Nociones básicas del nuevo delito de phishing en el Derecho Español

Pedro Jesús Macías Torres

Muchas veces se ha afirmado y nunca con falta de razón que las tecnologías muestran una doble cara; una de ellas que permite una calidad de vida mejor, más llevadera, rápida y sencilla y otra, no tan positiva contra la que debemos repeler sus consecuencias. El ser humano tradicionalmente se ha decantado en no pocas ocasiones por determinadas conductas al margen de lo que la sociedad, sobre todo el Derecho consideran licitud. Para el mundo de los penalistas, mucho se ha tenido que esperar para que el ordenamiento jurídico español tipificara lo que es delito de phishing, rellenando las lagunas que siempre existen ante un avance inconmensurable de los instrumentos que la técnica innova.

Recordando lo que en esencia es la estafa, nuestros profesores nos mostraban una realidad formada por cuatro actos escalonados para que el delito como tal llegara a consumirse y ser objeto de reproche por ley: el engaño, el error, la disposición patrimonial y el perjuicio a favor de un tercero y con el que la finalidad defraudatoria se había logrado. Pero con el phishing, ¿ocurre lo mismo?, ¿qué hay de común y de novedoso respecto de la estafa?

En esencia y ajustándonos a lo que constituye la cotidianidad muchos días hemos recibido e-mails con ofertas de trabajo bastante suculentas por las que a través de una labor efectuada desde casa y sin excesivas complicaciones, percibiríamos unos emolumentos difíciles de obtener, aun desempeñando un trabajo que requiera horas de esfuerzo, sacrificio, buena preparación y una considerable responsabilidad. En resumidas palabras, el phishing es una nueva modalidad de comisión delictiva por la que empleando las nuevas tecnologías, el verdadero defraudador quiere un beneficio económico; casi siempre una gran cantidad de dinero. El Código Penal español en su artículo 248.2 afirma que además de lo que viene siendo la estafa tradicional, también se consideran reos de la misma: “Los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro”. Es fácil deducir tras la lectura de este párrafo que el bien jurídico protegido es precisamente el patrimonio en sí. Las actuaciones de defraudadores que emplean herramientas cada vez más pulidas y que generan una credibilidad difícil de superar tienen su freno en el Código Penal a raíz de la modificación sufrida por la Ley Orgánica 5/2010, de 22 de Junio, reformándose de nuevo en 2015, por la Ley Orgánica 1/2015, de 30 de Marzo. Existen diversas variantes defraudatorias con peculiaridades que las diferencian del resto y todas con una terminología anglosajona; pongamos por ejemplo: el denominado whaling. Para diferenciarlo de lo que es el phishing, debemos atenernos a la víctima que lo padece. Con el primero el usuario de una entidad bancaria recibe un correo electrónico pensando que procede del banco donde tiene ingresado todo o parte de su dinero. El defraudador solicita unas claves a la víctima de estafa informática y ésta se los manda por medio de un archivo adjunto HTML enviado previamente por la supuesta entidad bancaria; de esta manera resulta más difícil si cabe el realizar un rastreo por parte de la policía al inicio de las investigaciones que se efectuasen. Con el whaling el grupo de víctimas tiene un carácter reduccionista, circunscribiéndose a los empleados o trabajadores del mundo de las finanzas incorporados a grandes empresas.

Con la estafa informática, modalidad phishing (o pesca de incautos), el defraudador recibirá esas claves necesarias para la extracción involuntaria o inconsentida de su titular. La cuestión se complica aún más; aparentemente el esquema conceptual no reviste dificultad alguna pero hay que saber que el autor material del delito no trabaja sólo, sino que junto a él intervienen

unos cooperadores que nuestro modo de ver son cooperadores necesarios para la comisión del delito, por tanto, el elemento doloso se encuentra presente, a menos que quepa desconocimiento por parte de estos cooperadores o intermediarios que reciben de manera popular y en lenguaje policiaco el nombre de “muleros” o “muleros bancarios”.

El verdadero defraudador, cabeza intelectual de la trama encarga al mulero que se ponga en contacto con las víctimas a fin de obtener dichas claves que sólo el titular de la cuenta puede y debe saber. Cuando la víctima de phishing proporciona inocentemente lo solicitado a quien se lo envía es al propio cooperador (que cobrará un porcentaje de lo acordado) y esta cantidad defraudada emprenderá un segundo viaje que por regla general va dirigida al extranjero, lugar donde se sitúa el defraudador autentico y que no tiene por qué mantener relación alguna con la víctima, a la que ya se ha desposeído de su patrimonio. Es obvio afirmar que la intervención de estos muleros son elementos esenciales para que el delito de phishing se efectué y además que se haga sin levantar ningún tipo de sospechas. No sólo debemos saber que la técnica empleada a través de los ordenadores es esencial para que el delito vaya “edificándose”; también la existencia de una cuenta corriente en el extranjero con la que cobrar las cantidades trasladadas en el menor tiempo posible nos puede dar una ligera idea de la rapidez con la que estos sujetos activos se emplean a fondo; la construcción de una web simulando a modo de ejemplo una entidad bancaria dista y mucho de los primeros intentos que allá por lo años noventa del pasado siglo se realizaban y por ello supone una dedicación de cara a generar una confianza en la que será la próxima víctima.

De cara a intervenciones por parte de la policía, resulta más difícil detectar al cooperador necesario, al mulero como tal que generalmente residirá en el mismo país que el sujeto pasivo, coincidan o no las poblaciones en las que habiten. Frente a un juicio de competencia, diversos pronunciamientos judiciales muy recientes colocan el lugar de residencia y actuación del mulero como el idóneo para que el juzgado correspondiente conozca del caso para su instrucción y parece viable que así fuera, pues si hablamos de un “circuito bancario”, expresión acertada a mi modo de ver por parte de los penalistas, este cooperador o intermediario evitará con su actuación la no reversión de ese dinero, es decir, un patrimonio económico considerable que probablemente nunca recuperará. La víctima tiene como opción preferente comunicarlo al banco del que es cliente y en virtud de nuestra Ley de Servicios de Pago, la entidad financiera debería devolver esas cantidades sustraídas sin su beneplácito pero para ello es conveniente la comunicación con el banco con inmediatez absoluta y la ausencia de un ánimo fraudulento con la empresa; el mismo mínimo fraudulento que el estafador y el mulero (no en todas las ocasiones) han tenido para elaborar esta modalidad delictiva. Regresando a las primeras líneas de este trabajo, hemos mencionado que la estafa se caracteriza por un engaño, posteriormente un error más tarde la entrega o disposición patrimonial y el perjuicio ocasionado a la víctima. Si éste no existe, no debemos hablar de un delito de estafa. Con la estafa informática los dos primeros elementos, es decir: engaño y error no suelen estar igual de definidos que la estafa tradicional recogida en el artículo 248.1 del Código Penal español. La intervención de las computadoras, les da un aire de autonomía, más que nada por el contenido del programa que incorporan éstas. Si el programa confeccionado se hace para defraudar, en mi opinión, sí cabe la existencia de una “colaboración de la víctima” en el mismo instante en el que en la mente del usuario de las claves se forja una realidad no ajustada a lo que es y accede por tanto al fraude. Si una falsa web de un banco solicita las claves que el cliente pudiera tener, al programa informático no se le puede exigir una concreta responsabilidad penal. Es el defraudador el que con mala fe elabora el programa para que la potencial víctima descargue el archivo adjunto e introduzca los datos requeridos.

El último de los aspectos que deseo destacar dentro de lo que es una explicación sucinta de esta nueva vertiente de delitos contra el patrimonio se encuentra en lo que se conoce como "ignorancia deliberada", un tanto criticada por la doctrina del Tribunal Supremo, pero que la mayor parte de nuestras Audiencias Provinciales la han apoyado. Consiste básicamente en la calificación de partícipe con existencia de dolo al tener constancia de que la actuación desempeñada sea algo ilícito, por parte del mulero. Para los jueces no es necesario el conocimiento exhaustivo de toda la operativa: cuando empieza, cuando se pretende concluir, identidad del defraudador, motivos que conducen a una actividad defraudatoria, etc. No es necesario a mi modo de ver que el mulero posea una basta formación académica; puede deducirse sencillamente que emitir una solicitud de trabajo con grandes contraprestaciones para integrarlos en una cuenta corriente que después pasa a otra del extranjero no forma parte de lo cotidiano. En palabras del Tribunal Supremo, los muleros "tienen un conocimiento necesario para prestar su colaboración y la ignorancia del resto del operativo no borra, ni disminuye su culpabilidad porque fueron conscientes de la antijuricidad de su conducta". Algunos casos en España en los que el recurso de apelación del mulero ha sido completamente desestimado y consideran que de manera efectiva había un dolo necesario y como consecuencia debería aplicarse el artículo 248.2 del Código Penal. En definitiva y cerrando este tema, el mulero siempre responderá cuando tenga conocimiento de los resultados que pudieran preverse y que su conducta conformara un hecho delictivo.

Si tuviéramos que hacer un comentario como conclusión en un supuesto de este tipo (delito de phishing) deberíamos decir que en puridad, todos son perjudicados: en primer lugar la propia víctima como el perjuicio que se le causa, ha confiado ella en la credibilidad que la web falsa expone en su pantalla y con su buena fe envía esas claves numéricas (o alfanuméricas), creyendo que el banco los necesita por ejemplo para el envío de promociones nuevas de productos con determinada rentabilidad, pero salen perdiendo también autores y participes interviniente en lo que a la tecnología se refiere. Como recomendación máxima se aconseja el cierre de todas las aplicaciones antes de acceder a la web del banco, escribir la URL en el navegador prescindiendo de cualquier tipo de enlace que se ofrezcan, cerciorarse que la web comienza por http://, de esta manera los datos que circulan por Internet estarán dotados de mayor seguridad, pues van cifrados y no acceder a los servicios de banca on line a través de ordenadores públicos. Si no se siguen estos pasos, muy difícil será atajar una lacra como la que este trabajo exponemos.

Pedro Jesús Macías Torres Sevilla – Diciembre 2016