2.1 Delitos contra la intimidad y la protección de datos de carácter personal

La protección penal de la intimidad, la propia imagen y los datos de carácter personal se encuentra recogida en nuestra legislación en el Capítulo I del Título X del Libro II del Código Penal, arts. 197 y ss., bajo la rúbrica de los delitos de descubrimiento y revelación de secretos. Aun cuando el art. 197 comprende diversas figuras delictivas, las aplicaciones de registro informático no permiten por el momento establecer distinción entre ellas, por lo que los datos estadísticos que se ofrecen agrupan necesariamente todos los procedimientos y/o actuaciones por estos ilícitos sin distinción, si bien el análisis de las distintas conductas se abordará de forma independiente a partir de la experiencia adquirida en la aplicación de unos u otros tipos penales.

Como ya hemos indicado, según los datos procedentes del Área de Especialización en Criminalidad Informática, estos comportamientos determinaron en el año 2019 la incoación de un total de 596 procedimientos judiciales, lo que supone un incremento medio del 35 % respecto de los 441 del año 2018, y de más del 27 % sobre los 466 del año 2017, cifras que, pese a las deficiencias en el control estadístico antes mencionadas, dejan constancia de una clara tendencia alcista en el entorno virtual. En cuanto a los escritos de acusación presentados en razón a estas conductas, el incremento es también evidente, pues los 110 realizados en 2017 se elevaron ligeramente hasta 115 en 2018, alcanzando en 2019 el número de 188, con un porcentaje de incremento en el último periodo anual del 63 %. A estas cifras habrán de añadirse, aun cuando no podemos descartar totalmente posibles duplicidades, los 168 procedimientos judiciales registrados en el ámbito de la Violencia contra la Mujer y los 149 escritos de acusación presentados por los fiscales especialistas en esa materia.

En referencia a los menores de edad, aunque por las razones indicadas no se puedan aportar cifras concretas, no es desacertado concluir que casi la totalidad de los delitos de descubrimiento y revelación de secretos registrados fueron cometidos a través de Internet.

Las figuras delictivas básicas del art. 197 CP, definidas en sus apartados primero y segundo, mantienen actualmente la redacción dada por la LO 10/1995, de 23 de noviembre que aprobó el texto vigente, si bien la fórmula abierta utilizada para describir la conducta típica está permitiendo su aplicación para el enjuiciamiento y sanción de los ataques contra esos bienes jurídicos en un entorno tecnológico.

El apartado primero, de carácter más general, protege los derechos fundamentales a la intimidad, la imagen y la inviolabilidad de las

comunicaciones frente a cualquier conducta de intromisión indebida ajena, con una descripción típica muy similar a la de los precedentes arts. 497 y 497 bis del Texto Refundido del Código Penal de 1973. Se trata de un precepto de marcado carácter intencional *–para descubrir los secretos o vulnerar la intimidad de otros–* que se integra por dos conductas delictivas distintas.

La primera de ellas se concreta en el apoderamiento de papeles, cartas, mensajes de correo o cualquier otro documento o efecto personal, es decir, de cualquier soporte, sea físico o electrónico, en el que se alojen información o contenidos considerados secretos por tener carácter privado y afectar a la intimidad de la víctima. La acción típica *apoderarse* abarca tanto la aprehensión física de documentos y efectos materiales como el apoderamiento intelectual o conocimiento no autorizado del secreto o de la información privada que, en el momento actual, puede hacerse también efectivo con los potentes medios de penetración que proporcionan las TIC. Tal sería el caso, entre otros, de la intromisión en el perfil de *Facebook* de otra persona para apoderarse de sus fotos y luego difundirlas, o de la lectura no permitida de correos electrónicos ajenos o, en fin, de cualquier tipo de acceso irregular al *WhatsApp* o a los mensajes SMS de un dispositivo móvil de otra persona. Buen ejemplo de ello es el supuesto contemplado en la STS n.º 544/2016 de 21 de junio, en el que el condenado había accedido al móvil de su ex-esposa sin su consentimiento, para leer los mensajes almacenados y conseguir información acerca de una relación íntima que aquella mantenía con un tercero, siendo de interés recordar, a esos efectos, que en la STS n.º 872/2001, de 14 de mayo, el Alto Tribunal ya afirmaba que no existe una dimensión familiar de la intimidad que permita a uno de los cónyuges violar la intimidad de otro, ya que la acreditación de la fidelidad no está por encima de la intimidad de cada uno de ellos. Otro ejemplo de la aplicación de esta figura en intromisiones *online* es el de la STS n.º 310/2015 de 27 de mayo que incardina en este precepto la conducta de quien, sin estar autorizado, accedió a la papelera de reciclaje de un dispositivo informático para rescatar y conocer el contenido de determinados archivos allí almacenados que habían sido previamente *borrados* por el titular del sistema.

También se incluyen en este precepto, como conductas típicas, *la interceptación de telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación.* En este segundo inciso, al igual que en el anterior, la forma abierta en que se define la conducta típica permite su aplicación a conductas surgidas

al hilo del desarrollo tecnológico. Así el acierto del legislador de 1995 –que sustituyó la tradicional referencia a la interceptación de las comunicaciones, por la actual mención de *interceptación de las telecomunicaciones*– ha permitido incardinar en este precepto la injerencia irregular en cualquier clase de comunicación –convencional, correo electrónico, telefonía móvil, mensajería instantánea como *WhatsApp*, *Telegram,* voz sobre IP, etc.– y por cualquier medio que haga posible dicha interferencia, tales como el desvío de llamada, los ataques *man in the middle*, o el acceso remoto al sistema a través de virus informáticos como los programas espía (*spyware*), entre otras posibilidades. Y lo mismo ha de indicarse a propósito de la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonidos, imágenes o señales de comunicación, figura en la que es posible encuadrar muchas de las conductas contra la intimidad y la propia imagen que se ejecutan a través de las TIC. Por ello, es frecuente sancionar con base en este tipo penal los diversos supuestos en los que los delincuentes se sirven de grabadoras o cámaras ocultas para captar imágenes o sonidos con distintas finalidades. La casuística en este ámbito es muy amplia: dispositivos ocultos en los baños de colegios, instalaciones deportivas o establecimientos públicos; grabaciones no consentidas de actos íntimos con terceras personas; activación a distancia del micrófono o la grabadora de dispositivos móviles para captar imágenes o escuchar conversaciones ajenas, etc. Un ejemplo de ello nos lo proporciona el fiscal especialista en criminalidad informática de Navarra a propósito de la Sentencia dictada por el Juzgado de lo Penal n.º 1 de Tafalla en el PA 998/2015, que aplica este tipo penal al dueño de un bar que colocó cámaras en el servicio del local logrando captar imágenes íntimas de 129 personas, supuesto similar, entre otros muchos, al analizado en el PA 24/2017 del Juzgado de Instrucción n.º 3 de los de Huelva.

No obstante, varios fiscales delegados de Criminalidad Informática plantean sus dudas sobre la posibilidad de encuadrar en este precepto algunas conductas que se detectan, cada vez con más frecuencia, en actuaciones entre particulares. Se refieren concretamente a la colocación de herramientas de seguimiento y/o de geolocalización en terminales móviles de los que son usuarios personas determinadas para conocer sus movimientos y los lugares a los que acuden habitualmente. Desde nuestro punto de vista, parece indiscutible que un acto de esa naturaleza constituye un atentado contra el derecho a la intimidad aun cuando su inclusión en este precepto –en su caso, como captación irregular de la *transmisión* de una *señal de comunicación*– pudiera resultar técnicamente dudosa, y ello sin perjuicio de su posible san-

ción en base a otros artículos del Código Penal, como el acoso permanente (art. 172 ter) o el acceso irregular a sistemas (art. 197 bis 1.º). Aun cuando la tipificación penal de esta conducta en el art. 197.1.º CP se ha mantenido por el Ministerio Fiscal en algún procedimiento (DP 169/2018 del Juzgado n.º 1 de Violencia contra la Mujer de Cádiz), no existe un criterio uniforme al respecto y, como recuerda el Fiscal Delegado de Lugo, debe precisarse que estos supuestos son sustancialmente diferentes de aquellos otros que se analizan en algunas resoluciones de diversos órganos territoriales (Sentencias 51/2019 AP de Jaén o 512/2011 AP de Tarragona, entre otras) en las que se rechaza esta posibilidad respecto de la colocación irregular de balizas en vehículos de motor porque no necesariamente son utilizados siempre por la misma persona.

Como se indicaba anteriormente, en ocasiones el atentado a la intimidad y el daño causado a la víctima se agravan de forma notable por la difusión o revelación a terceros de los contenidos irregularmente obtenidos, normalmente a través de redes sociales o programas de mensajería instantánea, lo que atrae la aplicación del apartado tercero [8] del citado art. 197 CP. Esta circunstancia concurre en una buena parte de los supuestos que llegan a nuestro conocimiento pues, con relativa frecuencia, el objetivo último de las grabaciones subrepticias o de la obtención de información en perfiles privados o en dispositivos ajenos es precisamente su difusión pública buscando el escarnio o descrédito de la víctima.

A propósito de este tipo de comportamientos, es de interés traer a colación la Sentencia n.º 239/2019 de 19 de noviembre de la Sección Segunda de la Audiencia Provincial de Navarra, por la que se condena a dos de los integrantes del grupo conocido como «La Manada» por la grabación de siete vídeos y dos fotografías del acto de agresión sexual cometido en las fiestas de San Fermín de 2016, por el que también fueron condenados, en el entendimiento, según razona el Tribunal, de que dicho material se obtuvo sin el consentimiento de la víctima. En la resolución se aplica, igualmente, la circunstancia de agravación prevista en el apartado quinto [9] del citado art. 197 CP, por considerar que *los vídeos grabados y las fotos tomadas afectan a datos de carácter personal pertenecientes al reducto más íntimo de la privacidad de*

---

[8] *Se impondrá la pena de… si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

[9] *Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial, vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán…*

la denunciante, como lo es (…) todo lo relativo a la vida sexual, reflejando actos de naturaleza sexual realizados sobre ella sin su consentimiento. Aborda de esta forma el Tribunal una cuestión controvertida cual es si la referencia, en el citado apartado del precepto penal, a datos y/o informaciones que *revelen* la *vida sexual* de la víctima permite aplicar la agravante en aquellos supuestos en los que los contenidos obtenidos sin consentimiento del afectado tengan por objeto situaciones impuestas forzadamente por terceros y, por tanto, no se refieran a planteamientos, conductas o formas de actuar libremente asumidas por la víctima. Aun cuando, a este respecto, la doctrina de la Sala Segunda del Tribunal Supremo venía siguiendo un criterio restrictivo y por tanto excluyente de la aplicación del precepto en dichos supuestos, algunas resoluciones más recientes, entre ellas la STS n.º 700/2018 de 9 de enero, han optado por una interpretación más abierta de esta circunstancia agravatoria, criterio que también fue asumido en la Conclusión Quinta de las Jornadas de Especialistas en Criminalidad Informática celebradas en Sevilla en marzo del 2019, como pauta de actuación de la Fiscalía en tanto no exista un criterio jurisprudencial consolidado en relación con ello.

En relación con este tema es importante destacar el preocupante incremento de estas conductas en las que al enorme daño ocasionado por la agresión sexual grupal, se añade la humillación que supone para la víctima que la imagen en que se concreta dicha agresión sea grabada y difundida a través de las redes, lo que exige una reacción contundente por parte de nuestro ordenamiento jurídico.

Por su parte el apartado 2.º del art. 197 CP, incorporado por la LO 10/1995, ampara penalmente el derecho fundamental derivado del art. 18.4 CE, protegiendo especialmente aquellos datos personales –cualquiera que sea su clase, según doctrina reiterada del Tribunal Supremo (por todas STS 525/2014 de 17 de junio)– que se hallen almacenados en archivos, soportes, ficheros o registros informáticos o telemáticos y también de carácter físico o convencional, por lo que su custodia se encuentra *especialmente protegida en orden a la autorización de su inclusión, supresión, fijación de plazos, cesión de información etc., de acuerdo con la legislación sobre protección de datos* (STS 40/2016 de 3 de febrero). Se trata también en este caso de una figura delictiva que, aun manteniendo inalterada su redacción original del año 1995, da cabida a las nuevas formas de comisión vinculadas al uso de las herramientas tecnológicas. De hecho, se viene observando que la potencialidad de las tecnologías para hacer posible el acceso virtual a registros, bases de datos o ficheros en los que se almacenan informáticamente ese tipo de datos está determinando un aumento en

el volumen de denuncias por ilícitos de este tipo cometidos tanto por terceros, ajenos al registro o sistema vulnerado, como por quienes, estando autorizados para el acceso y tratamiento de la información almacenada, exceden los límites de la autorización concedida. Son por todos conocidos los ataques informáticos con dicho objetivo como el sufrido en 2014 por *Yahoo*, que supuso la exfiltración de información personal de cuentas de millones de usuarios; el que afectó a *eBay* en la misma anualidad, o la más reciente, reconocida por *Lifelabs* en diciembre del pasado 2019. Igualmente debe reseñarse que, durante la vigencia del estado de alarma motivado por el COVID-19, se han constatado accesos irregulares a sistemas informáticos de centros hospitalarios con el único objetivo de apoderarse de información personal sobre pacientes ingresados en dichos centros.

Obviamente estas conductas, cuando se cometen a través de las TIC, suelen aparecer en concurso con otras figuras delictivas incorporadas al Código Penal en las reformas operadas por las LO 5/2010 de 22 de junio y 1/2015 de 30 de marzo y particularmente con el acceso irregular a sistemas informáticos y la interceptación ilícita de comunicaciones entre sistemas (arts. 197 bis 1.º y 2.º CP), y su objetivo último es la utilización posterior de los datos sustraídos, ya sea con fines lucrativos o para su difusión a través de redes sociales como medio de intimidar, acosar o humillar a los titulares de dicha información.