

2.2 Los delitos contra personas menores de edad en el entorno virtual

El problema que analizamos tiene, sin duda, un mayor calado por la incidencia que el progresivo traslado al entorno virtual de las relaciones personales de una buena parte de la ciudadanía está teniendo en la delincuencia. Dicha circunstancia ha dado lugar a la aparición de nuevos comportamientos –no contemplados hasta hace poco como delitos en la legislación penal– capaces de dañar bienes jurídicos necesitados de protección y que por ello se hacen acreedores de sanción y persecución penal.

En otros casos, estas herramientas han determinado la aparición de inéditas formas de ejecución de conductas delictivas ya tipificadas que, merced al uso de estas tecnologías, pueden planificarse y realizarse con más facilidad y mayores posibilidades de impunidad para las y los responsables de las mismas.

Pues bien, entre las manifestaciones criminales en las que se está detectando con mayor intensidad ese efecto perverso del uso masivo de las tecnologías, se incluyen precisamente los ataques contra menores de edad. Es un hecho incuestionable que las inmensas posibilidades que ofrecen estas herramientas para facilitar la comunicación entre las personas y la elaboración y difusión de todo tipo de contenidos están teniendo una demoledora influencia en la planificación y ejecución de determinadas conductas delictivas que encuentran en las personas menores de edad, víctimas particularmente indefensas.

El recurso generalizado por parte de las y los menores a estas herramientas para sus comunicaciones con compañeras/os y amigos/os en sus círculos internos de relación, el acceso no controlado por parte de los mismos a contenidos de adultos, y la frecuente falta de previsión de estos jóvenes usuarios/as acerca de los riesgos que entraña la utilización negligente o descuidada de internet o de las redes sociales son circunstancias que aprovechan los ciberdelincuentes para aproximarse a ellos con objetivos maliciosos, lo que les coloca en situación de especial vulnerabilidad ante acciones ilícitas que afectan muy seriamente a sus derechos, intereses y libertades.

Sería imposible en este breve estudio hacer un análisis pormenorizado de las distintas manifestaciones criminales de las que son víctimas las/los menores en el entorno virtual, si bien en una primera aproximación podemos afirmar que se trata de conductas que normalmente atentan contra bienes de carácter personalísimo, tales como la intimidad, la libertad y/o seguridad, la dignidad y sobre todo la libertad sexual, y que por tanto pueden tener una influencia muy negativa

en el proceso de desarrollo personal del afectado en una etapa de su formación esencial para forjar su personalidad e identificar sus intereses y objetivos vitales. De ahí la incuestionable gravedad de estas acciones y la importancia de prevenir su comisión y, en su caso, de actuar eficazmente para evitarlas.

Al respecto y sobre la base de nuestra experiencia profesional podemos afirmar que cada vez son más habituales las investigaciones y/o expedientes judiciales o del Ministerio Fiscal relativos a ilícitos *online* contra bienes jurídicos de esa naturaleza. Esto puede responder a una mayor frecuencia en su comisión, a una tendencia creciente en la denuncia de esta clase de agresiones, o incluso a ambas razones simultáneamente. En cualquier caso, parece evidente, que la canalización a través de las TIC de toda clase de relaciones sociales está determinando el traslado al ciberespacio de las mismas patologías que se generan en la convivencia tradicional entre las personas y ello tiene su reflejo en los contactos entre menores de edad.

2.2.1 DELITOS CONTRA LA INTIMIDAD

Entre las manifestaciones criminales de las que con relativa frecuencia son víctimas las personas menores de edad han de reseñarse las conductas que atentan contra su intimidad que se sancionan en el artículo 197 –particularmente en su apartado primero– del capítulo I del título X del libro II del Código Penal relativo a los delitos de descubrimiento y revelación de secretos.

Nos referimos concretamente a acciones cuyos responsables pueden ser tanto personas adultas como otros menores y que consisten, entre otros comportamientos, en intromisiones en perfiles privados; grabación no consentida de actos reservados o de naturaleza íntima, no necesariamente de carácter sexual; apoderamiento de fotos, imágenes o vídeos almacenados por la víctima en dispositivos o sistemas de uso particular; acceso no autorizado a sus comunicaciones por WhatsApp o correo electrónico etc, conductas que el legislador español penaliza más gravemente cuando las víctimas son menores de edad, en aplicación del artículo 197.5 CP, dada su condición de personas especialmente vulnerables. La posterior difusión, revelación o cesión a terceros de dichos materiales irregularmente obtenidos atraería la aplicación del artículo 197.3 CP circunstancia que, lamentablemente detectamos con frecuencia, pues la pretensión última del agresor/a suele ser la de denigrar, menospreciar o humillar a su víctima dando a conocer a terceros, habitualmente integrados en foros y chats del propio círculo de relación del menor, aspectos reservados de su privaci-

dad, lo que podría implicar también, en atención a las circunstancias concurrentes y al contenido difundido, la comisión de un delito contra su integridad moral.

En el apartado séptimo del mismo precepto cabría incluir, al menos en algunos supuestos, las conductas de difusión o cesión no autorizada, de imágenes o contenidos audiovisuales de personas menores de edad por parte de quien los ha obtenido con su anuencia en un marco circunstancial de confianza mutua o, en su caso, por parte de terceros a sabiendas de su origen y de que el afectado no ha autorizado su divulgación. La complicidad existente en determinadas etapas del desarrollo personal entre compañeras/os y amigas/os de edades similares puede determinar la grabación consentida o el intercambio entre menores maduros de contenidos íntimos de diversa naturaleza –consumo de drogas, práctica de rituales, etc– que posteriormente puede tener cierta difusión, por lo que para que la conducta sea típica es imprescindible no solo que dichos contenidos se divulguen sin su consentimiento sino también que ello comprometa la intimidad de la víctima.

En los supuestos en los que las imágenes o grabaciones audiovisuales así obtenidas presentan connotaciones sexuales, la conducta concurrirá generalmente con la comisión de ilícitos contra la libertad sexual, entre ellos, con los relacionados con la elaboración o difusión de material de abuso sexual infantil.

2.2.2 DELITOS CONTRA LA LIBERTAD Y SEGURIDAD

Por otra parte, es incuestionable que la capacidad de actuación que ofrecen las tecnologías y, en particular, las redes sociales y los sistemas de mensajería instantánea facilitan también la planificación y desarrollo *online* de comportamientos que pueden resultar lesivos para otros bienes de carácter personalísimo, como aquellos que pretenden menoscabar la capacidad de la víctima, eventualmente menor, para tomar decisiones o para actuar libremente en los distintos ámbitos de su vida como es el caso de las amenazas y coacciones sancionadas como delito en los capítulos II y III del título VI del libro II del Código Penal.

Tal es el caso de los comportamientos susceptibles de enmarcarse en los artículos 169 y ss. y 172 y ss. del Código Penal, que se exteriorizan actualmente en formas muy diversas y variadas como resultado del aprovechamiento de las posibilidades inherentes al uso de las TIC, hasta tal punto que el legislador se vio en la necesidad de definir, con ocasión de la reforma operada en el Código penal por LO 1/2015, un tipo penal novedoso, el artículo 172 ter CP, en el que se sanciona la

conducta de acoso permanente u hostigamiento para facilitar la actuación frente a determinadas conductas que no encontraban adecuado encaje en las figuras delictivas preexistentes. Figura delictiva, por cierto, que ha sido modificada más recientemente por la disposición final cuarta de la LO 10/2022, de 6 de septiembre, de garantía integral de libertad sexual, para tipificar la apertura de perfiles falsos en redes sociales, páginas de contactos o cualquier medio de difusión pública, utilizando imágenes de otra persona, para acosarla o humillarla.

Lo que es evidente –y a ello se refieren la mayoría de las memorias territoriales– es que estos comportamientos son especialmente frecuentes entre menores de edad. De hecho, el concepto de *cyber-bullying* se aplica específicamente al delito de acoso cometido entre iguales y planificado y/o ejecutado en el entorno virtual, en el que se incluyen una pluralidad de conductas tales como hacerse pasar por el menor en redes sociales y, usurpando su identidad, atribuirle comentarios u opiniones que le enfrentan a su grupo de amigas/os y conocidas/os y le aíslan socialmente; difundir por redes sociales rumores falsos sobre comportamientos o actuaciones de la víctima; intimidar al menor a través de WhatsApp, SMS o mensajes de correo electrónico o perseguirle y acecharle a través de internet, etc. En estos casos la difusión *viral* de los mensajes o contenidos y su permanencia en la red por tiempo indefinido; la accesibilidad de la víctima para el agresor por la constante situación de conectividad y las dificultades para contrarrestar o desvirtuar la información lesiva indebidamente difundida determinan la amplificación de los efectos del delito y, por ende, que las consecuencias para el afectado por estos comportamientos resulten extraordinariamente dañinas.

No obstante, y pese al notable esfuerzo realizado por el legislador para definir conductas típicas que permitan actuar penalmente frente a este tipo de comportamientos, seguimos detectando algunas carencias a efectos de poder actuar penalmente, de las que estimamos oportuno dejar constancia.

Concretamente entendemos oportuna la tipificación como delito independiente y de carácter genérico, de la conducta consistente en simular *online* una identidad perteneciente a otra persona de existencia real de forma tal que pueda generar confusión acerca de su efectiva intervención en el proceso comunicativo de que se trate. Son muchos los supuestos en que se suele recurrir este subterfugio para suplantar al menor en los foros o grupos *online* en los que se relaciona con los demás con finalidades diversas que no siempre encajan en los supuestos sancionados en los apartados 1.º 3 y 5.º del citado artículo 172 ter CP, por no responder a las finalidades que se reseñan en los mis-

mos o no servirse el intruso de imágenes del menor sino únicamente de sus datos de identidad. Como también son frecuentes los casos en que los agresores recurren a este medio para acercarse con más facilidad a sus futuras víctimas con fines ilícitos, ganándose su confianza al aparentar que es otro menor amigo o conocido del afectado con el que mantiene relaciones de confianza más o menos intensas.

La tipificación penal de esta conducta parece cada vez más necesaria en atención a la capacidad que ofrecen los sistemas de inteligencia artificial de llevar a efecto estos comportamientos con mayor realismo y, por tanto, con mayores posibilidades de lograr el resultado pretendido.

2.2.3 DELITOS DE RIESGO

No podemos finalizar este apartado sin referirnos, aunque sea someramente, a las nuevas figuras delictivas incorporadas al Código Penal por la disposición final sexta de la Ley Orgánica 8/2021, de 4 de junio, de protección integral de la infancia y adolescencia frente a la violencia. Nos referimos concretamente a los nuevos artículos 143 bis, 156 ter, 189 bis y 361 bis con los que se pretende atajar la difusión a través de las TIC de contenidos específicamente destinados a promover, fomentar o facilitar comportamientos que generan riesgos efectivos para la vida, salud e integridad física de menores de edad o personas con discapacidad o también de aquellos otros que incitan, fomentan o promueven la comisión de delitos contra la libertad e indemnidad sexual de los mismos.

Estas nuevas figuras, particularmente las de los artículos 143 bis, 156 ter y 361 bis, responden a la necesidad de reforzar la protección de las y los integrantes de estos colectivos frente a quienes, por inexplicables razones, aprovechando su fragilidad y/o falta de madurez, intentan influir, sobre ellas/os para que realicen determinados comportamientos en su propio perjuicio.

Hace años se viene detectando la proliferación en la red de páginas, blogs o sitios web, algunos dirigidos específicamente a niños, niñas o adolescentes, que difunden entre los menores prácticas alimenticias, técnicas de ingesta o eliminación de alimentos o el consumo de determinados productos o preparados que con el pretexto de ayudarles a mejorar su apariencia física –cuestión de interés prioritario para muchos de ellos en determinadas etapas de la infancia y adolescencia– influyen negativamente en sus destinatarias/os provocando trastornos obsesivos relacionados con la propia percepción de la imagen y aspecto corporal y que pueden provocar alteraciones graves en

la conducta alimentaria de los afectados y, en consecuencia un riesgo relevante para su salud.

La preocupación por las facilidades con las que los usuarios/as más jóvenes pueden acceder a estos foros venía siendo denunciada por numerosas asociaciones civiles que demandaban una respuesta contundente del legislador para evitar sus graves consecuencias en este sector de la población especialmente propenso, por su edad y grado de madurez, a dejarse influir por este tipo de mensajes.

En otras ocasiones los contenidos que se difunden *online* están relacionados con juegos consistentes en desafíos, conocidos como *retos virales*, que animan a menores y adolescentes a demostrar su valentía y capacidad personal de superación asumiendo voluntariamente la práctica de determinadas conductas o la ejecución de acciones de riesgo, algunas de las cuales pueden poner en serio peligro su integridad física o incluso su vida. Entre ellos fue tristemente popular hace varios años el conocido juego de la ballena azul *Blue Whale*, que se extendió rápidamente a través de internet y redes sociales, y consistía en incitar al niño o niña a someterse a ciertos retos o a ejecutar pruebas físicas cada vez más peligrosas hasta provocar el suicidio y que, en ocasiones, derivó en el fallecimiento de algunos de los participantes. En otros casos, como *la cicatriz francesa o el reto de la pastilla*, se incita a las/os menores a la autolesión o al consumo de ansiolíticos para mostrarse ante el grupo y con ello a alardear de su valentía y capacidad para soportar el dolor o mantenerse mayor tiempo despiertos. No faltan tampoco otros juegos como *la caza del pijo*, en el que resulta ganador quien consiga presentar el mayor número de grabaciones de vídeo obtenidas con ocasión de agresiones efectuadas por el propio menor o menores a personas que, a su entender, reúnen esas características.

Este tipo de retos virales se difunden con rapidez en las redes sociales y tienen una gran capacidad de penetración en los círculos de relación de los más jóvenes pues no en vano están planificados precisamente para aprovechar la falta de madurez y, por ende, escasa percepción del riesgo de sus destinatarias/os y provocar en ellos actuaciones o comportamientos motivados por el interés en lograr un mayor y mejor reconocimiento y una más completa aceptación del grupo en el que se integran.

En uno y otro caso la investigación de este tipo de actividades ilícitas presenta dificultades serias porque, en no pocas ocasiones, quienes gestionan los sitios web desde los que se coordina y dirige el juego, radican fuera de nuestras fronteras por lo que la identificación de sus responsables depende de instrumentos de cooperación internacional que no siempre resultan efectivos.

No obstante, la posibilidad que contemplan todos estos preceptos de adoptar medidas para evitar que dichos contenidos permanezcan accesibles en la red, incluso con carácter cautelar, con amparo en el párrafo 2.º del artículo 13 LECrim, en su redacción dada por la LO 10/2022, de 6 de septiembre, ya supone un paso importante para minimizar el riesgo que genera su difusión.

La preocupación del área de especialización en criminalidad informática de la Fiscalía General del Estado en esta materia ha determinado que hagamos extensivo el trámite de supervisión de acusaciones por la Unidad Especializada a los escritos de calificación que se vayan elaborando en referencia a estas conductas. Con ello pretendemos detectar de primera mano, y desde el inicio de su aplicación práctica, las cuestiones jurídicas que se vayan suscitando, así como recabar información detallada sobre todo ello, con el objetivo de poder elaborar en momento posterior algún documento de la Fiscalía General en el que se fijen los criterios esenciales que han de tenerse en cuenta en la aplicación práctica de estas nuevas figuras delictivas.

Aun cuando nuestra experiencia práctica en la interpretación y aplicación de estos tipos penales es todavía escasa, se encuentran ya en curso algunos expedientes, con origen, en ocasiones, en diligencias de investigación del Ministerio Fiscal, dirigidos contra personas responsables de blogs en los que se difundían contenidos de estas características y cuyo cierre y/o bloqueo cautelar ha sido solicitado por el MF a la autoridad judicial competente al amparo del artículo 13 LECrim ya mencionado.

2.2.4 DELITOS CONTRA LA LIBERTAD SEXUAL

Todas las reflexiones antes indicadas acerca del efecto perverso que el desarrollo tecnológico está teniendo en las agresiones ilícitas contra los más jóvenes, tienen sin duda un reflejo muy evidente en los comportamientos que atentan contra su libertad sexual. Es un hecho incuestionable que esa profunda penetración de las tecnologías en las comunicaciones interpersonales, a la que nos referíamos anteriormente, está facilitando extraordinariamente el acercamiento *online* a niñas/os y adolescentes con objetivos de índole sexual, al igual que la elaboración, distribución y puesta a disposición de terceros de material de abuso sexual infantil (en adelante, CSAM), por auténticos depredadores sexuales.

Esta situación se ha ido agravando con el paso de los años, a medida que se intensificaba la digitalización de la actividad social, económica y política y con ello el recurso por parte de las y los meno-

res a las tecnologías y a internet en su ámbito de relación personal y en el desempeño de todo tipo de actuaciones y tareas, entre otras, las relacionadas con su proceso educativo y de formación personal. Además, también ha influido en los últimos años la particular situación generada por la COVID-19 y el obligado confinamiento de una buena parte de la población mundial. De esta realidad dan cuenta múltiples indicadores nacionales e internacionales con origen en organismos públicos y privados, siendo especialmente relevante a estos efectos la Comunicación publicada por la Comisión Europea el 24 de julio de 2020 y dirigida al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones con el objetivo de articular una Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores.

En dicha Comunicación, con apoyo en otros documentos de interés como el informe publicado por Europol el 19 de junio del mismo año bajo el título *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*, la Comisión Europea hace una llamada de atención acerca del riesgo que implica para la infancia y la adolescencia el acceso generalizado a la red, en muchas ocasiones, sin supervisión por sus padres y o tutores, lo que les hace especialmente vulnerables a ataques contra su libertad sexual. Se refiere también esta Comunicación a la incidencia que están teniendo los avances técnicos y científicos en la elaboración y en tráfico mundial de CSAM y como los delincuentes se sirven de las capacidades de acción que ofrecen dichas herramientas para producir *online* material de esa naturaleza, obligando a aquellos con los que contactan a participar en actividades sexuales en emisiones en directo o a intercambiar con sus agresores o agresoras contenidos íntimos de carácter pornográfico. Los datos que se ofrecen en esa Comunicación no pueden ser más expresivos, pues revelan un drástico aumento de las denuncias por abuso sexual en línea en el territorio comunitario que han evolucionado *de 23.000 en 2010 a más de 725.000 en 2019*, cifras que incluyen notificaciones de más de 3 millones de imágenes y vídeos de contenido pedófilo.

A efectos de valorar la incidencia actual del comercio *online* de contenido CSAM tiene un especial interés la información proporcionada por el *National Center for Missing and Exploited Children* (NCMEC) organización privada sin ánimo de lucro con sede en EE. UU. que opera una *CyberTipline* en la que se reciben notificaciones sobre sospechas de material relativo a explotación sexual en línea que, posteriormente, dicha organización traslada a las autoridades competentes del país en el que tiene origen la difusión por si esti-

maran oportuno iniciar la correspondiente investigación y persecución penal. El volumen de notificaciones recepcionadas a través de dicha *CyberTipline* –importante indicador de dicho tráfico ilícito– se está incrementando de forma muy preocupante en los últimos años, habiéndose alcanzado a nivel mundial en 2023, la elevadísima cifra de 36,2 millones, lo que supone un incremento de más de un 12 % respecto de los datos obtenidos por igual concepto en 2022 y de casi un 100 % respecto de los 18,4 millones de notificaciones contabilizadas en 2018. En igual sentido el informe de la Fundación ANAR publicado en los primeros meses del presente año 2024 da cuenta de la presencia de las tecnologías en un 43 % de los supuestos de agresión sexual a menores y adolescentes, particularmente en los fenómenos de *childgrooming* o *sexting* no consentido.

La experiencia adquirida por el Ministerio Fiscal en la actuación frente a las manifestaciones *online* de estas graves actividades delictivas confirma lamentablemente estas mismas conclusiones. El seguimiento e intervención de quienes integramos el área de especialización en criminalidad informática del Ministerio Fiscal español en la investigación y el enjuiciamiento de los delitos que se planifican y ejecutan en el ciberespacio y, más concretamente, las funciones encomendadas a su Unidad central para la supervisión de determinados expedientes y de los escritos de acusación presentados con ocasión de los mismos –tal y como resulta de la Instrucción 1/2015 FGE y, en particular, de la Instrucción 2/2011, *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías*– nos coloca en una situación privilegiada para analizar y valorar la problemática que nos ocupa.

Esta circunstancia nos está permitiendo constatar el preocupante incremento no solo cuantitativo sino también cualitativo de dichas agresiones, favorecidas por la presencia constante en la red de jóvenes, cada vez de menor edad, desprevenidos frente a los riesgos que asumen y sin control suficiente por parte de sus progenitores, cuidadores o tutores. De ello se aprovechan los agresores sexuales para aproximarse a ellos/as, directamente si disponen de los datos para contactar, o acudiendo a los foros o chats que los mismos frecuentan, ocultando generalmente su identidad y haciéndose pasar por personas de edad similar a la víctima para, de esa forma, ganar su confianza y generar un marco de camaradería y complicidad que les facilite sus criminales y perversos propósitos.

Entablada esa relación de confianza los y las agresores sugieren a sus víctimas, con justificaciones diversas, la realización de actos de exhibición sexual o la entrega de fotografías o vídeos de similar natura-

leza que, una vez en su poder, utilizan para coaccionar al afectado/a y exigirle acciones o comportamientos que atentan cada vez más gravemente contra su libertad sexual, logrando una situación de dominación y control sobre el menor de la que le resulta difícil escapar y que puede llegar a prolongarse por periodos temporales relativamente extensos, afectando muy gravemente a su normal desarrollo y evolución.

Por otra parte, y con relativa frecuencia, el delincuente sexual diversifica su acción criminal simultáneamente respecto a una pluralidad de personas, de forma tal que no es extraño que una investigación originariamente centrada en la agresión a un menor derive en el descubrimiento de decenas de perjudicados/as por la actuación de un mismo agresor.

La alta definición y la calidad de la imagen en las comunicaciones digitales, la conectividad permanente que ofrecen las tecnologías y ese uso habitual de las mismas por parte de los niños/as al que nos venimos refiriendo, han determinado que este tipo de actividades que atentan contra la libertad sexual de la infancia y la adolescencia no solo se hayan ido desplazando a la red sino que se hayan visto favorecidas y facilitadas por esas mismas circunstancias, lo que está dando lugar a ese incremento progresivo al que nos referimos y, como consecuencia de ello, a una cierta normalización de estas situaciones y a la participación voluntaria, al menos ocasionalmente, de los menores en ellas.

En la actualidad se planifican y ejecutan *online*, de forma sencilla y ágil, todo tipo de conductas ilícitas de esta naturaleza, el *child-grooming*, los actos de provocación y exhibición sexual, las agresiones *online* –incluyendo las relacionadas con la introducción de objetos– o los espectáculos exhibicionistas y pornográficos en sesiones públicas directas que pueden presenciar en *streaming* un número indeterminado de personas con independencia del lugar en que se encuentren.

Y lo mismo ocurre con las actividades relacionadas con la elaboración, distribución y posesión de contenidos CSMA que se benefician de las extraordinarias prestaciones de dispositivos móviles cada vez más sofisticados y de mayor calidad técnica que permiten a sus poseedores no solo obtener grabaciones audiovisuales o imágenes de abuso en cualquier circunstancia y sin necesidad de especial pericia sino también trasladarlas rápidamente por múltiples canales de comunicación, ya sea a personas previamente determinadas o, de forma general e indiscriminada, a quienes tengan interés en ello. Estas indudables ventajas en la producción y tráfico de material ilícito de carácter sexual se van a ver potenciadas extraordinariamente en un futuro ya muy próximo con el aprovechamiento de los sistemas de inteligencia

artificial, circunstancia de la que ya hemos tenido algún ejemplo en nuestro país a propósito de la elaboración y difusión de lo que se define como pornografía virtual.

2.2.4.1 *Problemas relacionados con la investigación de estas conductas*

La preocupante situación que estamos comentando y su incidencia en las libertades y derechos de los más jóvenes se agrava significativamente por las dificultades que presenta la investigación de estas conductas y, en consecuencia, el ejercicio de la acción penal contra sus responsables. A ello se refería expresamente la Comunicación antes comentada de la Comisión Europea de 24 de julio del año 2020, en la que se dejaba constancia de los inconvenientes que a dichos efectos se derivan del desarrollo de nuevas técnicas de transmisión de contenidos y de mecanismos de encriptación o cifrado de extremo a extremo que, si bien contribuyen a proteger la privacidad de las comunicaciones en la red, constituyen a la vez importantes obstáculos para la investigación criminal.

Nuestra percepción al respecto es coincidente con el análisis y las reflexiones que realiza la Comisión Europea. Constantemente se articulan en el entorno virtual inéditos mecanismos para la transmisión y el acceso a contenidos de forma segura y anónima. La mensajería instantánea, el cifrado, el uso de la red Tor, o la visualización en *streaming* de archivos digitales almacenados en la nube sin necesidad de descarga, constituyen medios a través de los cuales es posible acceder, adquirir, compartir o difundir material de abuso sexual infantil con mayores garantías de impunidad ya que el incremento en la seguridad e impenetrabilidad de la comunicación o del contenido al que se accede que derivan de la utilización de dichos recursos, acrecienta también las dificultades para la investigación criminal.

La respuesta penal sancionadora frente a los ilícitos *online* que nos ocupan se encuentra también condicionada por el hecho constatado de que muchas de estas agresiones no sean objeto de denuncia por parte de los perjudicados/as, al tratarse de acciones planificadas y ejecutadas en la clandestinidad y en las que las víctimas, frecuentemente de muy corta edad, ni tan siquiera son conscientes de la agresión sufrida. De hecho, una buena parte de las investigaciones suelen iniciarse a partir de comunicaciones de ciudadanas/os que detectan material CSAM en la red o de las notificaciones recibidas de organismos como NCMEC o de los cuerpos policiales de otros países que

localizan, con ocasión de sus propias pesquisas, información sobre hechos de esta naturaleza acaecidos en nuestro país. Eventualmente, en otras ocasiones, son los padres, tutores, profesores o allegados de las víctimas quienes, de forma casual, descubren la agresión de que están siendo objeto sus pupilos y dan cuenta de ello a los órganos de la jurisdicción penal. Esta circunstancia determina que en un número de supuestos imposible de concretar la agresión no llegue a ser detectada, por lo que la cifra oculta de criminalidad en este ámbito es en la actualidad incalculable. Es por ello que cualquier iniciativa de carácter legislativo u operativo, orientada a mejorar la capacidad de actuación frente a estas gravísimas manifestaciones criminales exige necesariamente –y en ello insisten reiteradamente las propuestas internacionales sobre la materia– fomentar y facilitar la denuncia de estos comportamientos por parte de todos los ciudadanos/as y particularmente de aquellos que por razón de sus funciones o actividad profesional mantienen contactos más cercanos con niños, niñas y adolescentes, a cuyo fin la sensibilización y concienciación social acerca de la gravedad y peligrosidad de estas agresiones resulta esencial.

Toda esta situación a la que nos venimos refiriendo determina que la endémica carencia de medios personales y materiales en la lucha contra la ciberdelincuencia tenga en este ámbito concreto unas consecuencias especialmente graves. Desde nuestro punto de vista sería imprescindible ampliar las unidades policiales dedicadas específicamente a esta materia y dotarlas de los mejores medios materiales –los más avanzados y sofisticados– y de la formación especializada que resulta imprescindible para abordar la complejidad técnica que presenta el esclarecimiento de estos delitos; al igual que es necesario mejorar las capacidades en informática forense, dotando de mayores medios a los laboratorios de criminalística o policía científica y/o diseñando un sistema más adecuado y ágil en la elaboración de informes técnico-policiales o periciales. Es incontestable que la Fiscalía tiene un importante peso en esta función, debiendo aprovechar al máximo los mecanismos legales a nuestro alcance y otorgar la prioridad necesaria a las diligencias de investigación imprescindibles en estos procedimientos para evitar dilaciones indebidas que ponen en riesgo la posterior disponibilidad de las evidencias del delito.

2.2.4.2 *Tratamiento normativo de los delitos online contra la libertad sexual de los menores.*

La actividad delictiva contra la libertad sexual de los menores viene siendo desde hace años motivo de una especial atención en todos los países y también en los organismos e instituciones internacionales y ha dado lugar a la publicación de importantes instrumentos jurídicos con el objetivo de articular mecanismos legales que permitan actuar penalmente frente a estas conductas, tanto en el ámbito interno como, de forma coordinada, más allá de los límites fronterizos de los Estados.

En relación con ello han de reseñarse la Convención para la Protección de los Derechos del Niño, adoptada por la Asamblea General de Naciones Unidas el 20 de noviembre de 1989, así como el Protocolo Facultativo de ese mismo Convenio relativo a la venta de niños, prostitución infantil y utilización de los niños en actividades de pornografía infantil, en vigor desde el mes de febrero de 2002. Por su parte, en nuestro entorno más próximo son de obligada mención, en el marco del Consejo de Europa, la Convención de Lanzarote, de 25 de octubre de 2007, para la protección de los niños contra la explotación y el abuso sexual, y también la Convención de Budapest contra la Ciberdelincuencia, de 23 de noviembre de 2001, en particular su artículo 9 sobre delitos relacionados con la pornografía infantil. Ambas convenciones han sido ratificadas por España y la influencia de esta última en la actual tipificación en nuestro código penal de las conductas relacionadas con pornografía infantil es más que evidente, como también lo es el hilo conductor del artículo 23 de la Convención de Lanzarote en la definición de la figura típica del *child grooming*.

A su vez en el espacio geográfico común de la Unión Europea, hace casi 20 años, que la Decisión Marco 2004/68/JAI del Consejo de 22 de diciembre, llamó la atención sobre la incidencia de las nuevas tecnologías en la planificación y desarrollo de este tipo de actividades ilícitas. A su vez, la más reciente Directiva 2011/93/UE del Parlamento y del Consejo, de 13 de diciembre, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil, asumiendo ese mismo planteamiento, instó a los Estados miembros a potenciar, mediante una legislación adecuada, la investigación y enjuiciamiento de este tipo de actividades ilícitas *habida cuenta de la dificultad de las víctimas para denunciar los abusos y del anonimato de los delincuentes en el ciberespacio* y también a proporcionar *instrumentos de investigación eficaces* a los responsables de la investigación y del enjuiciamiento de estas conductas.

Con ese objetivo, esta Directiva europea articula su contenido en tres grandes líneas de actuación: i) definición de infracciones penales, sanciones y consecuencias accesorias; ii) impulso y fortalecimiento de las actuaciones relacionadas con la investigación de dichas conductas y iii) medidas de prevención, asistencia, apoyo y protección de los y las menores. La conjunción de las medidas desarrolladas en esos tres grandes apartados configura un amplio y detallado marco de protección de las víctimas de las acciones ilícitas que analizamos, muchas de las cuales se planifican y ejecutan actualmente en el entorno virtual.

En el ámbito interno, el legislador español ha ido incorporando al ordenamiento jurídico muchas de las previsiones recogidas en la Directiva (UE) 2011/93, principalmente con ocasión de la reforma del Código Penal derivada de la LO 1/2015, de 30 de marzo, y también –en lo que aquí interesa– de la que se llevó a efecto en el citado texto normativo y en la Ley de Enjuiciamiento Criminal por las disposiciones finales primera y sexta de la LO 8/2021, de 4 de junio, de protección integral de la infancia y la adolescencia frente a la violencia. También han de citarse en relación con ello las modificaciones que se introdujeron en nuestra norma procesal por la LO 13/2015, de 5 de octubre. De esta forma el legislador ha ido ofreciendo progresivamente soluciones legales al problema que nos ocupa a partir de esas tres líneas de actuación que define la Directiva europea.

– Así, al primero de los objetivos responden, entre otras previsiones, la incorporación en el artículo 189.2 CP de un concepto de pornografía infantil, que sigue esencialmente los parámetros del artículo 2 de la citada norma europea y del artículo 9 de la Convención de CoE sobre Ciberdelincuencia en el que se incluye específicamente como material ilícito el elaborado artificialmente. En la misma línea está la tipificación del acceso *online* a material de abuso sexual infantil por medios tecnológicos en el artículo 189.5 CP y del *childgrooming*, en el actual artículo 183 CP precepto este último que trae causa del artículo 6 de la Directiva y del artículo 23 de la Convención de Lanzarote del Consejo de Europa. También y con la evidente finalidad de garantizar una mayor protección a las víctimas de estas conductas, nuestro Código Penal, siguiendo los parámetros de la norma europea, contempla en su art. 189.8 medidas para evitar que los contenidos ilícitos permanezcan accesibles en la red.

No menos importante es la previsión de la obligación y/o posibilidad de imponer penas de inhabilitación especial para cualquier profesión, actividad u oficio, sea o no retribuido, que conlleve contacto con

personas menores de edad y otras, como privación de la patria potestad o inhabilitación para el ejercicio de la misma o de la tutela, curatela o acogimiento a las que se refiere expresamente el vigente artículo 192.3 CP.

Incluso el legislador español ha ido más lejos en la protección penal de la infancia y la adolescencia frente a este tipo de agresiones –adelantándose en este aspecto a las propuestas en curso en el territorio comunitario– con la tipificación en el artículo 189 bis del Código Penal de *la distribución o difusión pública a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II y IV del presente título.*

– Por otra parte, el impulso y fortalecimiento de la investigación de estas conductas, que promueve la Directiva en su segunda línea de acción, se focaliza en la necesidad de facilitar/promover su denuncia y en mejorar las técnicas y mecanismos de investigación criminal. A dicho fin el legislador español llevó a efecto por LO 13/2015 de 5 de octubre una importante modificación de la LECrim que incorpora en nuestra norma procesal las potentes medidas de investigación tecnológica que se recogen en los capítulos IV a X del título VIII del libro III LECrim, inspiradas en buena medida en la Convención de Budapest del CoE, y contempla en su artículo 282 bis apartado 6, la técnica del agente encubierto *online*, herramienta de extraordinaria utilidad para la investigación de ilícitos en el entorno virtual y muy especialmente de los relacionados con las agresiones sexuales de una u otra naturaleza a personas menores de edad.

– Por otra parte, también se han ido adoptando medidas para favorecer el «afloramiento» de estas graves conductas y la posibilidad de persecución penal de las mismas. A ello obedecen la ampliación en los plazos de prescripción de estos delitos (arts. 131 y 132 CP) o el establecimiento de líneas abiertas (*hotline*) para facilitar la denuncia por parte de los ciudadanos de los contenidos CSAM que detecten con ocasión de su navegación por el ciberespacio. En relación con este último aspecto hemos de recordar la importante implicación del Ministerio Fiscal español a través de la intervención de su Unidad Especializada contra la Criminalidad Informática en el Protocolo suscrito en diciembre de 2022 con el Instituto Nacional de Ciberseguridad (INCIBE) –miembro español de la red INHOPE– para la recepción de las notificaciones recibidas de otros países sobre contenidos CSAM a efectos de su investigación y retirada de la red.

– Finalmente y en referencia al tercero de los aspectos que se abordan en la Directiva europea, nuestra normativa interna ha ido acogiendo, en los últimos años, medidas legales para reforzar la protección y el apoyo integral a las víctimas de estas gravísimas agresiones y a minimizar en la medida de lo posible sus efectos lesivos. A ello responden, entre otras, la incorporación en la Ley de Enjuiciamiento Criminal del artículo 449 ter y las modificaciones operadas en los artículos 703 bis, 707 y concordantes del mismo texto legal orientados a garantizar los derechos de los y las menores con ocasión de su intervención en procesos penales, evitando los efectos de una *victimización secundaria*, así como también la modificación del artículo 13 de la LECrim, derivada de la disposición final primera de la LO 10/2022 de 6 de septiembre de *garantía integral de la libertad sexual*, que extiende a cualquier clase de delitos la posibilidad de acordar cautelarmente las medidas orientadas a hacer inaccesibles *online* contenidos de naturaleza ilícita.

2.2.4.3 *Nuevas iniciativas en el marco comunitario frente a los delitos contra la libertad e indemnidad sexual de los menores*

No obstante, y pese al acierto y trascendencia de los avances legislativos que se acaban de exponer, no ha sido posible frenar el vertiginoso incremento de estas graves y peligrosas conductas criminales, lo que ha determinado algunas iniciativas comunitarias actualmente en curso que se enmarcan en la *Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores*.

Dicha Estrategia tiene su origen la Comunicación que en fecha 27 de julio de 2020 dirigió la Comisión al Parlamento, al Consejo y a los altos organismos de la UE¹ en la que se reflexiona acerca de la problemática detectada en esta materia a la vista del *drástico aumento de denuncias por abusos sexuales de menores en línea en la Unión Europea* y con la que se pretende, a nivel comunitario, *ofrecer un marco para formular una respuesta firme y exhaustiva a estos delitos tanto en línea como sin conexión a internet*. A dicho fin esta Estrategia se articula en torno a determinadas iniciativas que se están desarrollando, debidamente coordinadas con otros planes de actuación, entre los años 2020 y 2025 y que resumimos a continuación.

¹ COM (2020)607 final Bruselas 24.7.2020

- a) La primera de ellas es la de adoptar y elaborar el marco jurídico adecuado para proteger a la infancia y la adolescencia frente a los nuevos riesgos que están surgiendo al hilo de los avances científicos y técnicos.

A este respecto la Estrategia pone el acento en la necesidad de impulsar la plena implementación y aplicación en los Estados miembros de la Directiva (UE) 2011/93 en todos los aspectos a los que hemos hecho referencia y, al tiempo, evaluar si la actual normativa resulta adecuada y suficiente en atención a los cambios sociales y tecnológicos de la última década.

Con ocasión de esta reflexión, el pasado día 6 de febrero se ha presentado por la propia Comisión Europea, una propuesta de modificación de la citada Directiva con la que se pretende redefinir algunas de las herramientas legales ya previstas e incluir otras nuevas para poder actuar con mayor efectividad frente a inéditas formas de agresión que han ido surgiendo en el entorno virtual. Por ello en el documento se desarrollan iniciativas tales como la ampliación de la definición del material de abuso sexual infantil, para dar entrada a los contenidos –desconocidos hasta el momento– que puedan generarse con el uso de sistemas de inteligencia artificial; la elevación de las penas en determinados supuestos; el incremento de los plazos de prescripción de estos delitos de tal forma que las víctimas dispongan de mayor margen temporal para denunciarlos o la posibilidad de tipificar penalmente la gestión de infraestructuras en línea que permitan o fomenten el abuso o la explotación sexual de los menores.

Pero, sin duda, la actuación eficaz contra estas conductas demanda también de la articulación de instrumentos legales que faciliten su investigación y, por ende, la persecución penal y enjuiciamiento de sus responsables. A ello responden otras iniciativas que si bien tienen un ámbito de aplicación mucho más abierto inciden igualmente de forma muy favorable en la lucha contra las agresiones sexuales *online*. Entre ellas ha de citarse por su especial interés, el conocido como *paquete e-evidencie* –Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544– sobre prueba electrónica en procesos penales, publicado en el DOUE de 28 de julio de 2023, y cuya importancia a efectos de la investigación y enjuiciamiento de los ciberdelitos es incuestionable pues va a facilitar considerablemente la obtención, mediante petición directa a los propios proveedores de servicios, de aquellas evidencias electrónicas almacenadas en otros Estados miembros que resulten imprescindibles para el éxito de las investigaciones y procedimientos penales relativos a ilícitos ejecutados en el ciberespacio.

También se enmarcan en ese mismo objetivo la ampliación, en virtud del Reglamento (UE) 2022/991 de 8 de junio, de la capacidad de Europol para cooperar con entidades privadas a efectos de obtención de datos con fines de investigación, o los trabajos en marcha sobre la propuesta de un Reglamento sobre privacidad y comunicaciones electrónicas, llamado a sustituir a la actual Directiva 2002/58/CE sobre ese mismo tema.

- b) Otro de los grandes objetivos de la Estrategia es el de reforzar la actuación de las fuerzas y cuerpos de seguridad y potenciar la cooperación entre las partes interesadas.

Como ya se ha indicado, uno de los aspectos en los que se insistía en la Comunicación de la Comisión de julio de 2020 era la necesidad de que los cuerpos policiales dispusieran de una preparación adecuada –*aptitudes digitales*– y de los medios materiales necesarios para poder actuar frente unas manifestaciones criminales cada vez más sofisticadas y difíciles de esclarecer.

A dicho fin, el documento contiene determinadas sugerencias a los Estados tales como la puesta en funcionamiento de unidades especializadas en este tipo de investigaciones, dotándolas, con apoyo financiero de la propia UE, de los medios personales y materiales necesarios y de capacidades técnicas de vanguardia acordes con el progreso tecnológico; fomentar y facilitar el intercambio de información de inteligencia en el territorio de la Unión; impulsar la actuación coordinada para la identificación de menores víctimas de estas conductas y, en definitiva, promover la colaboración entre los Estados miembros en la lucha contra el abuso sexual de menores a través del Centro Europeo de Ciberdelincuencia (EC3) de Europol.

La Estrategia también hace referencia en este apartado a las ventajas que ofrece la investigación secreta *online* y la infiltración policial y propone trabajar en la articulación de herramientas de esta naturaleza a nivel comunitario, con pleno respeto a los derechos fundamentales y a los principios y valores que inspira el funcionamiento de la UE, a cuyo fin aboga, entre otras medidas, por la puesta en funcionamiento de un *Laboratorio para la Innovación* centrado precisamente en el desarrollo y experimentación de dichas herramientas.

- c) Mejorar la capacidad de los Estados para la protección de los menores mediante la prevención de este tipo de agresiones.

En el documento se deja igualmente constancia de la conveniencia de adoptar programas de prevención y de establecer una red comunitaria de expertos e investigadores para respaldar y apoyar a los Estados miembros en orden a la adopción en sus respectivos territorios de medidas útiles y eficaces para prevenir este tipo de delincuencia y con ello conjurar los riesgos a los que se encuentran expuestos los niños, niñas y adolescentes en el entorno virtual.

Con dicho objetivo se analizan algunas posibles iniciativas tales como la detección de factores de riesgo y de las circunstancias que actúan como detonantes de estas agresiones; la preparación de campañas mediáticas de sensibilización social; la elaboración de materiales que informen a la ciudadanía acerca de la gravedad de estas conductas y de sus perniciosos efectos; el diseño de programas de formación especializada para los profesionales que trabajan habitualmente con menores de edad en cualquier área de actividad... etcétera. Particularmente la Estrategia hace hincapié en la importancia de concienciar y capacitar a los propios menores en el uso seguro de internet y de mantenerles informados de forma completa, detallada y adecuada a su edad y estado de desarrollo acerca de los recursos disponibles a través de las líneas de ayuda y de denuncia.

- d) Creación de un centro europeo de prevención y lucha contra el abuso sexual de menores en línea y fuera de línea.

Desde el año 2019 el Parlamento Europeo viene demandando la creación de un organismo central que asuma la coordinación de las actuaciones que se lleven a efecto en el ámbito comunitario en esta materia y, al tiempo refuerce la labor de los Estados miembros en relación con ello. Dicho Centro se plantea con un triple objetivo: i) garantizar la colaboración entre los distintos cuerpos policiales nacionales, evitando la duplicidad de esfuerzos (gestionar una base de datos única sobre pornografía infantil, coordinación en la investigación y en la retirada de material ilícito identificado... etcétera); ii) apoyo a los Estados en la adopción de medidas de prevención multidisciplinarias que resulten eficaces para disminuir la prevalencia de abusos sexuales de menores en el territorio comunitario, y iii) auxilio y asesoramiento a los Estados en el establecimiento de mecanismos de apoyo y asistencia a las víctimas.

- e) Aprovechar y fomentar la colaboración de los proveedores de servicios del sector privado para garantizar la protección de los niños, facilitando la denuncia y notificación de los abusos sexuales a menores que detecten en sus servicios y aplicaciones.

En relación con este aspecto, que constituye un eje esencial en cualquier planteamiento frente a la ciberdelincuencia, han de reseñarse dos grandes iniciativas desarrolladas en los últimos años. La primera de ellas, ya culminada, es la publicación del Reglamento (UE) 2022/2065, de 19 de octubre, relativo al mercado único de servicios digitales, en vigor desde el 17 de febrero del presente año, en el que se fijan con claridad las obligaciones que corresponden a los distintos servicios de la sociedad de la información, como mercados en línea, redes sociales o plataformas de intercambio de contenidos, tanto en los aspectos relacionados con la transparencia de sus operaciones como en lo relativo al cumplimiento de las órdenes emanadas de las autoridades competentes. Entre ellas, y en lo que aquí interesa, las relativas a la retirada de contenidos ilícitos (art. 9) o a las peticiones de entrega de información dictadas por las autoridades judiciales o administrativas en el ejercicio de sus competencias (art. 10) y también las obligaciones establecidas sobre notificación de sospechas acerca de la comisión de ilícitos penales o las orientadas a la protección en línea de los menores de edad (art. 28).

Además, y en segundo lugar, no podemos dejar de mencionar los esfuerzos que se están realizando a nivel comunitario para regular la utilización por los proveedores de servicios de determinadas tecnologías de tratamiento de datos personales y de otro tipo cuando dicha actuación resulte necesaria para la detección, en sus propios servicios, de abusos sexuales de menores en línea, así como para la denuncia de material de esa naturaleza y la retirada del mismo de sus servicios y aplicaciones. Con dicho objetivo se publicó en el año 2021 el vigente Reglamento (UE) 2021/1232 de 14 de julio en el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE, al tiempo que se está trabajando en un Reglamento en el que se pretende abordar definitivamente esta materia y cuya preparación ha centrado buena parte de la actividad de la Presidencia española de la Unión Europea.