

Espiar el móvil de la pareja: dos años y medio de cárcel

(Reeditado el 4 de febrero de 2020)

Así se titula un artículo publicado hoy mismo por el diario *El País* y que se puede consultar siguiendo este [enlace](#). En él, el periodista, acompañado de un magistrado de la Sala Segunda del Tribunal Supremo, de una inspectora de la Unidad de Investigación Tecnológica de la Policía Nacional y dos hackers, hacen un repaso sobre varios supuestos reales de intromisión, las resoluciones judiciales que los han resuelto, las interpretaciones de la norma que sanciona tales conductas, los instrumentos a disposición de los victimarios y algunos consejos para evitar ser víctima de una vulneración del derecho a la intimidad y a la propia imagen, especialmente en el ámbito de las relaciones entre parejas.

« Se trata de uno de los derechos básicos del ser humano que proscriben la injerencia de quien su titular no desee en el ámbito de su personalísima privacidad, que no cabe entender renunciado por el hecho de contraer matrimonio »

El artículo de prensa es mucho más sintético que este post. Aquí lo que se intenta es explotar la información que nos brinda, especialmente en cuanto a la relación de los supuestos con la norma penal y la interpretación dada por los juzgados y tribunales.

Los supuestos:

- ♦ [Fragmento del relato de hechos probados de la sentencia del juzgado de lo penal número 4 de Girona de 28 de junio de 2015](#): « El 22 de diciembre de 2014 Antonio J.S. accedió al teléfono móvil de su pareja, M.P.T., introduciendo la clave y descargó un fichero guardado en el correo electrónico con una fotografía de la señora M.P.T. (su esposa en aquel momento) con un hombre, así como varios mensajes de la aplicación *Line*, todo ello sin conocimiento de M.P.T. **No ha quedado acreditado que el acusado hiciera difusión o cesión de tales mensajes entre terceros. No ha quedado probado que el acusado realizara los actos con intención de menoscabar la integridad psíquica o causar temor a la denunciante.** Ha quedado acreditado que la señora M.P.T. ha estado 15 días de baja temporal sin que haya quedado probado que haya sido a consecuencia de los mismos ni que haya sufrido un especial sufrimiento o daño ». [Fragmento de la fundamentación jurídica](#): « no se trató de un mero fisgoneo o una visión fugaz o momentánea del contenido privado, sino que se ha hecho el acusado con el adecuado soporte material de captación del contenido ».

La sentencia refiere a que los hechos ocurrieron en el marco de un proceso de divorcio en cuyo seno el señor J.S. aportó como pruebas el material hallado en el teléfono de su esposa (sería interesante saber qué, pero sobre todo para qué, se pretendía probar una infidelidad puesto que el divorcio en España no exige causa alguna -aunque existe una excepción que no viene al caso-; también sería interesante ver, después de esta sentencia el pelaje y el rostro del abogado que le recomendó o al menos le permitió

« A mediados de julio en Jaén fue arrestado un joven acusado de instalar un programa espía en el móvil de su novia. El atestado policial incorporado al juzgado revela que ese software la permitía activar a distancia la cámara y el micrófono para escuchar las conversaciones de su pareja y tenerla permanentemente controlada. »

aportar tal material a un proceso judicial). **La condena: Dos años y medio de cárcel y multa de seis euros diarios durante 19 meses.**

Esta sentencia, pendiente de que se resuelva el recurso, sería la primera de este tipo que conllevaría el ingreso en prisión del condenado.

- ◆ **Fragmento de los hechos probados de la sentencia de la Sala de lo Penal del TS, de 21 de marzo de 2007:** « El acusado Paulino, [...], compró un ordenador y lo instaló en su casa, introduciendo su nombre de usuario y su propia contraseña. En julio de 2001 observó que las facturas mensuales de la compañía telefónica se incrementaban notablemente, porque se estaba disparando el consumo de internet, hasta 70 horas de consumo al mes, y a fin de averiguar quién utilizaba su ordenador, adquirió en su distribuidor legal en España, un programa llamado *eBlaster* para monitorizar la actividad informática y de internet desde una ubicación alejada, de forma que, desde su ordenador particular instalado en su domicilio, cada 30 minutos volcaba copia de todas las comunicaciones telemáticas a la cuenta de correo del ordenador que el acusado utilizaba en su oficina.- Al comprobar que la usuaria era su esposa Catalina, que entraba en chats con casados/infieles con conversaciones de contenido sexual y que además tenía otra pareja, contrató a una investigadora privada, la también acusada Doña Silvia, remitiéndose todos los correos interceptados aportando dicha información al juicio de separación que se avecinaba, ante la angustia y el temor a perder la custodia de su hija de tres años y que ésta se educara en un ambiente inadecuado.- Silvia, se limitó como investigadora privada a elaborar un informe con los correos que Paulino le remitía, aportarlo al juicio de familia y ratificarse en su informe, devolviendo personalmente la documentación a su cliente » (sic). **Fallo del recurso de casación:** Desestimatorio, confirma el fallo de la Sentencia de la Audiencia Provincial de Madrid de 25 de mayo de 2005 en el sentido de **ratificar la condena a Paulino como autor responsable de un delito de descubrimiento de secretos**, [...], concurriendo la circunstancia atenuante analógica del art. 21.6 (actualmente 21.7) en relación con el art. 21.3 (atenuante por arrebatado, obcecación u otro estado pasional irresistible)[...] a la pena de seis meses de prisión, y multa de seis meses con una cuota diaria de 6 euros. **Se absuelve a la investigadora Doña Silvia del delito de revelación de secretos por el cual venía siendo acusada.** »

En cuanto a los delitos, el conjunto de tipos criminales por los que se condena en los supuestos anteriores se hallan en el capítulo primero del Título X del **Código Penal**. La rúbrica del capítulo es « Del descubrimiento y revelación de secretos » y la del Título X « Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio ».

En buena técnica legislativa penal, los tipos delictivos responden a la necesidad de proteger un bien jurídico especialmente valioso, tan valioso que lo hallamos entre los **Derechos Fundamentales de nuestra Constitución**. Se trata del artículo 18 de la Constitución Española: « 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. [...]; 3. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos ».

Su reflejo en el Código Penal lo hallamos en los artículos 197 y siguientes del mismo. No obstante, para limitarnos al asunto que estamos tratando en este post sólo se analizará el artículo 197, el 197^{ter} y el 201.

Artículo 197 CP:

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

El artículo 197 del Código Penal incluye una interesante reforma que apenas ha entrado en vigor el pasado julio [por julio de 2017] la cual viene a ser el resultado de la necesidad de castigar conductas como la que afectó a la entonces concejal toledana Olvido Hormigos y que seguro será bien recordada por los lectores.

Observamos que este tipo penal requiere una finalidad, así lo destaca *El País* en su artículo haciendo referencia a la interpretación del Tribunal Supremo « El delito no es el mero fisgoneo debe haber una finalidad ». También es necesario que no exista el consentimiento expreso o tácito de la persona a cuya información íntima se accede. En cuanto al soporte de los secretos el legislador enumera una serie de ellos sin acotarlos; es decir, pueden ser los que aparecen en el precepto o cualquier documento o efecto personal, de la misma manera se ofrece una lista abierta de los medios para conseguir acceder a la información.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

En este apartado se castiga de la misma manera el apoderamiento, uso y alteración de datos reservados. La diferencia con el precepto anterior es que esos datos no tienen el mismo valor desde el punto de vista constitucional que las comunicaciones entre las personas; es decir, aquellas que implican un movimiento comunicativo en contraste con la información que simplemente se encuentra almacenada. Para que constituya un delito de este tipo es necesario que concurra el perjuicio del tercero o del titular y por supuesto, la ausencia de autorización.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

El primer párrafo establece un tipo agravado para el supuesto en el que, después de descubrir los datos reservados, o interceptar las comunicaciones, las comparta por algún medio con terceros, mientras que en el segundo se establece una pena inferior para el caso en que un sujeto que sin haber realizado ninguna actividad expresamente dirigida a obtener los datos o interceptar la comunicación la obtiene para a continuación difunde, revela o cede dichos datos o comunicaciones.

4. *Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:*

a) *Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o*

b) *se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.*

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

Este apartado agrava las penas para el caso en que las conductas señaladas en los apartados de referencia se cometan por personas con un acceso privilegiado a los datos y a las comunicaciones. En cuanto al inciso b) de este apartado, no se termina de entender la razón por la cual se agrava el castigo cuando se utilicen datos personales de la víctima puesto que el uso de estos resulta inherente a la comisión de los hechos y es difícil imaginar un supuesto en el que no recurra a ellos teniendo en cuenta que el nombre, el número del DNI o la contraseña son datos personales. Este inciso b) se ha introducido con la última reforma del Código Penal, y en la exposición de motivos el legislador no explica la razón de esta puntual modificación.

5. *Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.*

Este apartado no requiere mayor comentario, se trata de que cierta información y ciertos colectivos son especialmente sensibles por lo que requieren una protección más enérgica.

6. *Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.*

Este apartado por un lado castiga con más dureza si la finalidad de los actos incluye el beneficio económico y tratándose de datos especialmente sensibles como los del apartado cinco, la dureza del legislador es máxima.

7. *Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.*

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

En este apartado se introduce con la última reforma del Código Penal y es el que responde a la problemática convertida en alarma social por el caso *Hormigos*. La particularidad de este apartado es que aun cuando existió el consentimiento para el descubrimiento de la información o bien, para el acceso a la comunicación – que curiosamente se limita a imágenes o grabaciones audiovisuales por lo que, por ejemplo, un correo de alto contenido erótico estaría excluido del supuesto contemplado – no lo hay para difusión, revelación o cesión. Además es necesario que exista un menoscabo grave en la intimidad personal de la persona afectada.

El castigo se endurece cuando el actor sea o haya sido cónyuge o mantenga (o haya mantenido) una relación análoga de afectividad sin que sea necesaria la convivencia. Antes de la reforma el castigo se agravaba acudiendo a la circunstancia mixta (atenuante o agravante) de parentesco del artículo 23 del Código Penal.

Artículo 197^{ter} CP:

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

- a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o*
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.*

Este artículo a quien castiga es al individuo o empresa (puesto que este delito en particular puede ser cometido por personas jurídicas) que desarrolle sistemas o técnicas para cometer los delitos del artículo 197 o que *craquee* contraseñas para lograr acceder a la información o a las comunicaciones protegidas.

Artículo 201 CP:

- 1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.*
- 2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.*
- 3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130.*

Los delitos de este capítulo I del título X del Código Penal, con la excepción del art. 198 (delitos de este tipo cometidos por funcionarios o autoridades públicas) son de los considerados como semi-públicos. Al respeto de éstos, el ministerio fiscal o los órganos jurisdiccionales no actúan de oficio en un momento inicial sino que es necesario que el agraviado denuncie previamente salvo cuando el

agraviado sea uno de los individuos que merecen especial protección como los señalados o bien cuando existe un perjuicio general a la sociedad o a un grupo relevante de personas (habrá que delimitar caso a caso que se considera como grupo relevante).

Pasa a menudo y es posible, dada la naturaleza de estos delitos, que el agraviado perdone al denunciado y con ello decaiga la acción penal. No obstante, tratándose de menores o incapacitados los jueces o tribunales podrán rechazar que el perdón tenga los efectos aquí señalados ordenando en consecuencia que continúe el procedimiento. El momento para que el ofendido exprese su perdón puede ser cualquiera siempre y cuando lo emita antes de que se dicte sentencia.

La explicación del Magistrado:

Entrevistado por el diario, Don Miguel Colmenero Menéndez de Luarca, magistrado de la sala segunda del Tribunal Supremo explica que el derecho a la intimidad es uno de los más importantes que reconoce la Constitución y que por lo tanto su adecuada protección justifica una combinación con una pena privativa de libertad; no obstante, puntualiza que no se puede decir con carácter general que coger el teléfono de una persona y mirar el WhatsApp conlleva un delito. Hay conductas admitidas socialmente de personas que comparten el contenido de sus correos electrónicos que no ingresarían en la conducta típica del delito. Esto cambia cuando la finalidad busca descubrir los secretos del otro y si como consecuencia de ello, la intimidad queda afectada.

¿Terminaste la lectura y aún te quedan dudas? ¿Estás involucrada o involucrado en una situación por el estilo y necesitas orientación?. En cualquier caso, no dudes en contactar con tu abogado. Si te parece que ese abogado puedo ser yo, no dudes en contactarme.

Pastor A. Cañas Pérez
Director del Estudio Legal
Colegiado ICAM 125168