EL PREOCUPANTE INCREMENTO DE LAS CIBERESTAFAS

Daniel González Uriel

En los últimos tiempos estamos asistiendo a un notable incremento de la problemática relacionada con las ciberestafas o, por lo menos, eso es lo que se desprende del aumento de reportes, en los medios de comunicación, de casos de estafas *online* que afectan a una pluralidad de víctimas. Como ejemplo podemos mencionar la reciente publicación del periodista Luis Rendueles[1], en la que elabora una síntesis de esta situación, anotando algunas de las modalidades de ciberfraudes que se han producido recientemente. Cabe destacar que en dicho artículo se apunta una cifra que revela la importancia del fenómeno analizado: estas formas de ciberdelincuencia han crecido un 136% en los últimos cuatro años, 25 personas denuncian cada hora en España que han sido víctimas de tales conductas y en el año 2019 el número de denunciantes por ciberfraudes en nuestro país ascendió a 216000 afectados.

A su vez, en esa misma publicación se recoge que los datos correspondientes al año 2020 no serían extrapolables ni evidenciarían una tendencia, ante la situación de pandemia y consiguiente confinamiento domiciliario. No obstante, hemos de apostillar que, precisamente por la situación de confinamiento, con un prolongado encierro domiciliario en el que el acceso a Internet se convirtió en el medio de comunicación usual entre las personas, y durante el cual se incrementaron las horas de conexión de los internautas, es fácil inferir que se creó un terreno fértil para un mayor número de ciberfraudes: la demanda de bienes y servicios se canalizó, en gran medida, a través de la Red, lo que abrió la puerta a que se produjese una proliferación exponencial de los cibercrímenes, con una pluralidad de operativas diversas.

Evidentemente, somos conscientes de que las Tecnologías de la Información y de la Comunicación (TIC) han cambiado los hábitos sociales, han generado nuevos sistemas de interconexión y han facilitado la transmisión de contenidos, lo que conlleva una modificación sustancial de las formas de relación interpersonal, con empresas y con instituciones y administraciones públicas. Ello también se ha trasladado al ámbito del consumo, a la posibilidad de adquirir bienes y servicios a golpe de click. En este sentido, las TIC han permitido la inmediatez en las comunicaciones: ya no es indispensable aguardar largas colas en nuestras sucursales bancarias para realizar gestiones financieras, ya que disponemos de la banca *online* en el smartphone a través de una aplicación. Es posible realizar la declaración de la renta a través de la página web de la Agencia Tributaria, se puede pedir la cita para la vacuna del COVID a través de la aplicación móvil de la correspondiente consejería de sanidad autonómica o, por poner un último ejemplo, es posible darse de alta en el Servicio Público de Empleo Estatal (SEPE) a través de su sede electrónica. Como puede apreciarse, los ciudadanos hemos ganado en tiempo, en comodidad y en inmediatez mediante semejantes posibilidades. Sin embargo, y como contrapunto, hemos de ser conscientes que en la Red –y a través de ella– existe una

[1] Artículo titulado: "Estafas en red y en el móvil: 600 víctimas cada día en España", publicado el 28 de septiembre de 2021, disponible en https://www.levante-emv.com/sucesos/2021/09/28/estafas-on-line-victimas-datos-policia-nacional-57793923.html.

multitud de datos personales nuestros. En efecto, tal información ha sido calificada por algunos –y con razón– como el petróleo del siglo XXI, ya que genera pingües beneficios a las entidades que los tratan y comercian con ellos. No obstante, debemos poner de relieve que, desgraciadamente, tal transmisión de datos también puede ser la puerta de acceso de los ciberdelincuentes a nuestros ordenadores y terminales de telecomunicaciones, y que esta información puede ser utilizada en la comisión de ciberdelitos.

No podemos negar que el aumento del empleo de las TIC ha mejorado nuestra calidad de vida. Sin embargo, los delincuentes también se han adaptado y han diversificado las dinámicas comisivas de delitos, adaptándose a las posibilidades que brinda el entorno virtual. En este sentido, algunas de sus notas características, como el anonimato, la inexistencia de fronteras, la globalización, la posibilidad de comunicación inmediata y directa con una pluralidad indeterminada de personas, la ausencia de los oportunos sistemas de autoprotección y el gran desconocimiento de la población, en general, sobre los sistemas informáticos y sus vulnerabilidades, entre otros elementos, favorecen que el espacio cibernético se haya convertido en un terreno fértil para la comisión de delitos que ya existían en el entorno físico –pero que se han adaptado o trasladado a la Red–, o bien, para la comisión de nuevos tipos que tienen su origen y su razón de ser en las propias TIC.

El fenómeno de la ciberdelincuencia ha sido tratado de modo magistral en nuestro país por Miró Llinares, autor de una monografía[2] de obligada referencia en la materia. En ella, dicho autor propone varias clasificaciones de ciberdelitos. En primer término, a propósito de la relación entre el comportamiento criminal y la incidencia en él de las TIC, distingue entre los ciberataques puros –que solo se pueden cometer en el mundo virtual–, los ciberataques réplica –que tienen su fuente originaria en el medio físico, y suponen una adaptación al nuevo entorno– y los ciberataques de contenido, en los que el injusto se basa en la concreta información transmitida. En segundo lugar, propone otra clasificación que atiende al móvil del ciberdelincuente, así como al contexto criminológico, y que le lleva a distinguir entre ciberdelitos económicos, sociales y políticos.

En este caso, si seguimos la atinada explicación del profesor Miró, nos hallaríamos ante ciberataques económicos, que persiguen un beneficio patrimonial de su autor. Si tomamos dicho elemento como punto de partida, a continuación hemos de referir algunas de las particularidades que se siguen en su comisión, y que dan lugar a una pluralidad de afectados. Primero, la obtención de direcciones de correo electrónico y de números de teléfono de una multitud de personas permite que se les remitan comunicaciones a muchos sujetos, tanto por correo electrónico como a través de mensajes SMS, en las que los ciberdelincuentes simulan actuar en el marco de conocidas entidades bancarias, de otras mercantiles o de administraciones públicas. En tales supuestos, dado que se imitan las páginas web oficiales de tales emisores, el sujeto receptor baja la guarda, al considerar que existe un principio de autenticidad y que, en consecuencia, la comunicación remitida es verdadera. Como ejemplos recientes de estas operativas podemos mencionar la estafa

[2] MIRÓ LLINARES, F., *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012.

denunciada por la Unión de Consumidores de Galicia, a finales del mes de septiembre[3], en la que se daba cuenta de la remisión de un SMS a múltiples afectados, en los que el emisor fingía ser la entidad bancaria ABANCA, se alertaba de que la cuenta bancaria del receptor había sido suspendida temporalmente por razones de seguridad, y se remitía un link para su restablecimiento. En la noticia se comentaba que podrían estar afectadas por dicha estafa cerca de 50 personas en Galicia. No solo ello, sino que en desarrollo de esta modalidad defraudatoria también se realizaban llamadas telefónicas[4], desde un teléfono fijo con prefijo de A Coruña, 981, que además se correspondía con una sucursal física real que ABANCA tiene en A Coruña. En estas llamadas una mujer se hacía pasar por trabajadora de la entidad bancaria y, tras recabar los datos personales de las víctimas, y después de otro SMS con un código de activación, se llevaba a cabo la transferencia inconsentida, sin que la víctima fuese consciente de ello. Este *modus operandi* ha afectado a otras entidades financieras en los últimos tiempos, como al BBVA[5], que ha sufrido una operativa similar a la enunciada, mediante el envío de un SMS en que se informaba del bloqueo de la cuenta bancaria por movimientos sospechosos en ella.

En otra estafa reciente de la que dio cuenta la Policía Nacional, la empresa que sirvió de reclamo era MERCADONA[6]. En ella, se recibía un correo electrónico en el que se informaba de que el receptor había sido seleccionado para recibir productos gratuitos de dicha cadena de supermercados. En el cuerpo del correo electrónico se adjuntaba un formulario con una serie de campos que habrían de ser rellenados por el supuesto ganador del premio, si bien, los ciberdelincuentes lo que pretendían era obtener sus datos personales –mediante la técnica del *phishing*– para llevar a cabo ulteriores actos ilícitos con ellos. Tampoco podemos pasar por alto la reciente estafa relacionada con Bizum[7], en que los cibercriminales se amparan en la facilidad de esta aplicación móvil para realizar transferencias y en la que se ha detectado el envío de miles de solicitudes de cobro, haciéndose pasar por contactos de la agenda de las víctimas. En esta estafa, la cantidad que se reclamaba era de 50 euros, y los autores enviaban un mensaje de Whatsapp a números aleatorios, haciéndoles creer que eran contactos de su agenda, y en el que se indicaba que el emisor del mensaje había realizado al receptor, por error, una transferencia de 50 euros por Bizum, indicando que se había confundido y que quería enviar el dinero a otra persona.

---

[3] Noticia titulada: "Consumidores de Galicia advierte del aumento de estafas bancarias por 'phishing'", publicada el 27 de septiembre de 2021, disponible en https://www.elespanol.com/quincemil/articulos/economia/consumidores-de-galicia-advierte-del-aumento-de-estafas-bancarias-por-phishing.

[4] Noticia titulada: "Ola de estafados en Galicia por transferencias fraudulentas: "Me quedé con 10 céntimos en la cuenta"", publicada el 19 de septiembre de 2021, disponible en https://www.niusdiario.es/espana/galicia/ola-estafados-galicia-transferencias-fraudulentas-banco-quede-10-centimos-cuenta_18_3204345445.html.

[5] Noticia titulada: "¿Eres cliente del BBVA? La Policía Nacional alerta sobre una nueva estafa relacionada con el banco", publicada el 24 de septiembre de 2021, disponible en https://cadenaser.com/ser/2021/09/24/sociedad/1632470339_154500.html?ssm=tw.

[6] Noticia titulada: "Alerta de la Policía por un nuevo timo con Mercadona", publicado el 25 de septiembre de 2021, disponible en https://www.lavanguardia.com/economia/bolsillo/20210925/7745037/mercadona-estafa-timo-policia-premio-correo.html.

[7] Noticia titulada: "La policía alerta de una estafa por Bizum para robarte 50 euros", publicada el 21 de septiembre de 2021, disponible en https://www.elconfidencial.com/tecnologia/2021-09-21/estafa-bizum-alerta-policia-robo-50-euros_3293287/.

Otro triste ejemplo viene representado por el boom de compras de mascotas –significadamente perros– tras la pandemia. Los ciberdelincuentes han encontrado un nuevo nicho de mercado y han proliferado supuestos en los que se colocan en distintas páginas web anuncios de venta de cachorros de perro[8]. En esta modalidad, las víctimas, tras ver el anuncio, contactan con los falsos vendedores y, tras la negociación, conciertan la compra. Pese a que realizan el pago del precio convenido de modo puntual, el perro nunca llega a su destino. Éste es solo uno de los miles de casos en los que las páginas de venta de bienes, productos y animales albergan anuncios que, en realidad, son estafas. Baste ver en cualquier juzgado de instrucción el número de juicios por delito leve en los que se ventilan peticiones de videconsolas, teléfonos móviles, televisores, ordenadores u otros productos electrónicos, en los que se concierta la compra de un bien por un precio mucho más reducido de su PVP, el abono se produce pero el objeto de la compra nunca llega al comprador.

Asimismo, otras plataformas de contenido audiovisual, como Netflix, han sufrido ataques de los ciberestafadores. En este caso, los autores remitían correos electrónicos a direcciones de todo el mundo, simulando ser una comunicación de Netflix[9], y manifestaban que se había suspendido la renovación de la contratación, al no haberse recibido el pago, por lo que adjuntaba un link para actualizar la cuenta de usuario. Además, a propósito de los multinacionales de mayor relevancia, podemos anotar el catálogo de ciberestafas que se han cometido –o intentado cometer– bajo la cobertura simulada del gigante Amazon[10], y en las que, resumidamente, se comunicaba a sus receptores alguna de las siguientes eventualidades: i) que el sujeto se había dado de alta en el servicio Amazon Prime, con lo que, al recibir el mensaje e intentar cancelar esa petición, abría el portillo de su privacidad a los ciberestafadores, ii) que alguien había entrado en su cuenta de modo indebido, facilitando un enlace para subsanar tal situación, iii) que se ha realizado una compra que el receptor nunca realizó, para lo que se facilitaba un número de teléfono al que llamar –y que era aprovechado para sustraer los datos personales–, iv) que se había recibido una tarjeta regalo o v) que el receptor era ganador de un premio.

No obstante, no solo se emplea el nombre de entidades privadas sino que, en múltiples ocasiones, los ciberestafadores simulan ser una institución pública. Podemos reseñar, en los últimos meses, el correo electrónico en que se finge una comunicación en nombre de la Agencia Tributaria[11]. En el mensaje se señala que existen irregularidades en la declaración de la renta presentada y que se proceda al abono de la diferencia. En idéntico sentido, se han remitido correos electrónicos en los que se simula una

[8] Noticia titulada: "Cae una banda que cometió 33 estafas con la venta de cachorros en Internet", publicada el 21 de agosto de 2020, disponible en https://www.abc.es/espana/comunidad-valenciana/abci-banda-cometio-33-estafas-venta-cachorros-internet-202008211928_noticia.html.

[9] Noticia titulada: "Si eres usuario de Netflix y te llega este correo debes tener cuidado", publicada el 3 de junio de 2021, disponible en https://www.lne.es/tv-espectaculos/2021/06/03/usuario-netflix-llega-correo-debes-52587267.html.

[10] Noticia titulada: "Así son las estafas más peligrosas relacionadas con Amazon que buscan robarte", publicada el 30 de noviembre de 2020, disponible en https://www.abc.es/tecnologia/redes/abci-estafas-mas-peligrosas-relacionadas-amazon-buscan-robarte-202011290132_noticia.html.

[11] Noticia titulada: "La estafa que llega a nuestro correo electrónico en nombre de Hacienda", publicada el 23 de septiembre de 2021, disponible en https://www.elcomercio.es/economia/estafa-hacienda-correo-electronico-0210923131812-nt-20210923134629-nt.html#vca=eng-rrss&vcm=amp&vso=elcomercio&vli=tw.

comunicación del SEPE[12] en la que se indica que el destinatario tiene derecho a un reembolso cuando, en realidad, se pretenden obtener los datos personales e instalar un malware en el ordenador de la víctima –de igual modo, en otras comunicaciones los ciberdelincuentes simulan una comunicación de la Seguridad Social–. Por mencionar otros casos que se han documentado, podemos citar la estafa en la que un SMS se remite, presuntamente, desde Correos[13], y se solicita al destinatario que, para completar un envío que tiene que recibir, ha de abonar un pago. En el mensaje se reenvía a una URL falsa de Correos en la que se solicitan datos personales y bancarios del cliente, con lo que los ciberdelincuentes obtendrían acceso a las cuentas corrientes de las incautas víctimas.

No podemos dejar de citar otro clásico de las ciberestafas, siempre recurrente, en cuya virtud los cibercriminales remiten mensajes de correo electrónico a un número indeterminado de víctimas fingiendo ser un mail de la DGT[14] en que se informa de que existe una multa de tráfico pendiente, que no ha sido abonada, y en el que consta un enlace para proceder a la subsanación de dicha situación. Incluso otras entidades públicas, como la Universidad Rey Juan Carlos[15], han dado cuenta de ataques de *phishing*; en concreto, en dicha entidad se produjo el envío masivo de correos electrónicos que simulaban una cuenta de la Facultad de Ciencias Jurídicas y Sociales de dicho campus, siendo el fin perseguido por sus autores, nuevamente, la obtención de datos personales de las víctimas.

Estos son solo algunos ejemplos de comunicaciones que se realizan a diario, en las que se involucra a entidades privadas y públicas, y en las que siempre se persigue un mismo objetivo: obtener datos personales de las víctimas, vaciar sus cuentas bancarias o introducir malware en los dispositivos afectados. Desde una perspectiva judicial nos encontramos con las dificultades de investigación que brinda el ciberespacio. En muchas ocasiones, cuando se producen estafas, éstas no superan los 400 euros, por lo que se trata de un delito leve. Así las cosas, aunque se den denuncias, en numerosos casos las conductas quedan impunes, ya que en el juicio por delito leve no existe fase de instrucción, por lo que resultará complejo determinar un responsable de los hechos. Pese a ello, en aquellas ocasiones en las que sí se determine una IP desde la que se haya cometido el delito, también puede resultar imposible concretar quién ha sido el autor de los hechos. Otro aspecto destacable es que la Red favorece el anonimato, la deslocalización y el empleo de ardides técnicos como los *proxy* puede alejar al autor de los hechos de su descubrimiento. En otras ocasiones, los autores de las estafas se valen de las denominadas "mulas", ya sean voluntarias o involuntarias. En tales casos, cuando

---

[12] Noticia titulada: "El SEPE alerta de una estafa con correos que suplantan a la Seguridad Social", publicada el 11 de marzo de 2021, disponible en https://www.lavanguardia.com/economia/bolsillo/20210311/6338831/sepe-estafa-timo-sms-correo-seguridad-social-hackeo.html.

[13] Noticia titulada: "Regresa la estafa del SMS de Correos: así intentan robarte tus datos o introducir un virus", publicada el 7 de septiembre de 2021, disponible en https://www.eleconomista.es/actualidad/noticias/11382643/09/21/Regresa-la-estafa-del-SMS-de-Correos-asi-intentan-robarte-tus-datos-o-introducir-un-virus.html.

[14] Noticia titulada: "La DGT avisa: vuelve la estafa de las falsas multas de tráfico", publicada el 12 de abril de 2021, disponible en https://www.eleconomista.es/nacional/noticias/11154368/04/21/La-DGT-avisa-vuelve-la-estafa-de-las-falsas-multas-de-trafico.html.

[15] Noticia titulada: "La URJC alerta a sus miembros de casos de phishing con correos masivos para lograr datos personales", publicada el 19 de marzo de 2020, disponible en https://www.lavanguardia.com/local/madrid/20200319/474258684393/la-urjc-alerta-a-sus-miembros-de-casos-de-phishing-con-correos-masivos-para-lograr-datos-personales.html.

es voluntaria, la mula percibe los fondos a cambio de una pequeña comisión, si bien, su cuenta bancaria es la que figurará en las investigaciones como la perceptora del desembolso. En otras ocasiones, se pueden emplear cuentas de titulares sin su consentimiento y sin su conocimiento, y son instrumentalizadas para redirigir los fondos a otros destinos, dificultando su trazabilidad y su perseguibilidad.

Pero las dificultades judiciales no solo se quedan aquí: en determinadas ocasiones las víctimas de estafas pueden ser denunciadas, con posterioridad, como autoras de otros delitos de estafa, ya que los cibercriminales han empleado sus datos personales para cometer nuevos fraudes. Así las cosas, nos encontramos con una revictimización múltiple. Podemos mencionar el caso de una joven que sufrió una estafa online en la compra de un perro[16] que nunca recibió –de igual modo que el caso que apuntamos antes– y cuyos datos personales fueron empleados en multitud de estafas siguientes, lo que le acarreó numerosas denuncias, con sus consiguientes procesos judiciales. Esta operativa no es algo inusual: existen bastantes supuestos en los que los denunciados en delitos leves de estafa, el día del juicio –o con anterioridad, mediante envío de documentos al juzgado– ponen de manifiesto que ellos habían sufrido una estafa anterior, lo que constatan aportando la denuncia –e incluso la sentencia de los juicios en los que intervinieron como denunciantes– y que, a raíz de tales hechos, están recibiendo denuncias por estafas cometidas *online* por todo el territorio nacional. El común denominador de todos estos casos es que tales personas habían facilitado en determinadas adquisiciones en el ciberespacio –que nunca se habían ejecutado– sus datos personales, mediante fotografías de su DNI y de su rostro. Con posterioridad, tales datos eran empleados por los ciberdelincuentes en posteriores estafas.

Tampoco podemos soslayar que es posible que exista una relevante cifra negra de casos no denunciados, precisamente por el sentimiento de vergüenza de las víctimas, o por su desidia, al considerar que la cantidad estafada resulta de poca relevancia y que los gastos de un proceso judicial serían mayores. Apuntamos a los sentimientos de vergüenza en aquellos casos en los que la víctima ha pretendido un lucro económico –*v. gr*., el timo de la lotería, de la herencia que se va a percibir o del premio ganado, para cuya adquisición se solicita un previo desembolso por determinados gastos de gestión– y ha adelantado una cantidad dineraria, esperando recibir un beneficio mucho mayor que este aporte original. No dejan de ser sucedáneos del timo de la estampita o de los billetes tintados, aunque en su versión 5.0, y que ahora tienen lugar en el ciberespacio.

Una vez que hemos anotado la grave problemática a la que nos enfrentamos, y que se ha incrementado en los últimos tiempos, forzoso es reconocer que existen instancias policiales que están realizando activas labores de concienciación, de detección y de advertencia de estos delitos. Podemos mencionar la actuación en redes sociales del Cuerpo Nacional de Policía, de la Guardia Civil o de los Mossos d´Esquadra, en cuyos perfiles se comunican las nuevas ciberestafas y se dan pautas de comportamiento a los usuarios de Internet. A su vez, ocupa un papel destacado en esta misión de prevención de los ciberdelitos el Instituto Nacional de Ciberdelincuencia (INCIBE). A través de su

[16] Noticia titulada: "Estafan a una joven al comprar un perro, le usurpan la identidad y recibe decenas de denuncias", publicada el 6 de abril de 2021, disponible en https://www.diariodesevilla.es/mascotas/Estafan-comprar-usurpan-identidad-denuncias_0_1562544161.html.

página web[17] se brindan útiles consejos e información sobre ciberseguridad, y se reportan avisos sobre los últimos ciberfraudes. Se trata de una guía actualizada en la que se advierte de las últimas campañas de ciberataques detectadas en la Red, por lo que es recomendable su consulta de modo habitual, o la suscripción a sus boletines y publicaciones.

Con ser cierta la relevancia de los mecanismos formales e informales de prevención de las ciberestafas, hemos de subrayar que lo verdaderamente importante es que los cibernautas adoptemos las pertinentes medidas de autoprotección cuando usamos las TIC. Por ende, hemos de ser cautelosos y responsables en la facilitación de nuestros datos personales. Debemos sospechar cuando recibamos comunicaciones extrañas, inesperadas o de organismos con los que nunca nos hemos comunicado por email o SMS. Hemos de ser realistas cuando observemos anuncios de venta de bienes, servicios o animales a precios sensiblemente inferiores a los de mercado, porque eso puede ser un poderoso indicio de la falsedad de dicha publicidad. Debemos contrastar la veracidad de los sitios web a los que nos remiten los enlaces URL y, en caso de duda, no ha de llevarse a cabo ninguna de las acciones que se nos solicitan que, además, suelen ir acompañadas de las coletillas "urgente" o "muy importante". En este sentido, el principio de confianza que nos inspiran los mensajes con logos y membretes de organismos oficiales, o con los signos de conocidas marcas, ha de ser tamizado por la prudencia en el manejo de un espacio que nos puede poner en peligro. Ello se anuda a que, en muchas ocasiones, carecemos de los conocimientos técnicos e informáticos requeridos para ser conscientes del fraude sufrido, por lo que hemos de redoblar la atención puesta en cada golpe de ratón.

En definitiva, las TIC, bien empleadas, son un instrumento que nos facilita notablemente la vida y que nos ayudan en todos nuestros ámbitos de desarrollo, pero se pueden convertir en un grave problema si se utilizan de modo indebido y si no nos guiamos por unas máximas y pautas de cuidado y de prudencia. Desde estas breves líneas, por lo tanto, se hace un llamamiento a no bajar nunca la guardia cuando naveguemos en el ciberespacio. Las modalidades de ciberfraudes son variadas, en muchas ocasiones muy sofisticadas, y poseen un carácter dinámico y cambiante, al albur de las últimas novedades en demandas de bienes y servicios, por lo que los cibernautas también debemos actualizar y reciclar nuestros sistemas de defensa y autoprotección.

[17] Página web del INCIBE: https://www.incibe.es/.