3.2 **Bienes difusos en el ciberespacio**

La Unidad Especializada en Criminalidad Informática aporta en este capítulo importantes reflexiones. Comienza con la descripción de una realidad insoslayable, cual es que el espacio virtual, las tecnologías de la información y la comunicación e internet se han hecho omnipresentes tanto en la vida personal como colectiva de la sociedad.

Nuestra actividad profesional, social, económica, y privada se desarrolla, en buena medida, en el ciberespacio y la red constituye en la actualidad una herramienta imprescindible para las relaciones interpersonales en todos sus aspectos y dimensiones y, por tanto, para el desenvolvimiento de la vida en comunidad.

El uso generalizado de las tecnologías y el elevadísimo nivel de conectividad alcanzado en los últimos años a nivel mundial, particularmente tras la pandemia causada por la COVID−19, conlleva un sinfín de oportunidades para la humanidad, pero también genera nuevos riesgos para el pleno ejercicio de los derechos y libertades individuales que corresponden a todas las personas y nuevas amenazas para la sociedad en su conjunto y para la propia pervivencia de los principios y valores en los que se asienta el funcionamiento del Estado de Derecho y nuestro modelo de convivencia.

Ello es así porque la comunicación entre las personas y la difusión de todo tipo de contenidos, cualquiera que sea su naturaleza y finalidad, se desarrolla a gran velocidad y de forma masiva e indiscriminada más allá de los límites fronterizos de los Estados alcanzando a los ciudadanos y ciudadanas cualquiera que sea el lugar del mundo en que se encuentren.

Por ello la protección de intereses difusos, es decir, de aquellos bienes jurídicos que trascienden al ámbito individual y afectan a intereses colectivos de carácter supraindividual, adquiere una especial relevancia frente a determinados comportamientos que, al planificarse y ejecutarse en el ciberespacio y en conjunción con los factores antes indicados, generan situaciones de riesgo para los derechos y libertades de una generalidad de personas e implican una amenaza global y difusa para determinados colectivos o para la sociedad en su conjunto pudiendo lesionar, incluso gravemente, intereses de carácter general. De hecho, son múltiples las figuras delictivas que con ocasión de las últimas reformas legislativas se han incorporado al código penal español o se han ido redefiniendo o adecuando a la necesidad de actuar penalmente frente a algunos de estos comportamientos que, por el riesgo que entrañan, han sido objeto de especial atención por el legislador.

Algunas de ellas tipifican conductas que solamente es posible cometer *online* y, en otros casos, se trata de comportamientos susceptibles de planificarse y ejecutarse en el entorno físico, como así ocurre con los tipos penales de carácter más tradicional, que han ido evolucionando en las formas de comisión y desarrollo del *iter criminis* aprovechando las posibilidades de acción que proporcionan los avances técnicos y científicos e incrementando su efecto lesivo, como consecuencia generalmente de la mayor difusión de la conducta ilícita o del contenido lesivo.

Esa misma percepción ha determinado también que la circunstancia de haberse ejecutado la acción *a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información* haya sido tenida en cuenta por el legislador para contemplar una agravación de la pena inicialmente prevista en algunos tipos penales cuando ello haya contribuido a dar una mayor publicidad al hecho y, por ende, una mayor afectación a intereses colectivos. Las perversas consecuencias que pueden derivarse del uso del entorno virtual en la ejecución del *iter criminis* han sido claramente explicadas por la Sala Segunda del Tribunal Supremo en diversas resoluciones, entre otras en las SSTS 4/2017 de 18 de enero y 547/2022 de 2 de junio, que, aun referidas específicamente al discurso del odio, ofrecen un razonamiento plenamente aplicable a supuestos similares: *La extensión actual de las nuevas tecnologías al servicio de la comunicación intensifica de forma exponencial el daño de afirmaciones o mensajes que, en otro momento, podían haber limitado sus perniciosos efectos a un reducido y seleccionado grupo de destinatarios. Quien hoy incita a la violencia en una red social sabe que su mensaje se incorpora a las redes telemáticas con vocación de perpetuidad. Además, carece de control sobre su zigzagueante difusión, pues desde que ese mensaje llega a manos de su destinatario este puede multiplicar su impacto mediante sucesivos y renovados actos de transmisión. Los modelos comunicativos clásicos implicaban una limitación en los efectos nocivos que hoy, sin embargo, está ausente. Este dato, ligado al inevitable recorrido transnacional de esos mensajes, ha de ser tenido en cuenta en el momento de ponderar el impacto de los enunciados y mensajes que han de ser sometidos a valoración jurídico-penal.*

Las acciones ilícitas que atentan o ponen en riesgo intereses difusos se definen por su carácter genérico e indiscriminado ya que, en principio, no inciden directamente en bienes, intereses o derechos de personas concretas, sino que afectan a la ciudadanía en su conjunto, de forma indeterminada y en cierta medida indefinida. Por ello repercuten en los intereses de todos o de determinados colectivos integra-

dos por personas *ab initio* no identificadas si bien, en ocasiones, pueden dar lugar también a acciones lesivas concretas en los derechos y libertades de personas individuales.

Múltiples son las actividades que se desarrollan en el entorno virtual o que se sirven de esas herramientas en su planificación y ejecución que generan riesgos efectivos en intereses difusos. Nos centraremos en analizar aquellas que, por su frecuencia, sus efectos y por las consecuencias que producen en la ciudadanía, consideramos de mayor relevancia a los efectos que nos ocupan y que, por ello, están siendo objeto de una especial atención en el área de especialización en criminalidad informática:

3.2.1 Conductas que atentan contra los derechos e intereses de la infancia y la adolescencia y de las personas con discapacidad necesitadas de especial protección

Nos encontramos ante colectivos especialmente vulnerables que por sus circunstancias personales se encuentran indefensos ante contenidos maliciosos o contactos que entablan en la red, dado que carecen de la capacidad o formación necesaria para prever los riesgos que de ello se les pueden derivar. Consciente de esa vulnerabilidad, el legislador español con ocasión de la publicación de la LO 8/2021, *de protección integral de la infancia y adolescencia frente a la violencia,* incorporó en el Código Penal determinados delitos de peligro en los que utilizando una forma legal similar se sanciona *la distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación de contenidos específicamente destinados a promover, fomentar o incitar* al suicidio (art. 143 bis CP), la autolesión (art. 156 ter CP) o los trastornos alimentarios (art. 361 bis CP) entre personas menores de edad o con discapacidad necesitadas de especial protección.

En todos estos preceptos se produce un adelantamiento de la barrera de protección penal para amparar con mayor intensidad los derechos e intereses de los indicados colectivos, con el objetivo de protegerles frente a situaciones potencialmente peligrosas para su salud, su vida o su integridad física. Estos tipos penales, por tanto, no exigen que se haya producido una conducta lesiva ni que el riesgo se concrete en personas determinadas, sino que la mera difusión a través de los medios indicados de contenidos de esa naturaleza completa íntegramente la acción delictiva.

Algo similar ocurre con el artículo 189 bis CP en referencia a la distribución o difusión, en igual forma y a través de los mismos

medios, *de contenidos específicamente destinados a promover, fomentar o incitar a la comisión* de acciones ilícitas contra la libertad sexual de los menores. Este precepto, que fue incorporado en el Código Penal español con ocasión de la misma reforma, persigue idéntico objetivo que los anteriores, es decir, sancionar determinadas conductas que, por sí mismas, generan un riesgo que afecta no tanto a menores de edad perfectamente individualizados, sino a todos los integrantes de ese colectivo, ya que se trata de comportamientos que pueden alentar la práctica de agresiones contra la libertad sexual de cualquiera de ellos.

Por las razones antes expuestas, y con el objetivo de minimizar dicho riesgo, en todas estas figuras delictivas el legislador ha incorporado un párrafo segundo relativo a la retirada o el bloqueo de acceso a través de la red a dichos contenidos. Esta previsión, que en la actualidad se encuentra contemplada con carácter general para cualquier actividad ilícita cometida *online* en el artículo 13 LECrim –tras la reforma derivada de la LO 10/2022, de 6 de septiembre–, tiene una gran trascendencia ya que con independencia de las posibilidades de actuar efectivamente contra los responsables de dichas conductas, su utilidad es incuestionable a efectos de evitar el acceso a los contenidos o publicaciones ilícitos y, con ello, para que sigan produciendo sus perniciosos efectos respecto de los bienes jurídicos que se pretende amparar.

No obstante, los derechos y libertades de estos colectivos especialmente vulnerables pueden también verse comprometidos por otras conductas de carácter más tradicional, cuyos efectos lesivos se han visto amplificados por las connotaciones derivadas del uso de las TIC en la planificación y ejecución criminal.

El mejor ejemplo de ello lo constituyen, sin duda, las conductas sancionadas en el artículo 189.1 b) CP, que castiga la distribución y/o puesta a disposición de terceros, en cualquier forma, de material CSAM o relativo a personas en situación de especial discapacidad. La Consulta 3/2006 FGE se refiere al objeto de este tipo penal indicando que, *no protege bienes personalísimos, sino la seguridad de la infancia en abstracto y su dignidad, adelantando las barreras de protección y atacando el peligro inherente a conductas que pueden fomentar prácticas pedófilas sobre menores concretos*. Y así también lo ha venido indicando la Sala Segunda del Tribunal Supremo en diversas resoluciones, entre ellas SSTS 826/2017 de 14 de diciembre y 395/2021 de 6 de mayo. La puesta en circulación de este tipo de contenidos, e incluso su mera posesión (art. 189.5 CP), aunque no afecte directamente a la libertad sexual de menores concretos y determinados, ya que no implica una actuación efectiva sobre alguno o

algunos de ellos, genera un grave riesgo para el normal desarrollo y evolución de la infancia y la adolescencia en su conjunto, por lo que su tipificación penal se justifica precisamente en la necesidad de conjurar dicho riesgo. Y lo mismo ha de indicarse cuando se trata de la elaboración artificial y posterior difusión de material CSAM, práctica favorecida en la actualidad por la generalización del uso de los sistemas IA, que facilitan la creación de dichos productos en condiciones tales de realismo que el contenido resultante parece corresponder a personas y situaciones efectivamente producidas.

En ambos casos, se trata de actividades que fomentan el consumo y el comercio ilícito de ese tipo de contenidos y, en consecuencia, generan el riesgo de que se lleven a efecto agresiones sobre personas menores para satisfacer la demanda de material CSAM que de su grabación puede obtenerse.

Pues bien, es un hecho constatado que, la intensidad con la que las tecnologías han ido capitalizando la vida de las personas y, entre ellas, la de los menores de edad está incrementando de forma muy preocupante el tráfico *online* de estos materiales ilícitos con los efectos perversos que ello conlleva. El Gobierno de España es plenamente consciente de esta peligrosa tendencia alcista y por ello, para proteger los intereses de los niños, niñas y adolescentes, tanto a nivel individual como colectivo, ha remitido al Congreso un proyecto de ley para mejorar la protección de las personas menores de edad en el entorno digital. Por nuestra parte, la Red de Fiscales especialistas en criminalidad informática se encuentra seriamente implicada en este mismo objetivo ya que la actuación frente a los comportamientos que hemos analizado, junto con otras acciones que atacan directamente la libertad sexual de las personas menores de edad como conductas de *childgrooming,* elaboración de material CSAM, o agresiones sexuales directas *online,* constituye uno de los ejes esenciales de nuestra actividad como red especializada.

Esta preocupación por hacer posible una respuesta eficaz respecto de estos graves comportamientos determina que todos los escritos de acusación, por hechos ilícitos contra la libertad sexual de menores y personas con discapacidad necesitadas de especial protección, se encuentren sometidos a supervisión de la Unidad especializada y también, que las diversas cuestiones que periódicamente van suscitando la investigación y persecución penal de estas conductas sean habitualmente objeto de tratamiento conjunto y reflexivo en las Jornadas de Especialistas en Criminalidad Informática. Se mantiene una colaboración directa a través de la Unidad Especializada con el INCIBE en orden a impulsar y promover la investigación criminal y la retirada de

la red de aquellos contenidos CSAM que llegan a conocimiento de dicho organismo en su calidad de miembro español de la red internacional INHOPE contra el abuso sexual infantil.

3.2.2 Conductas que atentan contra la dignidad de las personas y el principio de igualdad de todos los seres humanos a través de la difusión del discurso del odio

Otras manifestaciones criminales que atentan o ponen en riesgo intereses difusos son las conductas encuadrables en el concepto genérico de crímenes de odio, es decir, aquellas basadas en la intolerancia, la discriminación del otro por sus características o connotaciones personales y la negación de la diversidad. Se trata de hechos ilícitos de diversa naturaleza que atentan contra los principios y derechos proclamados en los artículos 10 y 14 CE, y en los que el factor discriminatorio constituye la motivación de la acción criminal.

Estas conductas se sancionan en distintos tipos penales, entre ellos, los delitos de amenazas a grupos específicos de población (art. 170.1.º CP), el delito de discriminación laboral (art. 314 CP), los de denegación de prestaciones (arts. 511 y 512 CP), los delitos contra los sentimientos religiosos (arts. 522 a 525 CP) y los delitos sancionados en el artículo 510 CP. Son acciones ilícitas que, dada su motivación, implican un ataque contra los derechos e intereses del colectivo afectado, aun cuando el acto agresivo este dirigido contra una persona concreta y perfectamente individualizada. Pero, además, en último término, la conducta ilícita produce también efectos negativos para toda la sociedad y pone en riesgo la pervivencia de los principios y valores constitucionales sobre los que se asienta el funcionamiento de los sistemas democráticos y nuestro propio modelo de convivencia, y esa es la razón de su incuestionable gravedad y peligrosidad También, en relación con estos comportamientos se están dejando notar los efectos perversos del desarrollo tecnológico ya que, en muchos casos, su planificación y/o ejecución total o parcial se lleva a efecto en el entono virtual. De hecho, las redes sociales, los foros, chats privados o blogs se han ido revelando en los últimos años como espacios o plataformas de gran efectividad para difundir o publicitar mensajes o contenidos que incitan, promueven o justifican el rechazo, la discriminación o la intolerancia frente a determinados colectivos y con capacidad de hacerlos llegar a toda la población. E igualmente se recurre a estos medios para amenazar, acosar u hostigar a personas concretas por motivos de esa misma naturaleza; para estructurar y dirigir células

clandestinas con ese objetivo e incluso para organizar y coordinar virtualmente ataques físicos a individuos o grupos así definidos bien sea contra sus personas o contra sus bienes patrimoniales. Precisamente por ello en el artículo 510.3.º CP el legislador ha previsto una agravación especifica de estas conductas, sancionadas en el citado precepto como *discurso del odio,* cuando los contenidos hayan sido accesibles a un elevado número de personas por haberse difundido a través de medios de comunicación, internet o del uso de las TIC.

3.2.3 Conductas que atentan contra la intimidad o la privacidad de una generalidad de personas

Es claramente perceptible que las capacidades de acción que proporcionan las tecnologías están facilitando la comisión de determinadas actividades criminales muy novedosas que atentan de forma aleatoria contra derechos de carácter personalísimo de un número indeterminado e indefinido de personas y generan un riesgo para la seguridad de todos. Tal es el caso de los ataques, cada vez más frecuentes, a sistemas informáticos o bases de datos en los que se almacena información personal, más o menos sensible, de una pluralidad de ciudadanos y cuya tipificación penal como delitos de descubrimiento y revelación de secretos se encuadra en los artículos 197 y 197 bis 1.º y 2.º CP.

En estos casos la agresión directa, concretada generalmente en un acceso irregular a sistemas informáticos o una interceptación ilícita, se dirige inicialmente contra un único sujeto pasivo claramente definido y seleccionado con antelación –organismos, instituciones o entidades públicas o privadas– pero su objetivo último es la exfiltración de ingentes cantidades de datos o informaciones de una generalidad de personas, no determinadas previamente, que se encuentran alojadas en el sistema atacado. De esta forma, se ven afectados, conjunta e indiscriminadamente un número elevado de personas cuya privacidad queda expuesta al conocimiento público y al destino que quieran dar los autores de la agresión a la información obtenida, ya sea su venta o puesta a disposición de terceros o su utilización en actividades defraudatorias o con cualquier otra finalidad ilícita.

Además de estos efectos lesivos, la frecuencia cada vez mayor con que se producen este tipo de ataques, afectando incluso a bases de datos de contenido especialmente sensible– como es el caso de los centros de asistencia médica u hospitalaria– puede generar en las propias víctimas y en toda la población un sentimiento de desconfianza

en el funcionamiento y la seguridad de las entidades atacadas o, incluso, en la resiliencia y fiabilidad de los sistemas informáticos a través de los cuales se articula, en gran medida, la estructura y organización de la sociedad.

3.2.4 Conductas que ponen en riesgo la salud o el bienestar físico de una generalidad de personas

Determinados delitos contra la salud pública, definidos en los artículos 360 y ss. CP, entre los que se incluye, la venta no autorizada, la oferta, la puesta a disposición de terceros o la publicitación de medicamentos, productos sanitarios, o alimentos que resultan nocivos o puedan poner en riesgo la salud de las personas, se han configurado también como delitos de peligro en los que se adelanta la barrera de protección para salvaguardar los intereses de todos y, por ende, de la ciudadanía en su conjunto.

Se trata por tanto de conductas ilícitas que atentan contra intereses de carácter general o difuso y proyectan sus efectos a toda la población, pues generan el riesgo de que cualquier persona pueda ver afectada su vida, integridad física o su salud por la adquisición y el consumo de medicamentos, productos o sustancias que le son ofertados, a veces falseando su composición o efectos o atribuyéndoles propiedades supuestamente beneficiosas para el ser humano. Los riesgos que entrañan estas conductas, al igual que comentábamos anteriormente respecto de otros ilícitos, se han visto incrementados cuando la oferta o publicitación de dichos medicamentos, sustancias o productos se realiza en el entorno virtual, de modo tal, que la difusión de información a través de redes, foros y plataformas pueda llegar indiscriminadamente a un número mayor de usuarios. En estos últimos años y particularmente tras la pandemia generada por la COVID−19, se detecta la utilización del ciberespacio con el objetivo precisamente de facilitar la publicitación, la oferta y la puesta a disposición generalizada de este tipo de sustancias o productos. De hecho, en aquel periodo se incoaron en nuestro país una pluralidad de procedimientos por actividades ilícitas *online* de esta naturaleza, en las que no solamente se engañaba a las víctimas para que efectuaran un desplazamiento patrimonial en su perjuicio, sino que además se promovía el consumo de sustancias nocivas para el ser humano. En estas situaciones, el peligro para la salud de los ciudadanos y el riesgo de que se llegue a producir alguna lesión a persona concreta y determinada aumenta de forma exponencial.

3.2.5 Conductas defraudatorias que atentan contra intereses de carácter patrimonial y ponen en riesgo la confianza de los consumidores en la economía digital y en el funcionamiento y seguridad del mercado digital

En términos generales, las estafas y demás acciones ilícitas de carácter defraudatorio se planifican y ejecutan respecto de personas concretas que son las que sufren directamente el perjuicio causado por la acción ilícita. Sin embargo, también en este ámbito, junto a las formas de comisión tradicionales, han ido surgiendo en los últimos años otras modalidades en las que el sujeto activo se sirve de las capacidades que proporcionan las tecnologías para dirigir su acción criminal a una generalidad de personas, no previamente determinadas, con el objetivo de captar el mayor número posible de víctimas y obtener con ello mayores beneficios.

Los ejemplos son numerosos y muy diversos: ofertas engañosas de todo tipo de bienes y servicios, simulación de entidades públicas y privadas para contactar con los ciudadanos a fin de obtener sus datos personales y utilizarlos posteriormente, propuestas falaces de inversiones económicas aparentemente muy ventajosas, transferencias u operaciones bancarias ordenadas sin autorización ni conocimiento del titular de los bienes, etc. Cada vez son más numerosas las acciones ilícitas de estas características, las personas que se ven afectadas y las pérdidas económicas que se derivan de ello.

Estas conductas no solamente lesionan los intereses económicos de quienes han sido víctimas directas del delito sino que también, en ocasiones y como apunta el *Informe de Ciberdelincuencia y Salud Mental 2023 del Instituto Nacional de Ciberseguridad,* pueden producirles consecuencias de carácter psicológico, tales como sentimientos de culpabilidad y/o de desconfianza en el funcionamiento y seguridad de las plataformas digitales –fenómeno que se conoce como *trauma digital*– que pueden condicionar de forma importante sus futuras interacciones en línea.

Pero además, la frecuencia con la que se cometen estas modalidades de fraude, el carácter masivo e indiscriminado de sus efectos y la circunstancia de que en reiteradas ocasiones la actividad defraudatoria se lleve a efecto mediante suplantación de organismos y entidades de carácter público y/o encargados de la prestación de servicios básicos (servicios de suministro, entidades bancarias, operaciones de comunicación, etc.) está dando lugar, en importantes sectores de la población, a una creciente desconfianza en el comercio electrónico, la seguridad

de las entidades bancarias y financieras e incluso el normal funcionamiento de los organismos y servicios públicos.

Se trata por tanto de actividades delictivas que no solo perjudican a quien ha sufrido concretamente el perjuicio económico, sino también, a intereses generales, de carácter colectivo. Así, lo recuerda con claridad el Preámbulo de la Directiva (UE) 2019/713, *sobre lucha contra el fraude y la falsificación de medios de pago distintos del efectivo* que deja constancia de la incidencia negativa de estos comportamientos tanto en la seguridad de los Estados, al facilitar la comisión de otras actividades delictivas, como también en el funcionamiento del mercado único digital *ya que socavan la confianza de los consumidores y provocan pérdidas económicas directas.* Y por ello precisamente, dicha disposición normativa propone diversas modificaciones de carácter penal sustantivo para proteger la economía digital y la confianza de la población europea en el comercio electrónico y en el funcionamiento del sistema bancario y financiero.

3.2.6 Conductas que atentan o ponen en riesgo la seguridad pública y la actividad ordinaria de organismos e instituciones públicas o privadas y de infraestructuras críticas esenciales para el funcionamiento social

Estos comportamientos constituyen un excelente ejemplo de actuaciones ilícitas que afectan a intereses colectivos de especial trascendencia social. También en este caso, los avances técnicos y científicos han traído consigo el surgimiento de un tipo de agresiones a datos y sistemas informáticos con las que lo que se pretende no es tanto la obtención de un beneficio de carácter patrimonial o la causación de un perjuicio concreto a un tercero, sino la desestabilización del normal funcionamiento del orden social, la actividad ordinaria de las instituciones y/o las empresas o del propio sistema democrático. Sirvan de ejemplo a estos efectos, los ataques informáticos dirigidos a bloquear o perturbar los sistemas establecidos para el control y seguimiento de procesos electorales o las páginas web o aplicaciones de altas instituciones y organismos implicados en la seguridad del Estado, con la intención de impedir o alterar su actividad ordinaria, desacreditarlas o simplemente como forma de coacción o de «castigo» por determinadas decisiones o actuaciones adoptadas por dichos organismos. Igualmente es posible incluir en este mismo apartado las agresiones a infraestructuras críticas, como encargadas de la seguridad de

los ciudadanos y de la provisión de bienes de primera necesidad o servicios públicos esenciales, como es el caso del suministro de energía, electricidad, gas, agua o los que se prestan a través de la red de comunicaciones.

Estas acciones se encuentran sancionadas como daños informáticos –artículos 264, 264 bis y 264 ter CP– pero, en atención a su finalidad, pudieran considerarse como delitos de terrorismo a tenor de lo dispuesto en el artículo 573.2 del mismo texto legal, lo que atraería la competencia de los órganos judiciales y la Fiscalía de la Audiencia Nacional.

3.2.7 Actuación del Ministerio Fiscal en la defensa de los intereses colectivos frente a la ciberdelincuencia

Ante la realidad que se acaba de exponer, la Red de Fiscales Especialistas en Criminalidad informática, desempeña un papel esencial en la protección de dichos bienes jurídicos frente a los retos que plantea la ciberdelincuencia. Es evidente que la adecuada respuesta penal frente a este grave y peligroso fenómeno criminal contribuirá positivamente a garantizar a toda la población el derecho a disfrutar de un entorno digital seguro en el que sea posible asumir plenamente las ventajas y oportunidades que ofrecen las TIC, minimizando los riesgos que de ello pueden derivarse. En consecuencia, la defensa de los intereses difusos en la red resulta esencial para garantizar una evolución segura en una sociedad tecnológicamente avanzada.

Para conseguir ese objetivo resulta esencial combinar las actuaciones orientadas a la prevención de las amenazas y agresiones que se producen en el ciberespacio con una respuesta sancionadora rápida y efectiva respecto de aquellas que revisten carácter delictivo. En definitiva, se trata de coordinar e interrelacionar ambas vías de acción para que la actuación del Estado de Derecho frente a estas agresiones sea realmente eficaz. De acuerdo con este planteamiento se está trabajando desde hace años en el ámbito nacional e internacional, existiendo importantes avances normativos en materia de ciberseguridad y protección en el ciberespacio de los derechos de los ciudadanos y, en suma, del interés general (Directivas NIS 1 y 2, el Reglamento IA).

Ciertamente las funciones que están encomendadas a la especialidad en Criminalidad informática se enmarcan en el proceso penal y, en definitiva, en el ejercicio de la acción sancionadora del Estado frente a este tipo de comportamientos y la protección de sus víctimas. Pero, por las razones antedichas –particularmente por el riesgo que

entrañan estas conductas para los intereses de carácter general y plurisubjetivo–, resulta necesaria la coordinación con los organismos e instituciones que se ocupan de la seguridad en el ciberespacio. A ello obedecen actuaciones como los mecanismos articulados para la notificación a la Unidad especializada de incidentes de seguridad por parte de la OCC o para la recepción de reportes sobre material CSAM. Por ello, también estamos intensificando las relaciones con diversas entidades privadas implicadas en esta materia: proveedores de servicio, operadores de telecomunicaciones, entidades bancarias, infraestructuras críticas, etc., a fin de articular sinergias que hagan posible que los resultados de su actuación en la detección de amenazas o incluso ante agresiones específicas sirvan para mejorar nuestra capacidad de respuesta penal frente a estas conductas.

Es evidente que, en el ámbito del proceso penal, al Ministerio Fiscal le corresponde la protección de los intereses difusos o colectivos y que, en muchas ocasiones será la única parte procesal que velará específicamente por ello. De ahí la importancia de nuestro compromiso en garantizar que la investigación sea rigurosa, pormenorizada y efectiva y también nuestro interés en la supervisión de los escritos de acusación por hechos de esta naturaleza, pues ello nos permite garantizar su adecuación a los parámetros y criterios establecidos en las Circulares, Instrucciones y Consultas de la FGE y en las Conclusiones que sobre muchos de estos temas se han acordado en las Jornadas de Especialistas en Criminalidad Informática.

Dada la naturaleza de estas conductas, la protección de los intereses afectados ofrece unas connotaciones muy peculiares. Al margen de los supuestos en que la acción delictiva se haya concretado en alguna o algunas víctimas específicas –supuestos en los que la acción de la Fiscalía debe ajustarse plenamente a las importantes funciones que nos están encomendadas al respecto– en la materia que nos ocupa adquieren una gran importancia las medidas destinadas a impedir que permanezcan accesibles en la red los contenidos ilícitos, cualquiera que sea su naturaleza: material CSAM, crímenes de odio, ofertas fraudulentas, plataformas simuladas de inversión de criptomonedas, venta de datos personales previamente sustraídos, publicitación de productos nocivos para la salud, desinformación, etc.

No parece necesario justificar la trascendencia de estas medidas ya que, con la retirada o bloqueo del acceso *online* a este tipo de contenidos, se protegen los intereses y bienes jurídicos afectados y se evita la posibilidad de afectación a derechos e intereses de personas concretas. Por ello, esta materia ha sido objeto de significativos avances normativos en los últimos años –alguno de ellos a iniciativa de la

propia Fiscalía– que han venido a reforzar las medidas tradicionales de decomiso previstas en la legislación penal. Así, la inicial previsión en el Código Penal de la posibilidad de acordar provisionalmente medidas de retirada de contenidos, interrupción de servicios o bloqueo de unos y otros en el curso de la investigación recogida en determinados tipos penales (arts. 143 bis,156 ter, 189.8, 189 bis, 270.3, 361 bis, 510.6 y 578.4 todos ellos del Código Penal), ha sido completada posteriormente con la modificación del artículo 13 de la LECrim, por LO 10/2022 de 6 de septiembre. Ello ha supuesto la incorporación de un nuevo apartado en el artículo 13 de la norma procesal, en el que se contempla la posibilidad de adoptar esas mismas medidas, como primeras diligencias, en la fase instrucción de cualquier delito cometido *online* cuando se estime necesario para garantizar el éxito de la investigación o la protección de intereses de las propias víctimas o de terceros.

Y en ello se está insistiendo igualmente en la normativa internacional, dada la eficacia de estas medidas a efectos de protección de las víctimas y también de los intereses generales a que nos venimos refiriendo. A ello se refiere el Reglamento (UE) 2022/2065 de 19 de octubre relativo al mercado único de servicios digitales (LSD) que, en su artículo 9, obliga a los proveedores de servicios a acatar las decisiones sobre retirada de contenidos cursadas por autoridades judiciales o administrativas en el desempeño de sus competencias y también el Reglamento (UE) 2021/784 de 29 de abril sobre la lucha contra la difusión de contenidos terroristas en línea.

Las fiscalías territoriales también han realizado interesantes aportaciones, de las que solo se hará alusión a algunas de ellas, por imposibilidad material de reflejar sus contenidos íntegramente.

La Fiscalía de Almería considera que tiene una gran responsabilidad en la defensa de los consumidores y usuarios víctimas de estafas *online,* no solo en el ámbito penal sino también en el civil. En concreto se refiere a las prácticas que pueden calificarse de abusivas por parte de las entidades bancarias frente a sus clientes cuando las defraudaciones se producen en un entorno digital. Los delitos de estafa informática o a través de medios telemáticos son cuantitativamente numerosos en todo el territorio nacional. Lamentablemente es frecuente el robo de credenciales bancarias y datos personales mediante mecanismos de «ingeniería social» a través de SMS o correos electrónicos maliciosos. Cuando empezaron a producirse este tipo de ataques hace unos años, las entidades bancarias asumían de forma generalizada la restitución del dinero indebidamente extraído de las cuentas de los clientes. Sin embargo, en los últimos meses se ha consolidado la

política contraria, consistente en culpabilizar al consumidor engañado y reprocharle su falta de diligencia para que asuma la totalidad de la pérdida de capital.

Más allá de puntuales resoluciones judiciales en el ámbito penal, la mayoría de las sentencias sobre esta materia son fruto de demandas interpuestas a modo particular por el ciudadano frente a su entidad bancaria, sin intervención ni participación de la Fiscalía. Mayoritariamente, nuestros tribunales civiles adjudican al banco una responsabilidad civil *cuasiobjetiva* fruto de su deber de proporcionar un entorno digital seguro a sus clientes, siendo condenados a la restitución del dinero que indebidamente salió de la cuenta del perjudicado con el uso indebido de sus credenciales.

En otras ocasiones, las menos, se pueden encontrar resoluciones judiciales que consideran altamente negligente la conducta del consumidor al proporcionar sus datos y claves a terceros y desestiman sus pretensiones indemnizatorias frente al banco, e incluso, algunas sentencias concluyen que hubo concurrencia de culpas y reparte el perjuicio causado entre banco y cliente al 50 %. En el ámbito penal, por falta de pretensiones de las acusaciones al respecto, apenas hay sentencias que entren a valorar si las entidades bancarias deben responder civilmente y de forma subsidiaria en este tipo de supuestos conforme a lo previsto en el artículo 120.3 del Código Penal. Por citar una de las escasas sobre esta materia, la de la Sala Segunda STS 188/2024 de 29 de febrero de 2024 confirma la condena de la entidad bancaria como responsable civil por dicho precepto.

El problema tiene varias aristas. En una primera aproximación, al consumidor le resulta beneficioso que se concentren en un solo pleito las acciones civiles y penales de manera que recupere su dinero y se castigue al culpable de la forma más simplificada posible. Sin embargo, en este tipo de delitos muchas veces no se logra o resulta muy dificultoso identificar al autor de la defraudación, por lo que no puede formularse acusación penal y civil contra el mismo, ni por lo tanto por la responsabilidad patrimonial subsidiaria de la entidad bancaria. En estos casos puede resultarle más conveniente al ciudadano dirigirse de forma inmediata contra el banco en la jurisdicción civil (puesto que está perfectamente identificado desde un primer momento) en vez de esperar la resolución del procedimiento penal en su fase de instrucción y enjuiciamiento.

La Fiscalía de Bizkaia constata el incremento en los últimos tiempos de los delitos de estafa cometidos a través de las TIC mediante la utilización de identidades de terceros no conocedores del hecho para la apertura y manejo de cuentas bancarias *on line* usadas para una

actividad defraudatoria. Ello ha provocado un gran esfuerzo para evitar en la medida de lo posible condenas injustas contra estas nuevas víctimas a través de los expedientes de seguimiento que se abren a nivel nacional, y que gracias a la colaboración de los compañeros se puede constatar el recelo de los juzgados a la hora de dictar condenas por estafas por meros movimientos bancarios. La Fiscalía refiere que sería deseable para paliar los efectos de estas acciones que las fuerzas y cuerpos de seguridad del Estado pudieran contar con una base fiable de denuncias a nivel nacional que les permitiera, a nivel de consulta, poder enlazar los procedimientos abiertos con la misma persona y consultarlos, y que los mismos se pusieran a disposición de todos los cuerpos, tanto nacionales como autonómicos, para poder investigar mejor los hechos y poder terminar con los autores reales que manejan las cuentas bancarias que en la mayoría de las ocasiones están ubicadas en territorio nacional.

Igualmente sería deseable contar con un refuerzo por parte del sistema bancario a la hora de verificar las aperturas *on line* de cuentas bancarias y los movimientos de estas, pues no en pocas ocasiones tan solo las cuentas aperturadas con identidades fraudulentas tienen exclusivamente entradas y salidas de dinero sin estabilidad de ningún tipo. Todo ello teniendo en cuenta además la entrada de la IA que llegará como un elemento más de la modalidad delictiva de la estafa. Todo ello con la única finalidad de reforzar así el sistema y la protección de los intereses de los consumidores.

En cualquier caso y como elemento coadyuvante al esfuerzo institucional en la lucha contra el fraude *on line*, es necesario continuar con las campañas divulgativas, informativas y formativas para los ciudadanos que les permita la autodefensa en este tipo de delito patrimonial.

En este ámbito delictual, desde la Fiscalía de Jaén se destaca el aumento de las víctimas de delitos de estafa informática, resultando de gran importancia para la función del MF la localización de sus denuncias, ante la previsión de resultar afectados un gran número de consumidores, y ello pese a que en muchas ocasiones no denuncian –por escasa cuantía– o no se judicializan las que se interponen –por falta de autor conocido–. Aquí cobra especial importancia la actuación del Ministerio Fiscal acordando la práctica de diligencias para averiguar datos sobre los responsables y, sobre todo, para la concreción de pequeños consumidores afectados. Como ejemplo de lo anterior menciona como una página web que ofrecía gestiones en Ayuntamientos y organismos oficiales por un pequeño precio, defraudó a múltiples consumidores, hasta que en la localidad de Baeza, a pesar de la escasa cuantía (10 euros), se presentó una denuncia que, si bien inicialmente

se archivaron las diligencias judiciales a las que dio lugar, las mismas se reaperturaron por la intervención del MF y ello lo permitió la práctica de actuaciones de investigación y la localización de cientos de consumidores afectados que no habían denunciado los hechos.

Esta Fiscalía señala otra forma de intervención del Ministerio Fiscal en el ámbito de la defensa de bienes jurídicos colectivos y difusos que, aunque comienza con reclamaciones de usuarios ante la Agencia española de protección de datos referentes a delitos contra la intimidad, estas se derivan a la Unidad de criminalidad informática, dando lugar a la interposición de denuncia por el MF, a los efectos de la investigación de los hechos y de las personas responsables de los mismos, realizándose ofrecimiento de acciones a los perjudicados, consiguiéndose en muchos casos poner en marcha procedimientos que los usuarios no hubieran hecho y localizar más víctimas perjudicadas, al ser numerosos los afectados en redes sociales.

Por la Fiscalía de Lleida se detecta un incremento de comisiones delictivas que afectan a una pluralidad de ciudadanos, abundando cada vez más las modalidades de estafas con apariencia de ventas o inversiones en activos que resultan fraudulentos. A través de estas dinámicas se genera un perjuicio colectivo difícil de determinar en su conjunto y es aún más complicado desenmarañar. A modo de ejemplo menciona el caso *Forex* que tiene por objeto numerosas denuncias por estafas relacionadas con criptomoneda, desarrolladas a través de corredores en línea. Se recabaron numerosas denuncias de estafas a través de corredores en línea en inversiones en el mercado de opciones Forex /binarias (uno por 560.000 euros) en el que se observó por los instructores policiales que detrás estaba la misma organización criminal que operaba a nivel internacional. Por tal circunstancia se solicitó la cooperación del órgano *Eurojust,* desde el cual pronto se tuvo conciencia del gran alcance que tenía la actividad delictiva, ya que resultaban perjudicados numerosos países de la Unión Europea, con afectación de cientos y cientos de víctimas y con un perjuicio de millones de euros mensuales, siendo calificada en la actualidad como una de las operaciones europeas más difíciles de gestionar por parte de *Eurojust,* y tanto por parte de la Guardia Civil como de Mossos d´Esquadra coinciden que es la estafa de mayor envergadura económica que ha habido en nuestro país.