9. CRIMINALIDAD INFORMÁTICA

Uno de los aspectos de la vida de los ciudadanos y ciudadanas en el que se han percibido con mayor claridad los efectos de la pandemia causada por la COVID-19 es, sin duda, el relacionado con el uso de las tecnologías de la información y la comunicación (en adelante TIC). Las medidas de aislamiento social que nos hemos visto obligados a asumir la mayoría de habitantes del mundo para prevenir el contagio y la propagación de la infección han determinado, de forma inevitable, que todos los seres humanos con medios y posibilidades para ello, hayamos recurrido a las herramientas tecnológicas como mecanismo para mantener con la mayor normalidad posible nuestra vida personal y las relaciones con los demás.

La urgencia con la que hubo de llevarse a efecto esa trasformación en la actividad política, económica y social; la situación anímica de las personas preocupadas especialmente por su propia salud e integridad física y la necesidad de acomodar la actuación de toda clase de organismos, instituciones y entidades de carácter público o privado a esta nueva realidad, determinó que en muchos casos no fuera posible adoptar inmediatamente todas las medidas que resultaban precisas para dar plena continuidad al desenvolvimiento ordinario de la sociedad, garantizando al tiempo la seguridad exigible en el uso de dichas herramientas tecnológicas. Ello ha generado consecuencias perversas de distinta naturaleza en los múltiples sectores de la actividad humana: limitaciones en el normal desarrollo de las relaciones de carácter social y económico y en la prestación de servicios públicos; alteración en la actuación ordinaria de las instituciones; aparición de brechas de seguridad en los sistemas informáticos y mecanismos de comunicación, etc. y también ha tenido su incidencia en el ámbito de la delincuencia, como a continuación analizaremos con detalle.

Esta especial situación que afecta a la humanidad en su conjunto ha traído como consecuencia una intensificación del nivel de penetración de las tecnologías en los hábitos personales y sociales y en las formas y mecanismos de interrelación en toda clase de actividades y ha obligado a los poderes públicos de todos los Estados del mundo a promover e impulsar líneas de acción que mejoren la protección frente a los riesgos derivados del uso irregular del ciberespacio. La Comisión Europea en el documento *Nest Generation EU,* publicado en mayo del pasado año, al hilo de los trabajos de elaboración de una nueva Estrategia de Ciberseguridad, reflexiona acerca de cómo la pandemia ha evidenciado *la importancia de la digitalización en todas las áreas de la economía,* derivando de ello, a medio o largo plazo, *cambios per-*

manentes y estructurales en la vida social y económica entre los que menciona, como claramente perceptibles en el momento presente, la popularización del teletrabajo y la progresiva implantación de la formación en línea, el comercio electrónico y la Administración digital.

Obviamente, la actividad en la administración de justicia no podía ser ajena a toda esta situación y ello ha tenido también su reflejo en el trabajo que asume el Área de Especialización contra la Criminalidad Informática. Ciertamente, pese a los esfuerzos realizados tanto por la Fiscalía General del Estado como por el Ministerio de Justicia y el Consejo General del Poder Judicial para facilitar el funcionamiento de los órganos judiciales y la Fiscalía con las mínimas alteraciones, el obligado aislamiento social determinó la suspensión de una gran parte de los actos procesales, especialmente de aquellos que por disposición legal se celebran oralmente y en forma presencial y, como consecuencia, la paralización, o al menos la ralentización en la tramitación ordinaria, de la generalidad de los procedimientos judiciales. En ello influyó, sin duda, la rapidez con la que por razones de seguridad y salud pública hubo de sustituirse un modelo de actividad desarrollado habitualmente en un entorno físico y articulado (todavía en muchos territorios) sobre expedientes en papel por la utilización masiva del teletrabajo y los sistemas informáticos como medio de tramitación y resolución de los asuntos que nos competen. Las carencias existentes al respecto dificultaron la normalización en el funcionamiento de los Tribunales, que no se logró hasta transcurridos varios meses desde la declaración del estado de alarma.

Todas estas circunstancias han tenido influencia en los resultados estadísticos obtenidos en el área de especialización en criminalidad informática que, como comentaremos detalladamente en este mismo informe, aun cuando mantienen la tendencia alcista que venimos detectando en los últimos años, reflejan un índice de crecimiento más moderado que el registrado en la anterior anualidad tanto en el volumen de incoaciones como en el de acusaciones formuladas por el Ministerio Fiscal durante el año 2020. Efectivamente, si en la Memoria precedente informábamos de un incremento interanual del 44,92% y del 46% respectivamente en el volumen de nuevos procedimientos judiciales y escritos de acusación de la Fiscalía, el análisis comparativo entre los años 2019 y 2020 revela unos índices de aumento sensiblemente inferiores, 28,69% en referencia a nuevas incoaciones y 12,64% en acusaciones formuladas por la Fiscalía. No obstante, llamamos la atención sobre la circunstancia de que pese a las anomalías surgidas en la tramitación procesal, justificadas por la compleja situación existente, la actividad de los juzgados y del Ministerio

Fiscal en este ámbito ha seguido creciendo, particularmente en el segundo semestre del año, a medida que se iba retomando el ritmo normal de actuación tanto de las Fuerzas y Cuerpos de Seguridad como de los propios órganos de la jurisdicción penal e iba siendo factible «recuperar» una buena parte del retraso generado en los periodos más rígidos de aislamiento social. Este incremento de la criminalidad en el entorno tecnológico no es sino la consecuencia lógica de la profunda digitalización de las relaciones sociales y económicas, a la que la pandemia sin duda ha contribuido, que ha traído consigo el *traslado al ciberespacio* de la generalidad de las manifestaciones criminales, fenómeno, desde nuestro punto de vista, imparable y cuyos efectos en el momento presente solo somos capaces de vislumbrar pero que percibiremos con mayor claridad en un futuro próximo.

Uno de los ejemplos más claros de esta progresión es precisamente el de las conductas que atentan contra la libertad e indemnidad sexual de los y las menores de edad, manifestaciones criminales que se han visto extraordinariamente favorecidas por la necesidad de recurrir a las tecnologías como medio imprescindible de comunicación entre las personas. Las inmensas posibilidades que ofrecen estas herramientas y, por ende Internet, para facilitar la conectividad y la elaboración y difusión de todo tipo de contenidos está teniendo una demoledora influencia en la planificación y ejecución de este tipo de conductas delictivas y en concreto en el acoso *online* a menores con fines de carácter sexual y en la elaboración, distribución y puesta a disposición de terceros de material pornográfico. Así, la utilización masiva por niños, niñas y adolescentes de estas herramientas para todo tipo de comunicaciones y las limitaciones que les son propias, por su edad y falta de madurez, para prevenir los riesgos que asumen al mantener determinados contactos en la red (propiciados en buena medida por las posibilidades que ofrecen estas tecnologías para ocultar la verdadera identidad de sus interlocutores) ha acrecentado su vulnerabilidad ante acciones ilícitas que afectan muy seriamente a sus derechos y a su normal desarrollo y evolución y que son planificadas y ejecutadas por auténticos depredadores sexuales.

Esta situación ha ido agravándose con el paso de los años, a medida que las tecnologías han ido capilarizando las relaciones personales y sociales, y ha encontrado en las medidas de confinamiento derivadas de la infección por COVID-19 un perverso entorno facilitador. Los parámetros no pueden ser más evidentes y sobre ellos han llamado la atención organismos e instituciones nacionales o internacionales: los y las menores obligados a la utilización permanente de los dispositivos informáticos, incluso para la realización de sus activi-

dades escolares incrementando, de esta forma, su exposición al riesgo de ser víctimas de agresores sexuales; sus progenitores, tutores o guardadores, en ocasiones más preocupados por las circunstancias sanitarias, económicas o sociales que por la atención a la actividad *online* de sus pupilos; una buena parte de la población adulta más ociosa y sin otro medio de entretenimiento y/o diversión que el que ofrecen las tecnologías y, por último, los cuerpos policiales y organismos estatales volcando sus esfuerzos para atajar la pandemia y en proteger la seguridad y salud pública. Todo ello ha determinado –y así lo reseñan los cuerpos policiales y también muchos de los/as fiscales delegados/as– un aumento en la demanda y, en definitiva, en el tráfico de pornografía infantil en la red y, por ende, un mayor riesgo para el colectivo de personas menores de edad de sufrir conductas de ciberacoso ya sea con la finalidad de elaborar material pornográfico o incluso de llevar a efecto abusos sexuales en el entorno tecnológico.

Según el Informe publicado por Europol en junio de 2020 [1] sobre delincuentes y víctimas menores de abuso sexual en línea durante la pandemia, el número de reportes recibidos por esa Institución desde el NCMEC [2], por sospechas de distribución de pornografía infantil desde el territorio comunitario, ascendió a más de 1.000.000 en el mes de marzo, coincidiendo con el punto álgido de la pandemia en Europa, lo que implica un incremento del 1000% respecto de las 100.000 notificaciones recibidas en enero del mismo año, volviéndose a recuperar los niveles normales en el mes de mayo.

Esos datos se confirman en nuestro país con la información obtenida y facilitada por los cuerpos policiales a la Unidad Especializada en Criminalidad Informática. Así, según el informe elaborado en abril de 2020 por el Departamento de Delitos Telemáticos de la Guardia Civil sobre actividades vinculadas a la explotación sexual de menores en internet, los reportes del NCMEC dirigidos a España se incrementaron diariamente tras la declaración del estado de alarma en un 449% –de 105 a 578 reportes diarios– ascendiendo dicho índice al 730% con ocasión del periodo de confinamiento más intenso. Igual progresión se detectó en relación con otras vías habituales de intercambio de pornografía infantil. Concretamente el volumen de direc-

---

[1] Se trata del Informe titulado: *Exploiting isolation: Offenders and victims of online child sexual during de Covid-19 pandemic.*

[2] El Nacional Center for Missing and Exploited Children (Centro Nacional para Menores Desaparecido y Explotados) de EEUU es una corporación privada sin ánimo de lucro uno de cuyos objetivos es el de reducir la explotación sexual de los menores. Dicho organismo opera la CyberTipline destinada a la denuncia de pornografía infantil, tráfico sexual de menores y explotación sexual infantil.

ciones IP relacionadas con el tráfico de material ilícito en redes P2P se elevó en un 19,63% a partir de la declaración del estado de alarma, alcanzando un índice al alza del 23,76% en el periodo de confinamiento total. Igualmente se detectó un repunte significativo en las conexiones a la red TOR con idéntico objetivo que se concreta en un 36,51% tras declararse el estado de alarma y en un 42,21% durante el periodo de aislamiento más intenso.

A similar conclusión, a partir de los mismos indicadores, llegan también los grupos encargados de la actuación contra la explotación sexual infantil de la Unidad Central de Ciberdelincuencia del CNP, añadiendo además el dato obtenido en su línea abierta de atención a la ciudadanía, el correo electrónico denuncias.pornografía.infantil@policia.es. Los registros de esa *hotline* no pueden ser más esclarecedores: entre el 15 de marzo y el 30 de abril de 2020 se registraron 1732 avisos/denuncias de particulares por detección *online* de material pedófilo, lo que supone un incremento del 352% respecto de las 491 notificaciones recibidas en el mismo periodo temporal del año 2019.

Obviamente, la mayoría de esta información se obtiene mediante el uso de herramientas de rastreo que captan el *hash* de los archivos ilícitos que circulan por el ciberespacio, por lo que se trata de información que en la generalidad de los supuestos no llega a concretarse en investigaciones específicas y lo mismo ocurre con las denuncias ciudadanas que no siempre ofrecen datos suficientes para iniciar pesquisas por parte de las unidades especializadas de la Policía Judicial. Por esta razón no debe sorprender la diferencia entre estas cifras y las que resultan del análisis de los procedimientos judiciales por delitos de pornografía infantil tramitados durante el año (a las que nos referiremos detalladamente en el apartado correspondiente) que en 2020 reflejan un levísimo crecimiento de un 0,9% respecto del año precedente.

Por ello, lo que pretendemos con esta información es poner de manifiesto la gravedad del problema al que nos enfrentamos y sobre el que están llamando la atención tanto los organismos especializados de nuestro país como las instituciones internacionales. A título de ejemplo cabe mencionar la Comunicación que la Comisión Europea remitió el 24 de julio del pasado año al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones acerca de la necesidad de elaborar una Estrategia en la Unión Europea para hacer posible una lucha más eficaz contra el abuso sexual de menores. Según dicho informe la UE se ha convertido en el mayor centro de actividad relacionada con la pornografía infantil del mundo, vergonzante récord que implica necesariamente el desarrollo en el territorio comunitario de actividades destinadas a la producción de dicho mate-

rial, es decir, abusos sobre menores que en muchas ocasiones se planifican y ejecutan *online*.

Tal y como se deja constancia en dicho documento, en el ámbito de la UE ya se venía detectando desde hace años un drástico aumento de las denuncias por abuso sexual de menores *online* que han evolucionado desde las 23.000 del año 2010 a las más de 725.000 en 2019, situación que se ha agravado con ocasión de la pandemia. De hecho, el informe ofrece el escalofriante dato de que actualmente en Europa uno de cada cinco niños/as es víctima de alguna forma de violencia sexual ya sea *online* o en el entorno físico. En dicha comunicación se hace referencia también a la dificultad de investigar estas conductas dado el desarrollo constante de nuevas técnicas de transmisión de contenidos y también de mecanismos de encriptación o cifrado de extremo a extremo que, si bien contribuyen a garantizar el secreto de las comunicaciones, constituyen al tiempo importantes obstáculos para la investigación criminal. Se trata, por tanto –y a ello se refiere expresamente la citada comunicación– de que los Estados trabajen coordinadamente para mejorar las herramientas legales frente a este gravísimo fenómeno criminal, tanto en los aspectos penales sustantivos como en la articulación de técnicas de investigación que resulten realmente eficaces para esclarecer este tipo de acciones criminales, como es el caso de las relacionadas con la investigación secreta *online*, la infiltración policial o las que hacen posible el acceso a comunicaciones cifradas. En esta misma línea de acción, la propuesta europea apuesta por creación de un centro contra la explotación sexual de los y las menores, en el que ya se está trabajando y respecto del cual hemos efectuado algunas aportaciones desde esta Unidad de la Fiscalía General del Estado.

Desde un punto de vista cuantitativo, las manifestaciones criminales *online* que con mayor frecuencia se detectan en la red y las que dan lugar a la incoación de un número más elevado de procedimientos son las estafas y/o defraudaciones en sus múltiples y variadas modalidades y penalmente encuadrables en los arts. 248 y ss. CP. Esta clara preeminencia ha sido una constante observada invariablemente en los últimos años que en 2019 determinó que aproximadamente el 65% de los procedimientos judiciales incoados por ciberdelitos tuvieran por objeto conductas de esta naturaleza.

A tenor de los datos disponibles para la Fiscalía en el pasado año 2020, el número de procedimientos judiciales registrados por esta clase de delitos asciende a 12.250, lo que supone un significativo incremento, de más del 40%, respecto de los datos registrados en 2019. Las especiales circunstancias acaecidas en este periodo anual, y el hecho incuestionable de que un número no determinado de denuncias

no lleguen a conocimiento de los órganos de la jurisdicción penal, por mor de lo dispuesto en el art. 284 LECrim, determina la imposibilidad de pronunciarnos, por el momento y con los datos con que contamos, acerca de si dicho incremento –desde un punto de vista estrictamente cuantitativo– es atribuible en exclusiva a la generalización de la actividad comercial *online* a causa de las medidas de aislamiento derivadas de la pandemia o si en dicho resultado ha influido igualmente la evolución natural del fenómeno criminal que nos ocupa.

Ahora bien, lo que sí es posible afirmar rotundamente es que los y las delincuentes han ido adaptando los modelos defraudatorios a las peculiaridades de la situación vivida con ocasión de la pandemia, es decir, han utilizado como señuelo –y en cierta medida siguen haciéndolo– temáticas relacionadas con el confinamiento, los riesgos y consecuencias de la infección, los remedios para prevenir o curar la COVID-19 o la incertidumbre económica para captar la atención o el interés de sus futuras víctimas y articular el engaño generador del desplazamiento patrimonial o, en su caso, de la obtención de las claves o contraseñas personales que faciliten el apoderamiento económico en beneficio propio. Como se hace constar en el informe publicado por Europol el 27 de marzo de 2020[3], *los criminales han sido rápidos para aprovechar las oportunidades que les ha proporcionado la crisis adaptando su* modus operandi *o adoptando nuevas actividades criminales.* Las técnicas empleadas por los/as delincuentes están siendo muy variadas, por lo que, sin pretensión alguna de exhaustividad, nos limitaremos a exponer las más frecuentes o llamativas o las que han tenido un mayor impacto en la ciudadanía.

En primer término, es de obligada referencia la utilización de páginas web, plataformas de correo electrónico o cuentas en redes sociales para difundir públicamente ofertas fraudulentas de todo tipo de bienes y servicios de especial utilidad para cualquier persona en atención a las circunstancias concurrentes. Así, en los periodos con medidas de aislamiento más estrictas han sido frecuentes las denuncias sobre publicaciones engañosas realizadas a través de dichos medios en las que se simulaba poner a disposición del público mascarillas, guantes o, en general, material de protección personal o también aquellas que ofrecían bienes o prestaciones útiles para atender otro tipo de necesidades: productos de alimentación, ropa e incluso servicios de entretenimiento como suscripciones a plataformas de TV, equipos electrónicos, aparatos para hacer ejercicio en el domicilio

[3] *«Pandemic profiteering: How criminals exploit the covid-19 crisis».*

etc., efectos y servicios que los/as anunciantes no tenían intención de proporcionar pero que se ofrecían en condiciones tales que llevaban a las víctimas a efectuar el correspondiente desembolso económico, viéndose posteriormente defraudadas al no recepcionar los efectos o servicios adquiridos o concertados y resultar irrecuperable el importe adelantado que los/as delincuentes hacían propio en su beneficio.

Especial atención merecen en este apartado las ofertas fraudulentas *online* efectuadas con ocasión del confinamiento relativas a productos o compuestos médicos o farmacéuticos supuestamente aptos para prevenir o curar la infección, entre las cuales es especialmente llamativa la puesta a disposición en marzo de 2020, a través de un perfil de una popular red social, de una vacuna que se decía eficaz contra la COVID-19. Estas conductas, cuya finalidad suele ser exclusivamente la de obtener un beneficio económico irregular, presentan derivaciones de mayor interés cuando el consumo del producto ofertado puede generar un riesgo grave para la salud de las personas. En este último caso cabría incluso apreciar la comisión de un delito contra la salud pública, cuestión abordada específicamente por la Fiscalía de Lleida con ocasión de una investigación relativa a la publicitación a través de la red de un compuesto susceptible de prepararse artesanalmente al que se le atribuían efectos nocivos para el consumo humano, circunstancia que, tras las oportunas investigaciones, no pudo acreditarse debidamente por lo que las diligencias fueron finalmente archivadas.

Otras variantes de estas mismas actividades ilícitas son aquellas, también frecuentes en el periodo álgido de la pandemia, en las que los estafadores, siguiendo esta misma dinámica delictiva y haciéndose pasar por organismos o instituciones públicas o privadas, a través de páginas web falsas o de correos electrónicos, apelan a la solidaridad de las personas, solicitando la entrega de donativos supuestamente destinados a luchar contra la epidemia o a atender las necesidades de los colectivos más vulnerables, cantidades de las que posteriormente se adueñan en beneficio propio. Este tipo de conductas han dado lugar a la apertura de procedimientos judiciales en diversos territorios tal y como informan, entre otras, las Fiscalías de Valencia, Zaragoza y Madrid. Ha de reseñarse, aunque se encuentren extramuros de lo que se entiende estrictamente como actividad ilícita *online*, que en ocasiones estas acciones fraudulentas se han planificado y ejecutado contactando con las víctimas por vía telefónica, empleando idéntico ardid para engañarlas y obtener de las mismas entregas dinerarias que los delincuentes hacían propias.

Junto a estas modalidades de fraude de dinámica más tradicional se han detectado también otro tipo de conductas basadas en técnicas de

ingeniería social en las que el engaño, como elemento facilitador, no ha tenido por objeto motivar a la víctima a efectuar un desplazamiento patrimonial en su propio perjuicio sino obtener de la misma información personal que hiciera posible ordenar transferencias económicas en su nombre o que permitiera el acceso a su dispositivo móvil o sistema informático con la finalidad de apoderarse de sus claves y/o contraseñas bancarias o de cualquier otra información susceptible de utilizarse posteriormente para realizar disposiciones patrimoniales en propio interés y en perjuicio de las personas afectadas.

Buen ejemplo de ello son los supuestos en los que, a través de mensajería instantánea o correo electrónico y aprovechando las restricciones de movilidad de la población, los/as delincuentes simulaban la condición de miembros de las Fuerzas y Cuerpos de Seguridad y, con el pretexto de esclarecer supuestos hechos delictivos, solicitaban a la víctima información de carácter personal y/o bancaria. O también aquellos otros en los que, con idéntica finalidad de recabar datos personales, se hacían pasar por representantes de organismos públicos tales como la Agencia Tributaria o el Ministerio de Hacienda o en su caso de entidades prestadoras de servicios de primera necesidad –gas, electricidad, etc.– utilizando como reclamo la concesión de descuentos fiscales, ventajas en la facturación o supuestas ayudas económicas para afrontar los efectos de la crisis o, en otros casos, anunciando falsas ofertas de empleo para elaborar material sanitario.

La adaptación de la dinámica criminal a las circunstancias derivadas de la pandemia es claramente perceptible en referencia a los fraudes relacionados con la banca *online*, en los que el *iter criminis* combina el engaño con manipulaciones realizadas sobre sistemas informáticos para lograr los fines ilícitos pretendidos. Son muchas las variantes en que se manifiestan estas conductas, entre las cuales llama la atención la puesta en circulación de correos electrónicos maliciosos, aparentemente remitidos por los servicios correspondientes de diversas entidades bancarias, en los que falazmente se hacía creer a sus destinatarios/as que como consecuencia del confinamiento se estaban realizando modificaciones en sus protocolos internos de actuación para reforzar la seguridad de las operaciones *online*. En ese contexto, y para gestionar supuestamente los trámites oportunos de actualización, en el propio correo electrónico, se invitaba al cliente a pulsar un determinado enlace inserto en el mismo que le conducía a una página web, previamente preparada imitando la genuina del banco, pero controlada por los/as estafadores, en la que la víctima confiadamente introducía sus datos y claves privadas que de esta forma quedaban a plena disposición de los/as criminales. Se trata de

una técnica, ya habitual en las actividades fraudulentas relacionadas con la banca *online*, que los delincuentes han sabido hábilmente adaptar a la especial situación vivida por la ciudadanía.

Junto a estos supuestos se han detectado otros en los que el objetivo de la acción criminal era lograr el acceso irregular al sistema informático de la víctima con finalidades muy diversas. Es obvio que en las circunstancias vividas resultaba especialmente fácil invitar a cualquier persona a descargarse aplicaciones con variadas funcionalidades, algunas especialmente útiles como contrastar los síntomas de la enfermedad, asesorarse sobre medidas preventivas, obtener información sobre centros de asistencia próximos, etc. De una u otra forma, de lo que se trataba era de infectar el dispositivo o sistema informático de la víctima ya fuera para encriptar sus archivos, a través de un *malware* y posteriormente solicitar el correspondiente rescate por la recuperación de la información, ya para obtener información de diversa naturaleza sobre aspectos concretos de la vida del afectado/a –entre ellos los datos y claves bancarias a las que nos referíamos anteriormente– o, en su caso, de su actividad empresarial o incluso política o de relación social que pudiera ser posteriormente aprovechada por los/as agresores. Estas conductas, que también han dado lugar a la incoación de diversos procedimientos penales, serían encuadrables en las distintas figuras típicas que sancionan los ataques a los sistemas informáticos, tanto los de sabotaje previstos en los arts. 264 y 264 *bis* CP como los de espionaje informático contemplados en el art. 197 *bis* del mismo texto legal que, a su vez, y en atención a la información que irregularmente se pretende obtener, bien pudieran concurrir con otros ilícitos como los del art. 197.1 y 2 CP o de los arts. 278 y ss. y 598 y ss. CP.

La preocupación por las consecuencias de este tipo de acciones, particularmente tras el ciberataque dirigido contra el Hospital Universitario de Brno (República Checa) en el mes de marzo del año 2020, en pleno brote de COVID-19 en Europa, dio lugar a la difusión de distintas alarmas emitidas por organismos nacionales e internaciones orientadas a reforzar la protección de los centros médicos y sanitarios. Así, en nuestro país los distintos organismos de ciberseguridad a mediados del mes de abril informaron acerca de la detección de un *ransomware* conocido como *Netwalker*, que se estaba difundiendo a través de una campaña de correos electrónicos que utilizaba como reclamo la temática de la COVID-19. El correo se acompañaba de un archivo adjunto *CORONAVIRUS_COVID-19.vbs* con un código que al ser ejecutado se instalaba en el sistema atacado y cifraba sus archivos. Si bien en España por el momento no se han detectado ataques causados por este virus, nuestros centros hospitalarios en algunos casos han

sido objeto de accesos irregulares en sus sistemas informáticos orientados a la obtención y apoderamiento de datos personales de algunos pacientes para su utilización posterior con finalidades diversas como la difusión pública de dicha información o su aprovechamiento con fines lucrativos.

Finalmente, en este mismo apartado hemos de referirnos a las oportunidades que ha ofrecido y sigue ofreciendo el teletrabajo para el acceso o el apoderamiento de información a partir de deficiencias en las medidas de seguridad de los sistemas informáticos o de los mecanismos de comunicación electrónica establecidos con dicha finalidad que hacen posible, por ejemplo, el despliegue de VPN falsas o la obtención irregular de contraseñas o claves de acceso a los dispositivos personales en los que también pueden hallarse, dado el uso generalizado de este sistema de trabajo, datos o informaciones reservadas sobre actividades económicas de las empresas y de los organismos o instituciones públicas o privadas. De ello dan cuenta los diversos casos que hemos detectado de incursión no autorizada en reuniones o sesiones de trabajo o docentes por videoconferencia –recurso masivamente utilizado en estas fechas– aprovechando los delincuentes las propias vulnerabilidades del sistema o la configuración incorrecta de las opciones de privacidad.

No podemos finalizar este estudio sin abordar, aunque sea someramente, un problema que preocupa extraordinariamente por la incidencia que pudiera tener en los derechos y libertades de la ciudadanía y particularmente en las libertades fundamentales de expresión e información cuyo reconocimiento y ejercicio con plenas garantías resultan esenciales en la formación y mantenimiento de una opinión pública libre. Nos referimos a la utilización de las potencialidades que ofrecen las redes y sistemas informáticos para difundir información que, so pretexto de ofrecer soluciones o respuestas contra la infección o contra cualquier otro de los efectos sociales, políticos o económicos derivados de ello, lesiona el honor, la intimidad y la dignidad de las personas; incita al odio, la violencia o la discriminación respecto de determinados colectivos especialmente necesitados de protección; o pretende socavar falazmente los valores democráticos o la credibilidad de las instituciones nacionales o internacionales.

La situación de incertidumbre social generada con ocasión de la pandemia y el uso masivo de las TIC derivado de las medidas de aislamiento determinaron tal exacerbación en la difusión pública de este tipo de contenidos que la Comisión Europea, en el mes de junio de 2020, estimase conveniente dirigir una comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social y

al Comité de las Regiones dedicada expresamente a llamar la atención sobre la desinformación acerca de la COVID-19. En ella se advierte sobre las graves consecuencias que pueden derivarse de las campañas de tergiversación informativa en personas, aisladas por la situación de confinamiento y especialmente vulnerables frente a este tipo de prácticas, y sobre las consecuencias perversas que estas conductas pueden tener no solo en la salud y seguridad de esas mismas personas sino también en la pervivencia de los valores democráticos de los Estados de la UE y la credibilidad de sus instituciones y autoridades nacionales y comunitarias.

En nuestro país también hemos percibido en algunas ocasiones el uso inadecuado de las TIC con dichos objetivos, especialmente en el periodo en el que las medidas de aislamiento fueron más rigurosas. Es evidente que cualquier ciudadano/a está perfectamente legitimado/a para manifestar su opinión e, incluso, criticar públicamente y, en particular, a través de las TIC, la actuación de terceras personas y también de las autoridades y organismos públicos o privados en razón a su actuación o a la gestión llevada a cabo con ocasión de la pandemia o por cualquier otro motivo, pero ello ha de hacerse sin rebasar los límites establecidos en el artículo 20.4 CE al ejercicio de las indicadas libertades. Ahora bien, no todas las manifestaciones o expresiones públicas que superan dichas limitaciones pueden ser objeto de sanción penal sino únicamente aquellas que por su contenido y circunstancias, o por estar diseñadas específica y conscientemente para engañar a partir de datos erróneos, manipulados o directamente falsos, son encuadrables en alguna de las figuras típicas previstas en el Código Penal, como los delitos contra el honor o las amenazas a particulares, autoridades o instituciones de carácter público, los ilícitos contra la integridad moral de las personas o, incluso, los delitos de odio cuando las afirmaciones vertidas en la red supongan una incitación al odio, la violencia o la discriminación o lesionen la dignidad de los colectivos –o personas pertenecientes a los mismos– incluidos en el marco de protección del art. 510 CP.

En el periodo anual que nos ocupa se han tramitado algunas diligencias de investigación/procedimientos judiciales por hechos de esta naturaleza que, en principio, presentaban caracteres de delito. Buen ejemplo de ello son las actuaciones seguidas por un juzgado de Cieza (Murcia) y también las diligencias de investigación incoadas por esta Unidad Especializada de la FGE por supuestos delitos de injurias y calumnias al Gobierno o a determinadas Instituciones del Estado –remitidas finalmente en ambos casos a la Audiencia Nacional– o los distintos expedientes incoados en diversos lugares del territorio nacio-

nal para investigar publicaciones *online* en las que se pretendía responsabilizar de la infección a determinados colectivos o desplazar hacia ellos los reproches de la ciudadanía.

En cualquier caso, se trata de comportamientos que han de ser valorados cuidadosamente y atendiendo a las particularidades de cada supuesto evitando, en palabras de la STC 112/2016, caer en el riesgo de hacer del derecho penal un factor de disuasión en el ejercicio de la libertad de expresión. Es decir, solo será posible actuar penalmente frente a esos comportamientos concretos cuando la conducta claramente rebase los límites de la libertad de expresión y de la libertad de información y además esté prevista expresamente como delito en el código penal vigente.