8. CRIMINALIDAD INFORMÁTICA

8.1 **Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2020**

Es obligado en esta memoria profundizar en el análisis de los datos estadísticos obtenidos en el año 2020 con el objetivo de valorar de forma más detallada y precisa la evolución de las distintas manifestaciones criminales en el ciberespacio y la capacidad de reacción y respuesta al respecto de los órganos de la jurisdicción penal y de las Fuerzas y Cuerpos de Seguridad y, al tiempo, intentar definir futuras líneas de actuación que mejoren la eficacia del Estado de Derecho ante un fenómeno criminal extraordinariamente complejo, muy versátil y que puede alcanzar niveles preocupantes de gravedad y peligrosidad para los derechos de los/as ciudadanos y ciudadanas de interés general.

En primer término, es preciso recordar que la información estadística que se recoge en este apartado es el resultado de la recopilación por parte de esta Unidad Especializada de los datos facilitados por los propios órganos territoriales de la institución acerca de los procedimientos judiciales y diligencias de investigación incoados en el año y también sobre los escritos de acusación presentados por la Fiscalía en dicho periodo anual por hechos ilícitos competencia de esta área de especialización tal y como viene delimitada en la Instrucción 2/2011 de la FGE *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías.*

Del análisis de esos datos se colige que en el año 2020 se incoaron en el conjunto del Estado un total de 16.914 procedimientos judiciales para la investigación y enjuiciamiento de hechos susceptibles de tipificarse en las categorías que nos ocupan. Este resultado no solo da cuenta del incremento en un 28,69% en el volumen anual de procedimientos incoados, que en 2019 sumaron 13.143, sino que, además, confirma la tendencia ascendente que venimos constatando en relación con los ciberdelitos desde la puesta en funcionamiento de esta área de especialización en julio del año 2011.

Si tomamos como punto de partida los resultados del año 2017 –anualidad en la que se consolidan los efectos de la reforma operada en el art. 284 LECrim por la Ley 41/2015, que condiciona el traslado efectivo de atestados a las autoridades judiciales a la existencia de autor conocido– la progresión del fenómeno criminal que nos ocupa es evidente. Así, en 2017 se registraron en la Fiscalía un total de 6.676

procedimientos judiciales por delitos competencia de esta área de especialización, cifra que se incrementó en un 35,84% en el año 2018, alcanzando la de 9.069 al finalizar dicho periodo anual. Esta progresión alcista tomó mayor fuerza en 2019, en que el dato de nuevas incoaciones ascendió a 13.143 con un repunte de casi un 45% respecto de año anterior, si bien, como ya adelantamos, el ritmo de crecimiento se ha moderado significativamente entre los años 2019 y 2020 al situarse en un 28,69%. Posiblemente en este resultado haya influido la situación generada con ocasión de la pandemia y por ende la adopción de medidas de confinamiento particularmente estrictas en algunos periodos, lo que sin duda habrá tenido su reflejo tanto en el traslado de atestados/denuncias a los órganos judiciales y al Ministerio Fiscal como en el normal desenvolvimiento de la actividad de estos últimos y también, en cierta medida, habrá perturbado las labores de investigación de los cuerpos policiales. La valoración adecuada de estas incidencias hemos de posponerla a un futuro próximo, cuando hayamos logrado «poner al día» las indagaciones y pesquisas pendientes sobre la pluralidad de hechos presuntamente ilícitos que, habiéndose cometido durante ese periodo, no han sido denunciados y/o investigados hasta tiempo después. Por el momento solo pretendemos dejar constancia de que, pese a dichas anomalías, se mantiene la tendencia ascendente en los datos sobre la actividad delictiva *online* que, probablemente, seguirá creciendo cada vez con más fuerza en los próximos años.

Sin perjuicio de todo ello, antes de detenernos en la información relativa a las distintas manifestaciones criminales, resulta obligado efectuar diversas consideraciones, imprescindibles para la adecuada valoración de las cifras que ofrecemos. En primer término ha de recordarse que en esta memoria únicamente se analiza y valora la información referida a procedimientos o investigaciones que se encuentran bajo el control de los órganos judiciales y/o del Ministerio Fiscal. Son numerosísimas las denuncias o hechos presuntamente delictivos que llegan a conocimiento de los cuerpos policiales y que no son comunicados a las autoridades judiciales por falta de autor conocido, por mor de lo dispuesto en el artículo 284 LECrim. A falta de información sobre el año memorial citamos, a efectos indicativos, el Estudio sobre Cibercriminalidad del año 2019 del Ministerio del Interior, según el cual en dicho periodo se incoaron 218.302 investigaciones por ciberdelitos, dato revelador de que las cifras que barajamos en este informe solo reflejan una parte reducida de la actividad delictiva *online* y como tal han de ser valoradas.

También ha de precisarse que, a los efectos que nos ocupan, se computan los ilícitos planificados/ejecutados en el entorno tecnológico, cualquiera que sea su gravedad, es decir, sin distinguir si se trata de hechos que por sus características y circunstancias merecen la consideración de delitos graves o leves, dado que lo que se pretende es ofrecer una visión lo más veraz y amplia posible de la incidencia que el desarrollo tecnológico está teniendo en las distintas manifestaciones de la delincuencia. Avala este planteamiento la circunstancia de que en muchas ocasiones la denuncia inicial de una acción *online* presuntamente ilícita –un breve bloqueo de un sistema o dispositivo móvil, un desplazamiento patrimonial no consentido de escasa cuantía o un contacto molesto proveniente de un tercero a través de la red, entre otras posibilidades– resulta ser el indicador de una acción delictiva de mayor trascendencia y gravedad. De hecho, en muchas ocasiones las actividades criminales *online* son planificadas para que sus efectos se produzcan en distintos lugares y con consecuencias aisladamente poco relevantes aunque respondan a una dinámica común, lo que determina que acciones, en apariencia de carácter leve, encubran lo que en realidad constituyen efectos parciales de actos criminales complejos e, incluso, de proyección internacional.

Hechas estas aclaraciones, el examen de los datos estadísticos sobre procedimientos incoados en el año 2020 ofrece los siguientes resultados:

Delitos informáticos		Procedimientos Judiciales Incoados	%
Contra la libertad	Amenazas/coacciones a través de TICs (art.169 y ss. y 172 y ss.).	1.247	7,37
	Acoso a través de TICs (art 172 ter).	463	2,74
Contra la integridad moral	Trato degradante a través de Tics (art. 173).	79	0,47
Contra la libertad sexual	Pornografía infantil/discapaces a través de TICs (art. 189).	707	4,18
	Acosos menores a través de TICs (art. 183 ter).	349	2,06
	Otros delitos c/libertad sexual a través TIC.	382	2,26
Contra la intimidad	Ataques / interceptación sistemas y datos (art 197 bis y ter).	60	0,35
	Descubrimiento/ revelación secretos a través TIC (art. 197).	695	4,11
Contra el honor	Calumnias/ injurias autoridades a través TIC (arts. 215 y ss.).	98	0,58

Delitos informáticos		Procedimientos Judiciales Incoados	%
Contra el patrimonio y el orden socio-económico	Estafa cometida a través de las TICs (art. 248 y 249).	12.250	72,43
	Descubrimiento secretos empresa a través de TIC (art. 278 y ss.).	18	0,11
	Delitos c/ servicios de radiodifusión/ interactivos (art. 286).	87	0,51
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter).	99	0,59
	Delitos c/ propiedad intelectual a través TIC (art. 270 y ss).	138	0,82
De falsedad	Falsificación a través de las TICs.	124	0,73
Contra Constitución	Discriminación a través TIC (art. 510).	80	0,47
Otros		38	0,22
Total		16.914	100,00

Del examen de la tabla que ofrecemos claramente se colige que las estafas/defraudaciones de los artículos 248 y ss. CP siguen siendo el tipo de ilícitos *online* que generan anualmente un volumen mayor de procedimientos judiciales. En esta ocasión la cifra asciende a 12.250, lo que implica un incremento del 42,25% concretado en 3.639 expedientes, respecto de la cifra obtenida por igual concepto en el año 2019 y un porcentaje anual del 72,43% del volumen total de nuevos expedientes por ciberdelitos. Es decir, casi tres cuartas partes de las causas judiciales por ciberdelitos registradas en 2020 tuvieron por objeto hechos ilícitos de estas características. Aunque esta preeminencia de las estafas y defraudaciones es una constante desde que venimos efectuando este seguimiento estadístico, en esta anualidad los resultados son aún más llamativos. Así, si comparamos los datos obtenidos en los últimos años, el porcentaje de estos expedientes ha ido oscilando entre el 55% y el 65% del total incoaciones: 61,35% en 2016; 55,63% en 2017; 61,54% en 2018 y 65,51% en 2019, ofreciendo en este año un índice significativamente más alto que supera en casi 7 puntos porcentuales el de 2019 y da cuenta de la utilización cada vez más frecuente de la red como medio en el que planificar y ejecutar acciones de esta naturaleza.

Ahora bien, una vez más queremos dejar constancia de que estos resultados no deben llevarnos a la errónea conclusión de que la delincuencia en la red es principalmente de carácter defraudatorio. En efecto, son las conductas que más habitualmente se denuncian y las

que dan lugar a un volumen mayor de procedimientos judiciales, pero ya comentábamos anteriormente que la cifra oculta de criminalidad en otros ilícitos, como los atentados contra la libertad e indemnidad sexual de los y las menores o los ataques a sistemas informáticos, es hoy por hoy difícil de cuantificar, dado que su detección y denuncia ofrece una mayor complejidad y por ello no quedan reflejadas en las estadísticas policiales o judiciales. Sin pretensión alguna de minimizar la gravedad de estas manifestaciones delictivas y los perjuicios económicos que de ellas se derivan, lo que quiere expresarse es que su incidencia efectiva en la ciberdelincuencia ha de ser debidamente contextualizada.

Avala este mismo planteamiento otra particularidad que influye inevitablemente en los resultados estadísticos obtenidos. Nos referimos a la dispersión geográfica de las distintas fases de la acción criminal y de sus efectos, característica inherente a una buena parte de los fraudes *online*. Precisamente la capacidad que tienen las tecnologías para hacer llegar con facilidad la superchería a una generalidad de personas, con independencia del lugar en que se encuentren, es una de las ventajas que aprovechan los/as delincuentes para multiplicar sus beneficios sin incrementar el riesgo y el esfuerzo empleado en la ideación y planificación criminal. Ello puede dar lugar a una pluralidad de denuncias presentadas aisladamente por los múltiples perjudicados/as que, por responder a la misma actividad delictiva, derivan en ocasiones en un único proceso penal, aunque figuren estadísticamente como ilícitos independientes, lo que constituye un factor de distorsión de los datos registrados.

Pues bien, la circunstancia de que las defraudaciones *online* a menudo afectan a muchas personas sin contacto físico alguno entre ellas, unida a las carencias detectadas en las bases de datos oficiales para cotejar o entrecruzar la información recopilada por los diversos cuerpos policiales, está generando unos efectos perversos sobre los que ya hemos alertado en anteriores ocasiones. Nos referimos a aquellos supuestos en los que los/as delincuentes usan la documentación o los datos obtenidos de sus víctimas mediante engaño –documentos de identidad, fotografías, permisos de conducir o de circulación etc.– para utilizarlos posteriormente, suplantando la identidad de aquellas, en la ejecución *online* de ulteriores fases de la misma actividad ilícita o en otras de similar dinámica y finalidad dirigidas contra terceras personas. Lamentablemente, estos casos en que las víctimas son de nuevo perjudicadas al verse demandadas como presuntos responsables de ilícitos que no han cometido son cada vez más frecuentes y así lo han puesto de manifiesto los/as integrantes de la red. Se trata de asuntos

en los que las personas afectadas no solo sufren los efectos directos del engaño inicial, sino que, además, se ven obligadas a «justificar» su inocencia, a veces a través de la correspondiente representación procesal en uno o más jugados –incluso de distintos territorios– con el perjuicio que ello conlleva, tanto económico como moral, y el riesgo de verse injustamente condenados/as como autores de un delito.

Desde esta Unidad Especializada y en el ejercicio de la función de coordinación que le compete, se están intentando solventar estas situaciones localizando con la mayor rapidez posible las causas judiciales en curso contra los/as afectados/as; trasladando a los correspondientes fiscales delegados/as la documentación acreditativa de la suplantación de identidad generada y promoviendo la utilización procesal de todos los recursos legales necesarios para evitar o, en su caso, dejar sin efecto una condena manifiestamente injusta que incluso en algún supuesto ha llegado a producirse.

Resulta no obstante evidente que la solución no puede descansar exclusivamente en la capacidad de coordinación interna del Ministerio Fiscal en la que empeñamos todo nuestro esfuerzo, sino que exige de una actuación mucho más ambiciosa que implica necesariamente a otras instituciones del Estado. Como decíamos anteriormente son muchas las denuncias por actividades ilícitas en el entorno tecnológico –en su mayoría estafas y defraudaciones– que por mor de lo dispuesto en el art. 284 de la LECrim, no llegan actualmente a conocimiento de los órganos de la jurisdicción penal por lo que la información derivada de las mismas queda exclusivamente a disposición policial. Se trata en todo caso de una información valiosa, no solamente para evitar las situaciones que se han expuesto, sino también para interrelacionar los múltiples efectos de una misma acción delictiva y hacer posible su análisis y tratamiento conjunto, imprescindible para una adecuada respuesta desde el Estado de Derecho ante este tipo de actividades criminales. A dicho fin resulta esencial mejorar la capacidad de coordinación interna y de tratamiento de la información por los propios cuerpos policiales, tarea en la que se está empeñando un especial esfuerzo que recientemente se ha concretado en un Plan Estratégico contra la Cibercriminalidad aprobado por la Instrucción 1/2021 de la Secretaría de Estado de Seguridad.

Sin perjuicio de nuestro apoyo y contribución a este proyecto, la Unidad de Criminalidad Informática viene trabajando en esa misma línea a través de los Expedientes de Coordinación que, con amparo en la Instrucción 2/2011 y con la colaboración imprescindible de los/as fiscales delegados/as y de las oficinas de enlace con los cuerpos policiales, tienen como objetivo analizar conjuntamente toda la informa-

ción relacionada con una misma actuación criminal con efectos en distintos territorios, a fin de orientar de forma centralizada la investigación; coordinar sus resultados y, si resultara procedente, promover la acumulación de los diversos procedimientos ante el órgano judicial que resulte competente.

En las memorias provinciales se llama la atención acerca de la proliferación de ofertas engañosas de productos financieros supuestamente de alta rentabilidad, en moneda de curso real o en criptomonedas, que se realizan a los ciudadanos y ciudadanas como inversiones seguras y plenamente garantizadas y, por tanto, sumamente atractivas en un entorno económico crítico y complejo. De esta forma los/las delincuentes logran atraer la atención de sus víctimas que, confiadas en la apariencia creada, realizan importantes desembolsos económicos por los que posteriormente no solo no llegan a percibir beneficio alguno, sino que sus aportaciones resultan irrecuperables, al ser incluso desconocido/a el/la destinatario/a último/a de las mismas. Son investigaciones extraordinariamente complejas ya que quienes planifican estas acciones suelen integrarse en grupos organizados transnacionales que se sirven, al menos ocasionalmente, de proveedores de servicios de intermediación y cambio de monedas virtuales y de custodia de monederos electrónicos, respecto de los cuales la obtención de información presenta todavía muchas dificultades. Por ello sería deseable una rápida implementación de la Directiva (UE) 2018/843, de 30 de mayo, sobre prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo, en la que se contemplan mecanismos legales para solventar algunas de estas dificultades.

Por otra parte, siguen proliferando otras modalidades de fraude ya detectadas en anualidades anteriores. Varias memorias provinciales refieren procesos en trámite por la llamada *estafa del soporte técnico*, en la que se combina hábilmente el engaño con la manipulación informática, de forma tal que una vez infectado el dispositivo de la víctima mediante una intrusión irregular –normalmente a través de un *malware* adjunto a un *link* o a un *email* malicioso– quien opera como atacante hace que «salte» en el mismo una advertencia de mal funcionamiento acompañada de un mensaje que aconseja contactar con el equipo técnico correspondiente. Esto permite a los/as delincuentes, simulando actuar como tal equipo, tomar el control del sistema y ejecutar sus criminales objetivos, ya sea obtener cantidades indebidas por simuladas reparaciones no realizadas, exfiltrar información o cualquier otra que estimen de interés.

Esa misma combinación de engaño y manipulación informática es propia también de otras técnicas falsarias que se detectan con frecuencia creciente sobre las que informan, entre otros, los/as delegados/as de Araba, Cádiz, Castellón, Córdoba, Guadalajara o Illes Balears. Se trata de los ataques *Business Email Compromise* (BEC), dirigidos generalmente contra entidades empresariales, en los que los/las delincuentes, en primer término, obtienen por medios diversos –técnicas de ingeniería social, acceso irregular al sistema etc.– información sobre el funcionamiento de la empresa objeto de ataque y concretamente sobre extremos tales como la identidad y criterios de actuación de sus directivos/as o representantes, proveedores y clientes; actividades económicas en curso o medidas de seguridad establecidas. Posteriormente, con dicha información a su disposición proceden a suplantar la identidad de cualquiera de los que operan en el tráfico ordinario de la entidad atribuyéndose falsamente sus datos personales y a ordenar por medios electrónicos operaciones económicas, aparentemente justificadas, desviando de esta forma importantes cantidades de dinero en su propio beneficio.

Al igual que en periodos anuales anteriores siguen siendo numerosísimas las denuncias presentadas por utilización irregular *online* de numeraciones de tarjetas de crédito o débito ajenas. A dicho fin, los datos se obtienen copiándolos o clonándolos mediante técnicas de *skimming,* aprovechando la posesión física de la tarjeta original por los/las delincuentes –con ocasión de su uso en establecimientos abiertos al público– o instalando herramientas de copiado en los cajeros automáticos o a través de técnicas de *phising, smishing* –suplantación de entidades bancarias en páginas web o mensajes SMS– o *hacking*, entre otras. Muchas de las denuncias por estas conductas no llegan a conocimiento de los órganos de la jurisdicción penal y, por ende, no se reflejan en nuestras tablas estadísticas, dadas las dificultades para la determinación de sus autores que frecuentemente se integran en organizaciones criminales internacionales. Sin embargo, la cooperación internacional y la profesionalidad de los grupos de investigación policiales y de las autoridades judiciales y el Ministerio Fiscal están haciendo posibles progresos importantes en la capacidad de respuesta frente a estas formas de defraudación. Ejemplo de ello es el proceso judicial en curso, seguido en Granada, en el que el esfuerzo de nuestros profesionales unido a la colaboración de la Fiscalía y las unidades policiales de Chile está favoreciendo la obtención de resultados muy prometedores en orden a la desarticulación de quienes se sirven de esta técnica y de la propia transnacionalidad de su actividad para intentar asegurarse la impunidad.

En este breve repaso de las actuaciones fraudulentas *online*, es obligada la mención de las conductas que afectan al sector de las telecomunicaciones en sus distintas variantes, y muy relacionadas con ellas, aunque el perjuicio se genera en la banca *online*, el conocido vulgarmente como fraude *SIM Swapping,* que está siendo utilizado con alarmante frecuencia en los últimos años. La técnica consiste en burlar las medidas de seguridad de las entidades bancarias accediendo a los códigos alfanuméricos de confirmación, de uso único, generados con ocasión de las transacciones electrónicas y que ordinariamente se comunican a los/as clientes a través de mensajes SMS. Para ello, los/as delincuentes obtienen previamente un duplicado o una nueva tarjeta SIM a nombre de su víctima, ya sea solicitándola del operador correspondiente, simulando la identidad de aquella, ya sea valiéndose de una metodología más elaborada, como en el supuesto objeto de instrucción judicial en Zamora, en el que se aprovechaba con esa finalidad un establecimiento de reparación de móviles. Una vez tienen la tarjeta SIM a su disposición, los delincuentes se garantizan la recepción en su propio dispositivo del código de confirmación de la transacción fraudulenta y, en definitiva, la posibilidad de hacer efectiva la misma en su beneficio, evitando que en ese momento sea conocida por el perjudicado o perjudicada. Esta forma de defraudación ha generado en los últimos años múltiples investigaciones policiales y la incoación de procedimientos judiciales en distintos territorios como A Coruña y Valencia. Su efectividad y la facilidad con que los/as delincuentes logran sus ilícitos propósitos ha determinado la adopción por los operadores de telefonía de medidas específicas de prevención y fortalecimiento de las garantías para la emisión de estas tarjetas o de sus duplicados.

Los delitos cometidos a través de las TIC contra bienes jurídicos de carácter personalísimo adquieren cada año una mayor importancia, a medida que las relaciones interpersonales se han ido trasladando a la red, circunstancia de especial incidencia durante el periodo anual que nos ocupa en el que los ciudadanos y ciudadanas, por razones de salud y salud pública, se han visto obligados a limitar sus contactos en el entorno físico.

En este apartado incluimos, en primer término, los ilícitos *online* contra la libertad y seguridad personal que en 2020 dieron lugar a la incoación de 1.710 procedimientos judiciales, un 10,10% del conjunto de los registrados por ciberdelitos, de los que 1.247 lo fueron por delitos de amenazas o coacciones de los artículos 169 y ss. CP y los restantes, un total de 463, por el tipo penal de acoso permanente u hostigamiento del art. 172 ter CP. La comparación con los datos obte-

nidos en 2019 revela un incremento conjunto del 19,23% que sin embargo resulta desigual respecto de los diversos tipos delictivos examinados. Así, llama la atención el fuerte repunte de las amenazas y coacciones que, habiendo mantenido una situación estable en los últimos años –905 y 961 expedientes respectivamente en 2018 y 2019–, muestran un incremento de casi el 30%, en tanto que las conductas de hostigamiento, que presentaban una constante y rápida evolución al alza con 200 registros en 2017; 337 en 2018 y 420 en 2019, moderan ligeramente su ritmo de crecimiento en el pasado año, en que el dato de 463 expedientes refleja un ascenso de poco más del 10%.

Aunque, como acertadamente apuntan muchos de los/as fiscales, se trata de conductas frecuentemente vinculadas a la violencia de género que, en un número difícilmente cuantificable, quedan extramuros de nuestras estadísticas –al ser registradas en dicha área de especialización– no siempre concurre dicha circunstancia, sino que cada vez proliferan más los comportamientos de este tipo dirigidos contra personas vinculadas al agresor o la agresora por razones profesionales, de vecindad etc., o también respecto de quienes han mantenido con el o la atacante una relación puntual o incluso le son completamente desconocidas. Buen ejemplo de ello son las diversas investigaciones policiales y/o judiciales actualmente en curso respecto de aquellas conductas conocidas como *sextorsión*, en las que el/la delincuente chantajea a la víctima, amenazándola con divulgar imágenes suyas de carácter sexual si no recibe de la misma una compensación normalmente de carácter económico. Las variantes que ofrece este comportamiento son diversas: en ocasiones el agresor obtiene directamente del perjudicado/a dichas imágenes simulando –por sí o a través de otras personas– una supuesta relación íntima entre ambos/as que luego resulta ser una superchería para conseguir el material comprometido. En otros casos, las imágenes son obtenidas accediendo irregularmente al dispositivo de la víctima y también se han detectado supuestos en los que el chantaje se lleva a efecto sin contar con material alguno, haciendo creer al o la afectado/a que se dispone del mismo o basando la coacción en meros contactos entablados por el/la perjudicado/a en la red con dicha finalidad, aunque no se hayan llegado a materializar en forma alguna. Las dificultades para el esclarecimiento de estos ilícitos son evidentes ya que, por lo común, se trata de actividades planificadas y ejecutadas por grupos internacionales de delincuentes que actúan mediante personas interpuestas, lo que complica extraordinariamente la determinación de sus autores. No obstante, su investigación ha dado lugar a la incoación de una diversidad

de procedimientos judiciales, circunstancia que bien puede justificar el repunte en los datos estadísticos sobre estas tipologías delictivas.

En el apartado correspondiente a los delitos contra bienes personalísimos es también obligada la mención de las causas por delitos contra la integridad moral, sancionados en el art. 173.1.º CP cuyo número se concreta en un escaso 0,47% de los registros anuales. Se incluyen aquí los comportamientos que atentan contra la dignidad de la persona, como el caso de la difusión pública a través de las TIC de contenidos humillantes y ofensivos que ridiculizan y denigran al o la afectado/a o de otras conductas que ofenden al mismo bien jurídico y que no encuentran acogida en tipos penales más específicos.

Aun incidiendo igualmente en bienes personalísimos, merecen consideración independiente por su gravedad y preocupante evolución los delitos *online* contra la libertad sexual y en particular los que afectan a las personas menores de edad. El total de procedimientos por hechos de esta naturaleza cometidos en el entorno tecnológico asciende a 1.438, lo que supone un porcentaje del 8,5% de todos los incoados en el año memorial, y un incremento del 18,45% respecto de los 1.214 registrados en 2019. Analizando separadamente los resultados referentes a las distintas tipologías delictivas, se constata que los actos de *child grooming*, sancionados en el art. 183 ter CP, dieron lugar a 349 incoaciones en 2020, cifra que refleja un claro repunte de más del 55% en comparación con los 225 procedimientos registrados en 2019 y de casi el 175% respecto de los 127 del año 2018. En cuanto a las anotaciones por delitos de pornografía infantil y/o de personas con discapacidad, sancionados en el art. 189 CP, presentan una gran estabilidad en los últimos años, con una ligera tendencia al descenso ya que los 754 procedimientos incoados en el año 2018 se redujeron a 714 en 2019 y a 707 en el periodo anual que nos ocupa. Sin embargo, como ya hemos adelantado y detallaremos más adelante esta aparente estabilidad no responde a la evolución real de la elaboración y tráfico de material pornográfico ilícito en el entorno tecnológico.

Ya se ha hecho referencia a la perversa incidencia que ha tenido en estas gravísimas conductas el obligado confinamiento de los ciudadanos a causa de la pandemia, y también a la preocupación que dicha circunstancia está generando en los organismos nacionales e internacionales. Las cifras relativas a los delitos de acoso sexual a menores responden claramente a esta situación, pues dan cuenta de un aumento muy significativo de procedimientos incoados por estos ilícitos motivado, en parte, por el mayor número de agresiones de esta naturaleza y también por la creciente sensibilización de progenitores, cuidadores y tutores ante la especial vulnerabilidad de los y las menores frente a

los depredadores sexuales que ha dado lugar, como consecuencia, a un aumento en el número de denuncias presentadas. Aun así, los datos que ofrecemos en cifras absolutas no constituyen un reflejo fiel de la dimensión real del problema que nos ocupa. Lamentablemente, es frecuente que en muchos de los procedimientos judiciales incoados por hechos de esta naturaleza se investiguen y enjuicien conjuntamente una diversidad de acciones atribuidas a una misma persona, pero reiteradas en el tiempo y ejecutadas respecto de un número más o menos elevado de menores. En estos casos, cada anotación estadística integra por lo general una pluralidad, no precisada, de conductas y de víctimas. Las carencias en los sistemas informáticos no permiten una mayor concreción ni en lo que se refiere al volumen total de actos ilícitos investigados/enjuiciados, ni respecto a los o las menores afectados/as por las mismas, que, de ser posible, reflejaría, sin duda alguna, unos resultados mucho más preocupantes.

Los delitos de pornografía sancionados en el art. 189 del CP se encuentran íntimamente vinculados a los anteriores, hasta el punto de que, con relativa frecuencia, el acoso sexual a los y las menores tiene por objeto, precisamente, la elaboración u obtención de material pornográfico infantil. Al respecto, desde nuestro punto de vista, resulta especialmente preocupante la reiteración con la que se están detectando en nuestro país actos de elaboración de pornografía infantil a partir de contactos directos por vía electrónica en los que el agresor invita al o a la menor a mostrarse desnudo/a y en posiciones sexualmente explicitas o, incluso, le incita a realizar actos sobre su propio cuerpo –como introducción de objetos por vía anal o vaginal– que en sí mismos constituyen abusos sexuales del artículo 183 CP. Ya no se trata, por tanto, de comportamientos relacionados exclusivamente con la puesta en circulación de contenidos pedófilos, sino de actos de abuso o agresión en los que, además de satisfacer sus instintos, el agresor o agresora busca obtener dichos materiales ya sea para su propio consumo o para distribuirlos a terceros.

En relación con estos ilícitos, llama poderosamente la atención el escaso volumen de incoaciones, que se mantiene prácticamente invariable en los últimos años, aun cuando los datos nacionales e internacionales sobre tráfico de pornografía en la red crecen exponencialmente, como ya se ha indicado en el apartado inicial de esta memoria. Ello puede ser debido a que las conductas de elaboración o distribución de material ilícito en el entorno tecnológico, a diferencia de las conductas de acoso sexual, no son habitualmente objeto de denuncia por parte de los perjudicados/as, al tratarse de conductas clandestinas en las que las víctimas –habitualmente menores de muy corta edad– ni

tan siquiera son conscientes de la agresión sufrida. Estas investigaciones suelen iniciarse de oficio, a partir de notificaciones de ciudadanos/as que detectan material de esta naturaleza en la red o de las comunicaciones recibidas de organismos y/o cuerpos policiales de otros países, por lo que precisan de una intensa actuación indagatoria que comienza por la identificación del usuario/a de la dirección IP desde la que se puso en circulación el contenido pedófilo. Queremos decir con ello que no toda la información recibida se logra materializar en investigaciones concretas, en ocasiones por falta de información suficiente para ello y, en mayor medida, debido a la carencia de recursos personales y materiales adecuados para abordar la investigación de una actividad criminal en continua expansión que está siendo planificada y ejecutada a través de sistemas de comunicación cada vez más complejos y sofisticados –archivos compartidos en la nube; mensajería instantánea, redes TOR– y protegidos con sistemas de encriptación muy difíciles de quebrar. Una situación que demanda de una mayor concienciación social y un esfuerzo especial para dotar a Fuerzas y Cuerpos de Seguridad –y también a los operadores jurídicos– de mayor formación y mejores medios para reforzar la respuesta ante estos graves comportamientos.

No podemos finalizar el análisis de los procedimientos por actuaciones *online* contra bienes personalísimos sin llamar la atención, una vez más, acerca de la conveniencia de tipificar penalmente determinados supuestos de suplantación de identidad ajena en la red. Son conductas que se producen con frecuencia creciente –creando perfiles falsos o haciéndose pasar por otro en chats, foros o plataformas similares de contacto interpersonal– y que, en determinadas circunstancias, pueden ser objeto de investigación y sanción penal por encuadrarse en concretas figuras tipificadas legalmente. Así ocurre cuando la simulación forma parte del engaño utilizado como medio para defraudar o cuando la suplantación de otra persona se lleva a efecto en cualquiera de las formas previstas en el artículo 172 ter CP. En ocasiones estas acciones también pueden dar lugar a la aplicación de la circunstancia de agravación prevista en los artículos 197.4.º b, 264.3 y 264 bis.3 CP.

Sin embargo, esta respuesta penal no resulta tan clara en otras ocasiones como en aquellos supuestos en que la acción del o de la agresor/a, tiene como único objetivo perjudicar a la persona suplantada, haciéndose pasar por ella en sus relaciones *online* –personales, profesionales o sociales– y atribuyéndole opiniones, pensamientos o formas de actuar que no se corresponden con la realidad y le hacen desmerecer en su proyección, consideración pública y reconocimiento

social. Es evidente que, aun cuando en estos últimos casos pueden resultar afectados bienes jurídicos merecedores de protección penal, la consideración de estas acciones como delito presenta serias dificultades salvo que, por las circunstancias concurrentes, pueda apreciarse la comisión de alguno de los ilícitos contra el honor, la intimidad o la integridad moral.

Un número importante de fiscales delegados/as alertan acerca de la proliferación de estos comportamientos en el entorno tecnológico y algunos de ellos/as, en apoyo de sus afirmaciones, facilitan datos parciales pero muy significativos a estos efectos. Así, entre otros, los fiscales delegados de A Coruña, León y Badajoz dan cuenta respectivamente de 36, 42 y 113 denuncias/atestados policiales por hechos de esta naturaleza, en tanto que la Fiscal Delegada de Bizkaia se refiere a las 382 denuncias interpuestas ante la Ertzaintza y el de Barcelona al centenar que, aproximadamente, registraron en ese territorio los Mossos d'Esquadra. La mayoría de estas denuncias resultaron archivadas por falta de tipicidad de la conducta pese al incuestionable perjuicio que dichas acciones pueden llegar a causar a las personas afectadas.

Resulta evidente que utilizar de forma deliberada la identidad de alguien perfectamente identificado, con efectos de permanencia y con unas connotaciones que aporten credibilidad e induzcan a error efectivo sobre la intervención de la persona suplantada, puede implicar un atentado grave contra la privacidad y afectar seriamente a las relaciones de la víctima con terceros. Por esta razón los fiscales que integran esta área de especialización entienden absolutamente necesaria la tipificación penal de estos comportamientos y no se puede dejar de aprovechar la oportunidad que nos ofrece la Memoria para dejar constancia de ello.

Otra manifestación importante de la ciberdelincuencia son los ataques a los sistemas de información que se encuentran tipificados en dos apartados distintos del Código Penal: los relativos a delitos de descubrimiento y revelación de secretos y a daños informáticos. En cuanto a los primeros, sancionados en los arts. 197 bis y ter CP, determinaron en 2020 la incoación de 60 procedimientos y, por ende, un descenso de aproximadamente el 28% respecto de los 84 y 83 expedientes registrados respectivamente en 2019 y 2018. Este dato contrasta sin embargo con el progresivo incremento en los procesos por otras figuras de descubrimiento y revelación de secretos –esencialmente las previstas en el art. 197.1.º, 2.º y 7.º CP –que se sitúa en el 16,6% respecto de los 596 incoados en 2019 y en el 57%, si lo comparamos con los 441 de 2018, una aparente disparidad que, no

obstante, puede explicarse por la relación concursal que ocasionalmente existe entre ambas figuras, cuando el acceso irregular o la interceptación de comunicaciones entre sistemas tiene como último objetivo el apoderamiento de datos personales o de información reservada, lo que en su caso podría determinar una única anotación estadística en este último apartado.

Aunque son ilícitos relacionados con la seguridad de los sistemas informáticos que pueden tener como objetivo finalidades muy diversas –acceso a datos de carácter médico o económico, entre otros– los/las delegados/as vinculan el incremento de estas acciones con el aumento de los actos de intromisión en dispositivos móviles en el marco de los conflictos intrafamiliares como medio de ejercer acciones de control y espionaje sobre la víctima.

En cuanto a las anotaciones referentes a agresiones informáticas tipificadas en los delitos de daños de los artículos 264 y ss. CP, su número se mantiene estable, 99 nuevos registros frente a los 101 de 2019, como contrapunto a la línea ascendente que veníamos observando en años anteriores y que se concretó en un repunte de más del 55% en el periodo 2018-2019 y del 12,2% entre los años 2017 y 2018. La compleja situación acaecida en 2020 nos lleva a interpretar estos resultados no como un cambio de tendencia sino, más bien, como lógica consecuencia de las alteraciones producidas en el funcionamiento de organismos e instituciones y también de los órganos de la jurisdicción penal, que han provocado disfunciones en la denuncia/tramitación de este tipo de expedientes. De hecho, los ataques a sistemas informáticos han sido una de las grandes preocupaciones generadas durante la pandemia, hasta el punto de motivar la emisión de alertas específicas de prevención tanto a nivel nacional como internacional, en particular respecto de instalaciones críticas como los centros médicos y hospitalarios. Buena muestra de la persistencia de estos ilícitos son los ataques de *ransomware* dirigidos respectivamente en los meses de julio y septiembre contra la empresa pública española ADIF, encargada de la infraestructura ferroviaria y la compañía de salud Adeslas.

Por su parte, las causas incoadas por delitos contra la propiedad intelectual acusan un llamativo descenso, superior al 75%, dado que en 2020 se registraron 138 incoaciones frente a las 555 contabilizadas en 2019. Igual circunstancia concurre respecto a los ilícitos contra los servicios de radiodifusión e interactivos que se reducen en casi un 52%, habiendo dado lugar en esta última anualidad a 87 incoaciones. En ambos casos sin duda alguna esta bajada encuentra su explicación en el hecho de que las actuaciones procesales derivadas de la gran operación realizada en 2018 por la Unidad de Investigación Tec-

nológica del CNP –por denuncia de la Liga Profesional de Fútbol– contra los titulares de 1.106 establecimientos públicos que ofrecían irregularmente a sus clientes retransmisiones deportivas de difusión limitada, a través de decodificadores no autorizados, se han reducido considerablemente a medida que se han ido incoando y tramitando los correspondientes procedimientos judiciales, muchos de ellos ya resueltos por sentencia firme, como se ve reflejado al examinar los escritos de acusación presentados por dichos ilícitos.

En último término deben mencionarse los 80 procedimientos por conductas tipificadas en el art. 510 del CP, cifra muy similar a las 83 incoaciones contabilizadas en 2019. En ellos se investiga esencialmente la difusión *online* de contenidos –susceptibles de calificarse como *discurso de odio*– que incitan, fomentan, promueven o favorecen la hostilidad, la violencia y la discriminación respecto de quienes son diferentes. Aunque en la Fiscalía hay una Sección específicamente dedicada a los Delitos de Odio y Discriminación, como quiera que muchas de estos comportamientos se planifican y ejecutan a través de la red, también el área de especialización en criminalidad informática, en total coordinación con aquella, se encuentra activamente implicada en la investigación, persecución y enjuiciamiento de estas acciones. La preocupación generada por la difusión de esta clase de contenidos a través de las TIC y los perjudiciales efectos que de ello se puedan derivar para el mantenimiento de los valores inherentes a una sociedad libre y democrática en la que se garanticen los derechos y libertades de los/las ciudadanos/as y, en particular, el principio de igualdad y el respeto a la dignidad de las personas dio lugar, en su momento, a la articulación de unidades especializadas en esta materia no solo en los cuerpos policiales sino también en el Ministerio Fiscal. Este proyecto de actuación especializada ha culminado a finales del año 2020 con la firma de un *Protocolo contra el discurso de odio online* que tiene por objeto la retirada de la red de contenidos de esta naturaleza y en el que la Unidad de Criminalidad Informática ha asumido la responsabilidad de realizar la función de punto de contacto nacional con los proveedores de servicio radicados en otros países.