoin. Una moneda no se eleva sobre el dólar en el mercado de divisas internacional si no es por su revalorización.

R- Bueno, el aumento del valor del bitcoin no creo que tenga que ver sólo con la criminalidad. El aspecto especulativo del bitcoin tiene que ver con la naturaleza especulativa de la economía. La economía de por sí es especulativa. ¿Qué sucede?, que el bitcoin no tiene una autoridad central que regule el valor de esa moneda, por lo que los ataques especulativos se vuelven más fuertes. Pero ha habido ya ataques especulativos. En Europa hubo uno contra la libra orquestada por una gran corporación, pero el banco central británico no fue capaz de luchar con ella. La economía tiene un carácter especulativo por sí sólo. Los bitcoins más todavía. Es un espacio completamente desregulado, y no creo que el valor especulativo de los bitcoins esté asociado a la criminalidad. Yo creo que está asociado también a que hay personas poniendo dinero ahí porque a nivel especulativo es rentable. El valor del bitcoin era X y en tres años se ha disparado. El que tuviera su dinero invertido en bitcoins ha pegado un pelotazo. Ahí también hay un interés por parte de inversionistas. Esto es oferta y demanda. Si todos quieren comprar bitcoins, pues su precio se dispara. El cambio de una moneda, de euro a dólar, viene controlado por una autoridad central que emite más o emite menos. En el caso del bitcoin, la emisión es continuada por parte de toda la infraestructura de mainer que hay.

P- ¿Mainer?

R- Sí, hay softwares que generan monedas.

P- Ok, apunto el término.

R- Es fácil llegar a esta conclusión: TOR es igual a deep web y deep web es igual a criminalidad, ¿no?, Bitcoin es especulativo y especulativo es igual a criminalidad. Los ataques especulativos los hay también... Nosotros estamos sufriendo una crisis especulativa muy fuerte por el tema inmobiliario, ¿y qué es lo malo? ¿la vivienda de por sí es mala o es el euro el malo?

P- El mal uso, digo yo.

R- Es obvio que si alguien entra en la deep web ya se está visibilizando. Por ponerte un caso, mira, tú has visto que en los navegadores web, en cualquiera de ellos ya hay una manera de abrir una pestaña de navegación privada, de incógnito. ¿Sabes cómo funciona esa tecnología?

P- Pulsando CTRL + Shift + N, ¿verdad?

R- Vale... a nivel de usuario, aprobado. Ahora, por debajo de eso, lo que está haciendo es que envía información al servidor, hay un campo en el mensaje que envía al servidor diciendole: "quiero privacidad", y el servidor, de acuerdo con su política va a aceptar eso. Y le estás publicando también a tu proveedor de servicios que quieres privacidad. Si la gente que pulsa la pestaña de privacidad lo hace para esconderse porque está haciendo una actividad delictiva, ese mensaje aparece como "quiero privacidad". Obviamente, dentro del motor de big data que circula por el canuto de internet, se está visibilizando como alguien que quiere estar conectado de manera anónima, y le está diciendo al resto de la humanidad o a quien monitoriza esa infraestructura: "oye, quiero privacidad" y tú vas a decir: "por qué".

P- No entiendo cómo puede intuir quien monitoriza esa infraestructura que tu demanda de anonimato vaya a ser fraudulenta.

R- Bueno, tú tienes una actitud de querer privacidad. Tu tienes infraestructura, como con todo el tema de Snowden, se ha comprobado algo que se lleva sopesando mucho tiempo. Hay una infraestructura que está permitiendo clasificar información y desviarla al sistema que la analiza. Tu piensa que esto es un canal por el que circula información de todo tipo, y aquí, en el montón de paja, tú lo que quieres es hilar fino, quieres encontrar las agujitas. Cuando tú navegas por internet y estás usando TOR o la pestaña de privacidad, o estás utilizando criptografía para tu mensajería personal. Ya casi todos los servicios web te permiten navegar en SSL -¿sabes lo qué es SSL?-, donde la información va cifrada entre el cliente y el servidor. Tu piensa que dentro de ese gran canuto de información hay gente que se está visibilizando, está levantando la manita dentro de la red.

P- No sé que estás haciendo con TOR, pero veo que lo estás usando.

R- Eso es. ¿A ti te importa la privacidad?

P- Hombre, pues claro.

R- ¿Sí? ¿Tienes un correo de Gmail?

P- Sí.

R- Pues entonces no te importa la privacidad. Porque Gmail tiene robots que están analizando todo el tráfico que se genera, porque es el negocio de Google, venden la información que todos generamos.

P- ¿Entonces Google lee mis correos?

R- Quizá no una persona físicamente, pero sí que lo hacen sus robots, que clasifican la información.

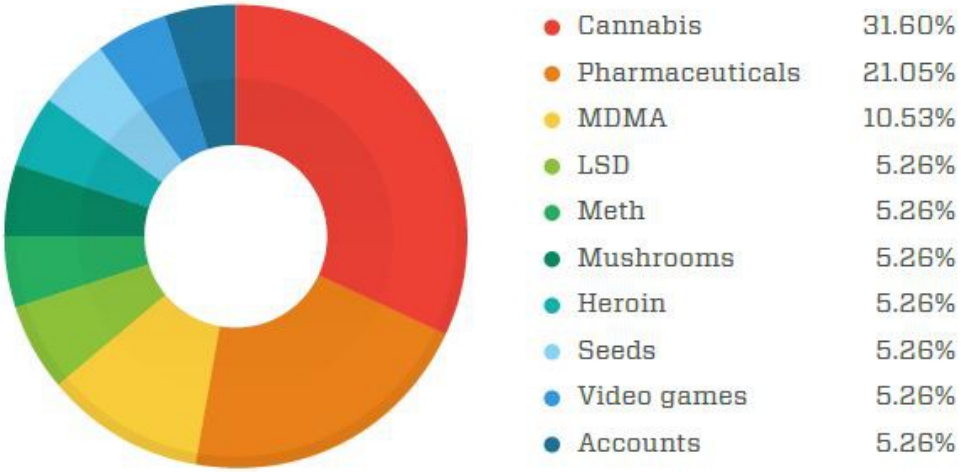
P- Si escribo la palabra "bomba" va a la carpeta de posibles.

R- Sí, pero ya no solo relacionado con actividades delictivas, si no para la una estructura puramente comercial que quiera ofrecerte sus productos. Saben que eres joven, que tienes una franja de edad, que te interesa el periodismo, que te interesa la deep web... Desde el momento en que tu le preguntas a alguien que si quiere privacidad, todo el mundo te dice que sí, pero luego en realidad, cuando entras a internet con este tipo de servicios no la estás teniendo.

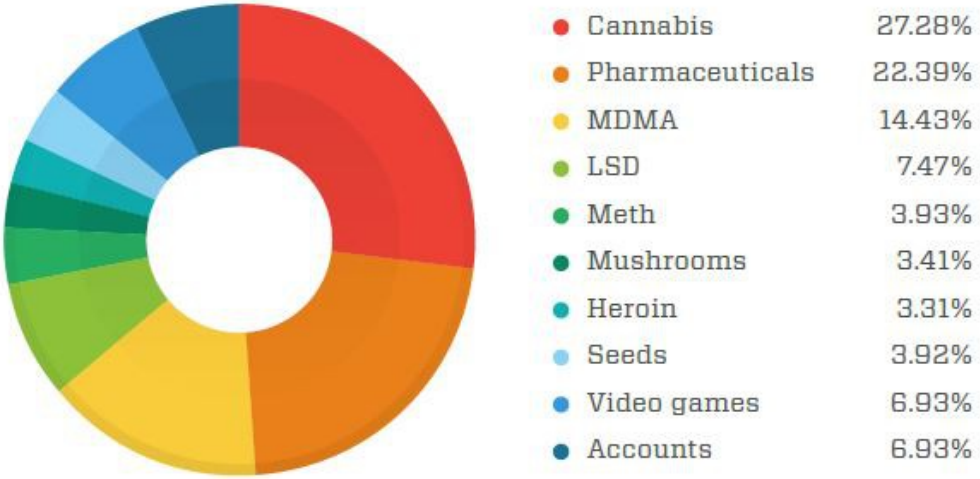
P- Pero supongo que mis datos estarán protegidos por la Ley de Protección de Datos

R- Claro, están protegidos por las leyes de California, que es donde está instalado Gmail. Aplican las leyes de donde está el servidor desde el que te conectas.

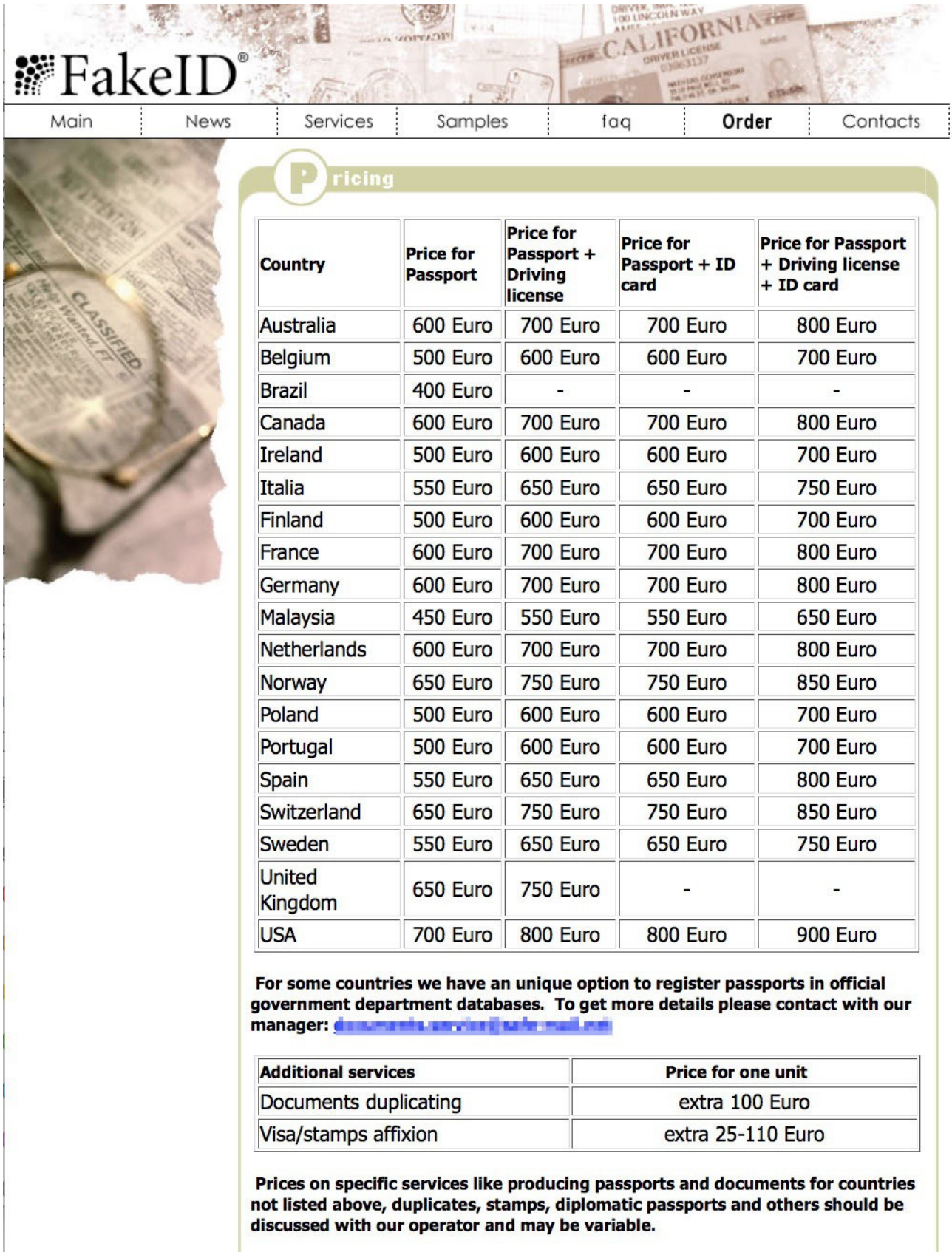
ANEXO 3: IMÁGENES



1. Principales productos ofrecidos por los vendedores a través de la deep web



2. Principales productos demandados por los compradores a través de la deep web



FakeID®

Main | News | Services | Samples | faq | **Order** | Contacts

Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

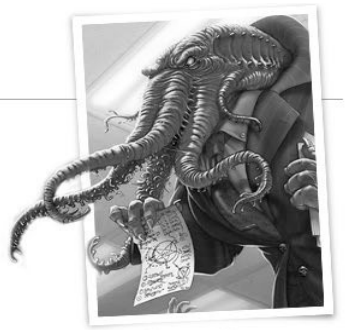
For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager: [redacted]

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.

3. Lista de precios en un portal de la deep web para obtener pasaportes falsos

C'thulhu



Email: [redacted]Lq4dYTtAxW7U@bitmessage.ch

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail).

So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. And know, we are only one, real contractor there. Any other will try cheat you. ← Contract Killer © 2011.

☞ *No fish too big, no job too small - HITMAN does it all!*

Q & A!

Can I see some proofs of your last work?

Every contract is Private, and all data is Purged after elimination proof is sent to the customer. It is Mandatory for Customer's and our Security!

Can You give me contact to person who already used your services?

Again, Every contract is Private! Without Exceptions! And we will never store or share such info after completing.

Can you give to me a good feedback about, you and some proofs of succeeded work?

Sorry, but no one of our happy customers stay on forums, or have time to post feedback on some trusted site. All feedbacks is written directly to our mail, and it will not show you any proof if we'll post it on our own page. And even if you'll find an feedback on an page, it was write by an random person, who don't have with as any business.

How I would can to know that you are not a scammer as else?

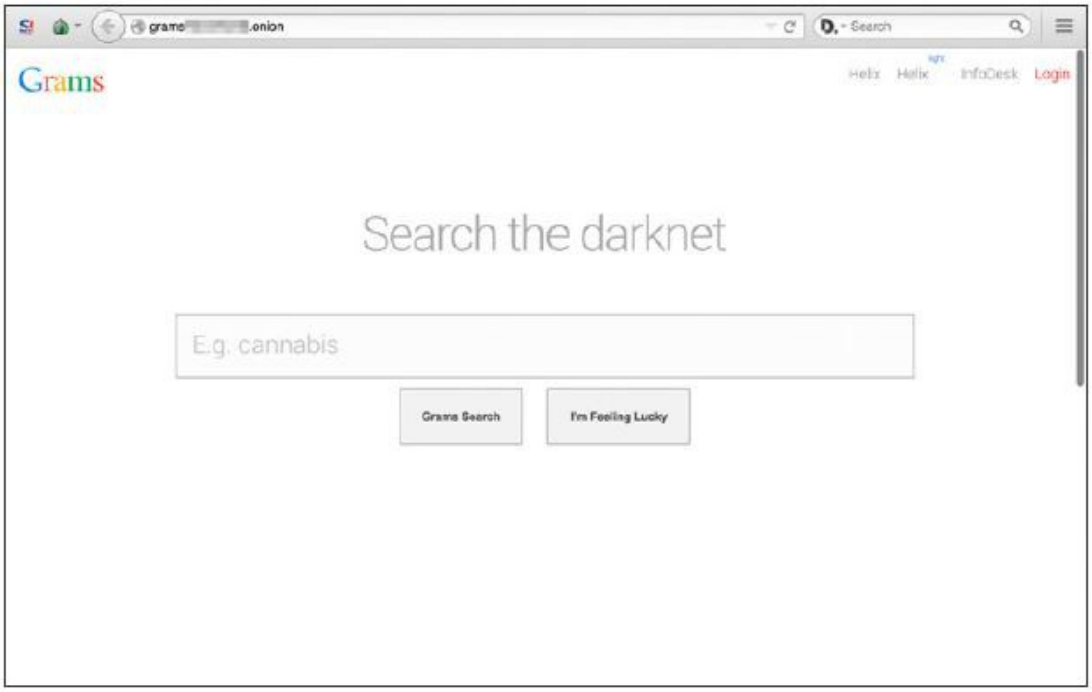
Simply, we don't take any prepayments. We are only who ask just for proof that you have this money in your wallet, and you'll to arrange full escrow on trusted for both third party site.

Ask more, we'll add more.

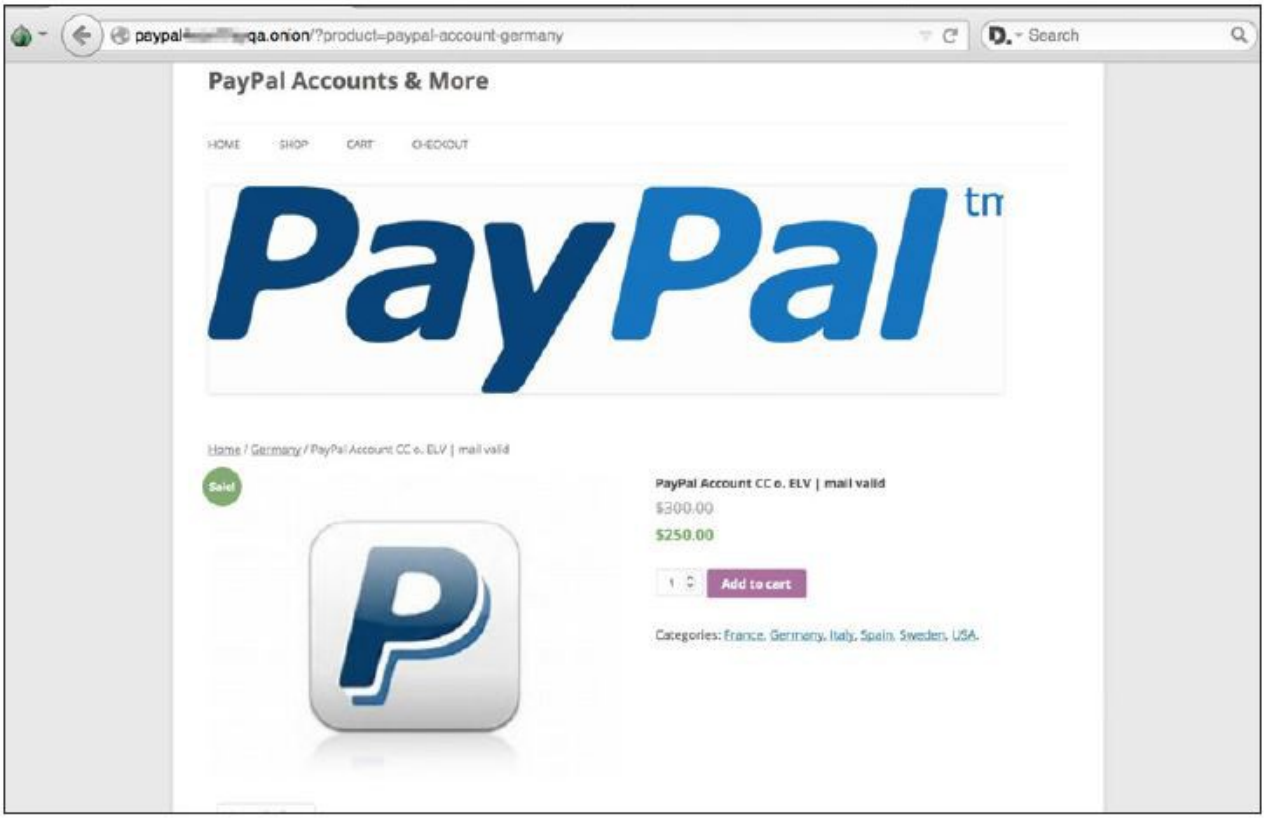
We should probably get started if you'll have at least this:

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	$45,000	$90,000	$180,000
Missing in action	$60,000	$120,000	$240,000
Death in accident	$75,000	$150,000	$300,000
Criple Types	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$12,000	$24,000	$48,000
Uglify	$18,000	$36,000	$72,000
Two Hands	$24,000	$48,000	$96,000
Paralyse	$30,000	$60,000	$120,000
Rape	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$7,000	$14,000	$28,000
Under age	$21,000	$42,000	$84,000
Bombing	**Low Rank**	**Medium Rank**	**High Rank and Political**
Simple	$5,000	$10,000	$20,000
Complex	$10,000	$20,000	$40,000
Beating	**Low Rank**	**Medium Rank**	**High Rank and Political**
Simple	$3,000	$9,000	$18,000

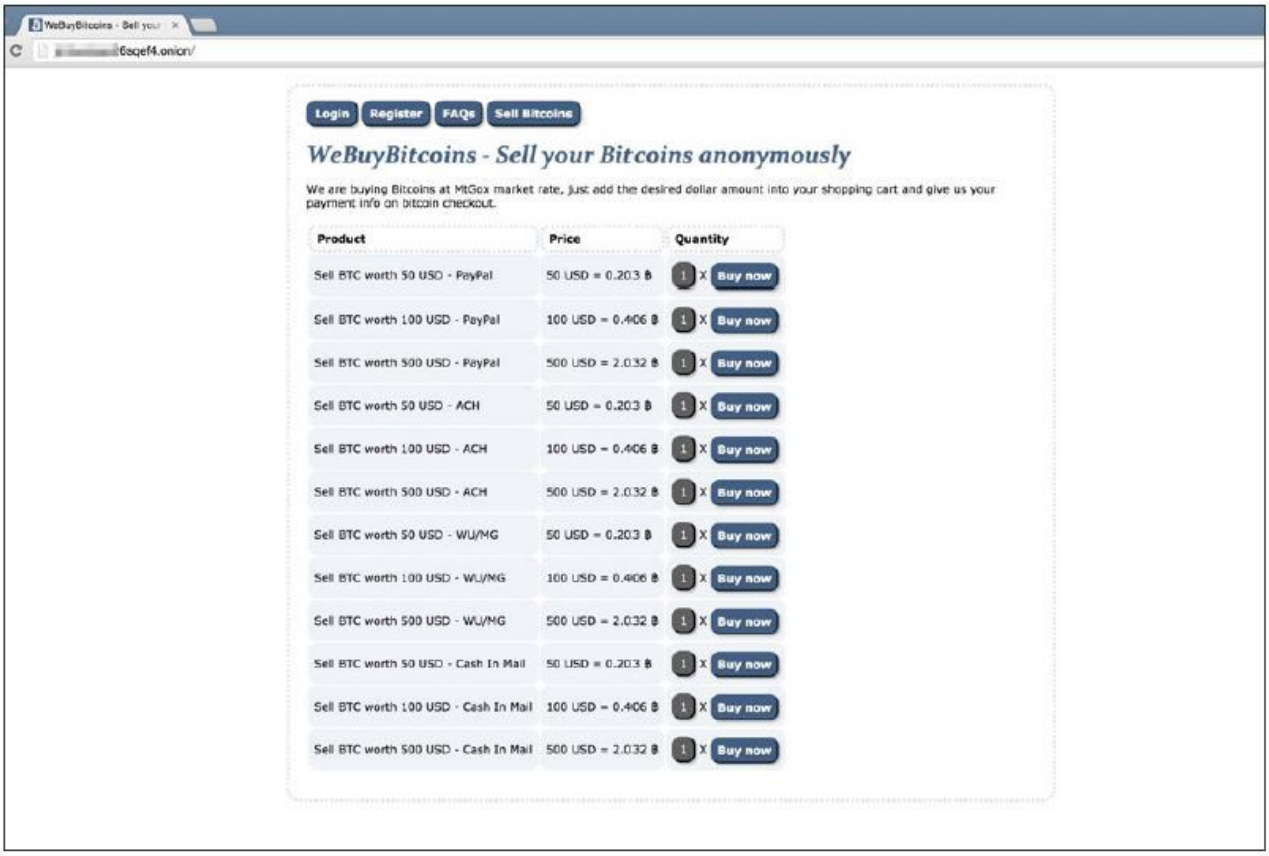
4. Distintos precios para contratar servicios de matones y sicarios en la deep web



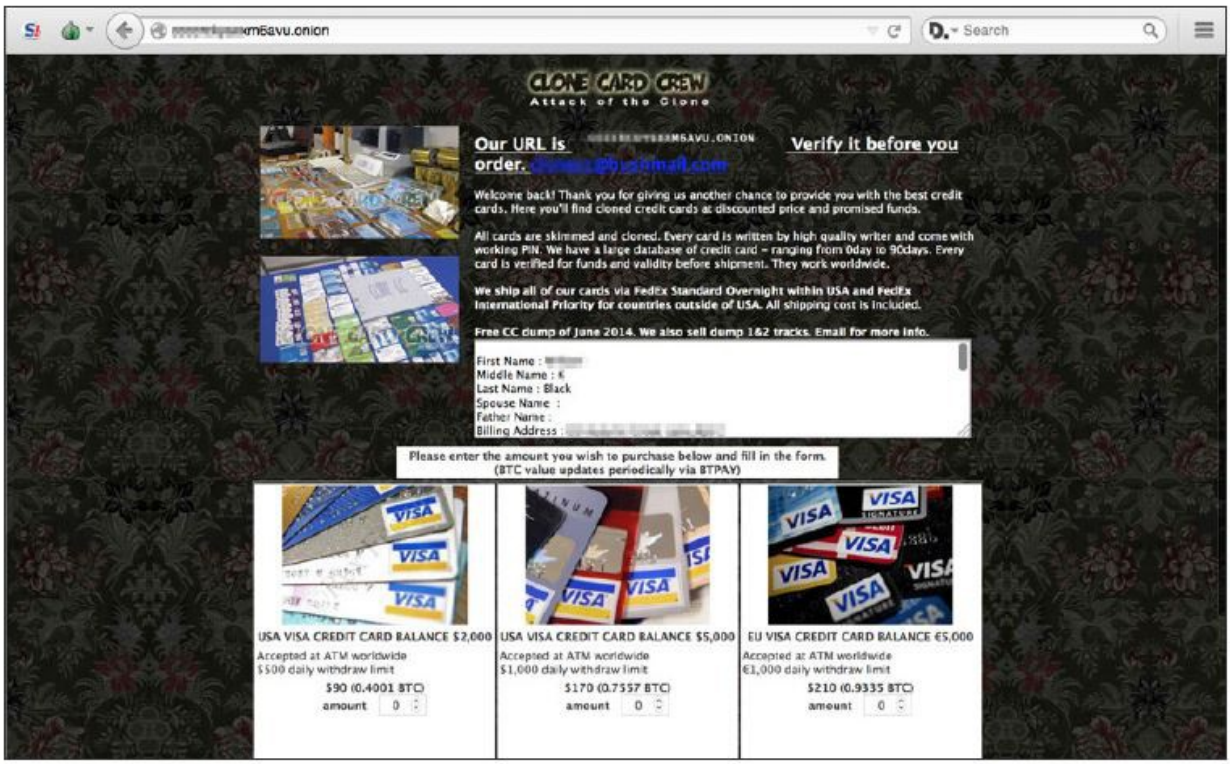
5. Uno de los buscadores de drogas más populares en la deep web



6. Un portal para comprar una cuenta validada de PayPal con saldo positivo



7. Portal de intercambio de divisas. Cambian los bitcoins por dólares



8. Página que ofrece tarjetas de crédito clonadas en la deep web