Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. El art. 18 de la CE garantiza la protección de la intimidad en todas sus manifestaciones; en el apartado 1, a la intimidad personal y familiar y a la propia imagen; en el apartado 2, a la inviolabilidad de domicilio; en el 3, el secreto de las comunicaciones, y en el apartado 4, garantiza la intimidad con la limitación del uso de la informática.

El CP de 1995 intenta abordar en el Título X del Libro II una tutela global de la intimidad, que en el texto anterior se limitaba al secreto. Dedica ahora dos capítulos, «Del descubrimiento y revelación de secretos», y el segundo, «Del allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público».

El bien jurídico que se protege es la intimidad, que abarca las manifestaciones concretas a que se refiere el art. 18 de la CE y que se extiende a diversos ámbitos de aplicación: intimidad corporal, intimidad domiciliaria, intimidad económica y secreto bancario, intimidad médica, intimidad de correspondencia, intimidad informática, etc.

En el delito de descubrimiento y revelación de secretos, se tutela penalmente la intimidad personal, protegida en el art. 18 de la CE y entendida, en sentido amplio, como el derecho de todo individuo a mantener un ámbito de privacidad, reservado frente a la injerencia y conocimiento de tercero, ámbito necesario para el ejercicio de otros derechos y el libre desarrollo de la personalidad. En el allanamiento de morada es la inviolabilidad de domicilio o lugar reservado de la persona para el desarrollo de sus aspectos básicos.

Estos tipos delictivos entroncan, por consiguiente, con el derecho fundamental a la intimidad personal y familiar, reconocido en el art. 18.1 de la CE. Como establece la STC núm. 134/1999, de 15-7, lo que tal precepto constitucional garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio y pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibir su difusión no consentida, lo que ha de encontrar sus límites en los restantes derechos

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

fundamentales y bienes jurídicos constitucionalmente protegidos. Indican las SSTC 186/2000, de 10-7, y 119/2001, de 29-5, que el derecho a la intimidad garantiza la existencia de un ámbito propio y reservado frente a la acción y conocimiento del demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida. Este derecho fundamental, como dicen las SSTC 156/2001, de 2-7, y 121/2002, de 20-5, se halla estrechamente vinculado a la propia personalidad y deriva de la dignidad de la persona que el art. 10.1 de la CE reconoce, de tal suerte que atribuye a su titular el poder de resguardar dicho ámbito frente a la divulgación del mismo por terceros y frente a una publicidad no querida.

En el ámbito normativo, debe mencionarse la LO 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal que deroga la LO 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, modificada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible en su Disposición final quincuagésima sexta, y la LO 1/1982 de Protección del Honor, la Intimidad Personal y Familiar y la Propia Imagen. Y en el ámbito internacional, el Convenio sobre la Ciberdelincuencia del Consejo de Europa hecho en Budapest, 23.11.2001 y el Protocolo Adicional de 2008, ratificado por España el 3 de junio de 2010, si bien debe advertirse que en nada integran los tipos penales pues no nos hallamos ante normas penales en blanco.

2. DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

Se tipifica el descubrimiento y revelación de secretos en el art. 197 CP que después de la reforma operada por LO 5/10 de 22 de junio se divide en 8 apartados (se crean dos nuevos apartados, el 3 y el 8), con un tipo básico que se estructura básicamente sobre dos conductas diferenciadas, y varios subtipos agravados. Dos tipos especiales en los arts. 198 y 199 que se diferencian de los delitos comunes en cuanto que solo determinadas personas pueden ser sujetos activos de los mismos, al exigirse una determinada condición en ellos. En cuanto al sujeto pasivo, también alcanza a las personas jurídicas, tal y como se prevé en el art. 200 CP, y finalmente, el art. 201 establece determinadas condiciones de procedibilidad.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Debe exigirse, en todo caso, cierta entidad en los secretos. En este sentido, la doctrina ha venido reconociendo la operabilidad del principio de insignificancia, con aceptación por parte de la jurisprudencia, principalmente en aquellos tipos que presentan una dualidad de sanción según su gravedad o levedad, por tanto, como constitutivos de delito o de falta, así se pronuncia la AAP de Madrid, Sec. 3.ª núm. 690/2008, de 19-11, que señala que «una conducta de entidad objetivamente insignificante no puede convertirse en típica por la percepción subjetiva de la persona afectada, pues la consideración contraria equivaldría a someter la trascendencia de hechos objetivos a la reacción subjetiva y variable del destinatario, en este caso la publicación de la noticia de la celebración de un matrimonio concluye carece de antijuridicidad material».

2.1. Tipo básico

2.1.1. Apoderamiento para descubrir o interceptación de las comunicaciones

2.1.1.1. Apoderamiento para descubrir

El tipo básico es, y en esto existe acuerdo doctrinal, el recogido en el párrafo primero. Dice el art. 197.1:

«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 o 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».

Pues bien, el objeto de protección en el art. 197.1 CP no es otro que la intimidad de las personas, entendida como la esfera en la que se desarrollan determinadas facetas reservadas de la persona, o su privacidad en cuanto conjunto de aspectos de la personalidad del sujeto que aisladamente considerados pueden carecer de significación intrínseca, pero que enlazados entre sí arrojan como resultado un «retrato» de la personalidad del individuo que este tiene derecho a mantener reservado. Como señala la STC 70/02, «es doctrina constitucional reiterada que el derecho a la intimidad personal

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

garantizado por el art. 18.1 CE, en cuanto derivación de la dignidad de la persona reconocida en el art. 10.1 CE, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura para mantener una calidad mínima de la vida humana». Se trata de tutelar datos, efectos personales, noticias, etc., que deben quedar a reserva del conocimiento de las demás por voluntad expresa o tácita del titular, de suerte que el contenido de los documentos, cartas, efectos personales, etc., revista objetivamente relevancia para hacerle merecedor de tutela penal. Por consiguiente, es necesario que la conducta de apoderamiento intencional haya puesto en peligro el bien jurídico protegido, la intimidad personal, con independencia de que el sujeto llegue o no a utilizar el contenido de los objetos de que se apoderó. Teniendo en cuenta para determinar cuándo un dato, efecto o documento es relevante para la intimidad no hay que atender solo a la voluntad del perjudicado, sino que en aras de la seguridad jurídica, habrá que conjugar esa voluntad del interesado con la existencia de un interés jurídicamente relevante, conforme a criterios de adecuación social y objetiva de los datos o documentos para materializarse en ellos una proyección de la intimidad personal.

Obviamente, el consentimiento del titular del bien jurídico protegido, que no se confunde siempre con el titular del secreto, es relevante, constituye una causa de exclusión del tipo; se configura, pues, como elemento negativo del tipo que determina la atipicidad de la conducta.

La difusión de la imagen de una menor a través de terminales móviles entre personas menores de edad de su entorno por la red social «WhatsApp» -que se habría producido por la recepción inicial y voluntaria de dicha imagen en el móvil del chico con el que mantenía una relación por esas fechas, a partir de cuyo momento se produce una difusión en escala en el que participaron como receptores y divulgantes, otros dos menores, es considerada atípica por la SAP Granada 351/2014, de 5 de junio. Para esta Sala los hechos no encajan en ninguna de las conductas que regula el art. 197 CP, por muy execrables que puedan parecer.

Así, pone de manifiesto que las conductas del citado precepto exigen, con carácter general, un acceso inconsentido a un secreto, y en el caso de autos, ni

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

hubo acceso, por cuanto los tres acusados lo que hicieron fue recibir, y no acceder, un mensaje de imagen, ni cabe hablar de “no consentimiento” cuando lo que desencadena la difusión "en cascada" del mensaje es un acto previo de la menor, como lo es su remisión al teléfono móvil de su “novio”. Tal consentimiento –asevera la Sala- debe considerarse válido aunque la menor cuente a fecha de los hechos con quince años de edad, pues si el Legislador viene a considerar válido el consentimiento de una persona a partir de los trece años para mantener relaciones sexuales, parece evidente que también debe considerarse válido dicho consentimiento para remitir una fotografía donde aparece desnuda, con un alto contenido sexual. Aduce la Audiencia, no obstante lo anterior, que pueden quedar a salvo las acciones, en su caso, que la menor, o quienes la representen, puedan ejercitar por la intromisión ilegítima sufrida, al amparo de la LO de 5 de mayo de 1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El sexting supone el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consienten en ello y que forma parte de su actividad sexual, que se desarrolla de manera libre. La difusión de las imágenes por sus receptores no encuentra encaje en las conductas que describe el citado artículo, y por ello, el legislador, tras un escándalo mediático a raíz del conocido caso de una exconcejal -que envió un vídeo sexual que fue distribuido por su amante vía «whastsapp»-, pretende introducir una nueva conducta en el art. 197 CP (4º bis) en el Proyecto de Código Penal, que alude a los casos de obtención consentida de imágenes íntimas con difusión inconsentida posterior. El nuevo precepto, caso de aprobación, establecería:

«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 aquella que hubiera obtenido con su anuencia en un domicilio o en cualquiera otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona».

Significan, las SSTS de 23 de octubre de 2001, la SAP Madrid, Sec. 7.ª, núm. 205/2008 de 17-7, o el AAP de Madrid, Sec. 4.ª, 15-1-2007, que, «si bien el tipo

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

penal se ubica en el capítulo I del Título X del Libro II del CP, bajo la rúbrica, de «Del descubrimiento y revelación de secretos», lo cierto es que el art. 197.1, tutela dos bienes distintos, que son objeto de la protección jurídico penal, la salvaguarda de los secretos propiamente dichos y la intimidad de las personas; viniendo a representar este tipo penal una especie de desarrollo sancionador a las conductas que vulneren el derecho fundamental a la inviolabilidad de las comunicaciones consagrado en el art. 18 CE, como parte integrante del derecho a la intimidad personal del individuo».

Resalta la STS 694/2003, de 20 de junio, que respecto al iter criminis, es una figura delictiva que se integra en la categoría de los delitos de intención, y en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse.

La conducta típica ha de ser dolosa, pues no se recoge expresamente la incriminación imprudente (art. 12 CP), que ha de llevarse a cabo con la finalidad de descubrir secretos o vulnerar la intimidad, ya que la dicción literal del precepto emplea la preposición para. Por tanto, dicho delito solo admite naturaleza dolosa, dolo específico requerido por esta figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de privacidad e intimidad. En este sentido, el tipo que nos ocupa exige un elemento subjetivo del injusto, cual es la intención de vulnerar los secretos o la intimidad de otro, debiendo entenderse por «secretos», por razones de tipo sistemático (utilización en el Título relativo a los delitos contra la intimidad) y de tipo teleológico en atención al bien jurídico protegido, tan solo los «secretos personales», y no cualesquiera otros, como los profesionales, políticos, etc. Lo que excluye tanto los apoderamientos accidentales o negligentes como los apoderamientos carentes de esa finalidad o intención descubridora.

ATENCIÓN. Pese a la ubicación sistemática del art. 197, lo cierto es que dicho precepto tutela dos distintos bienes que son objeto de la protección jurídico penal: la salvaguarda de los secretos propiamente dichos y, aparte, la intimidad de las personas. El tipo requiere del dolo, es decir, del conocimiento por el

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

autor de los elementos del tipo objetivo, y además de un especial elemento subjetivo consistente en que la acción se ejecuta con la finalidad («para») de descubrir los secretos o vulnerar la intimidad de otro. No es suficiente, pues, un dolo genérico.

Por secreto ha de entenderse el conocimiento reservado a un número limitado de personas y oculto a otras. No ha de confundirse con el concepto vulgar de secreto. Secreto será, pues, todo conocimiento reservado que el sujeto activo no conozca, o no esté seguro de conocer, y que el sujeto pasivo no quiera que conozca. Desde luego será irrelevante que, una vez descubierto el secreto, el sujeto activo ya lo conociera previamente: la confirmación del mismo constituye una conducta típica.

El bien jurídico protegido es la intimidad individual. Aunque la idea de secreto puede ser más amplia, como conocimientos solo al alcance de unos pocos, en realidad deben estar vinculados precisamente a la intimidad pues esa es la finalidad protectora del tipo. En este sentido, la STS 666/2006, de 19 de junio, que plantea la delimitación del campo semántico de los términos «secretos» e «intimidad», en la que se dice que «la idea de secreto en el art. 197.1 CP resulta conceptualmente indisociable de la de intimidad: ese ámbito propio y reservado frente a la acción y el conocimiento de los demás». Así se desprende de la ubicación del precepto en el Título dedicado a los delitos contra la intimidad, y es coherente con su propia redacción, pues en el primer apartado relaciona los papeles, cartas o mensajes de correo electrónico con otros documentos o efectos personales. Y en el segundo apartado se refiere a datos reservados de carácter personal o familiar. No es preciso que pertenezcan al núcleo duro de la privacidad, pues de ser así se aplicaría la agravación del apartado sexto del art. 197, pero es necesario que afecten a la intimidad personal. Igualmente STS 358/2007, 30-4, que señala que la idea de secreto puede ser más amplia, como conocimientos solo al alcance de unos pocos, en realidad deben estar vinculados precisamente a la intimidad, pues esa es la finalidad protectora del tipo.

La SAP de Madrid, Sec. 7.ª, núm. 205/2008, de 17-7, recoge la SAP de Las Palmas, Sección 1.ª, de 3 de diciembre de 1999, que dice «sea lo que fuere, insistimos, habida cuenta de que el bien jurídico protegido es la intimidad ajena,

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

debe recalcarse que dicho ámbito de tutela no tiene porque corresponderse con un ámbito de desconocimiento absoluto frente a todos. Sí es cierto que se trata de tutelar datos que han de quedar a reserva del conocimiento de los demás por voluntad expresa o tácita del titular, no es menos verdad, sin embargo, que la dilucidación de cuando estamos ante un dato, efecto personal o documento relevante para la intimidad no es algo que pueda fiarse de forma exclusiva a la voluntad del titular de los mismos. Hace falta, pues, conjugar la voluntad del sujeto con la existencia de un interés relevante jurídicamente. Por lo tanto los objetos reconducibles al ámbito de la integridad relevante deben delimitarse, teniendo en consideración criterios de adecuación social y, sobre todo, atendiendo al dato de que se trate de objetos en los que se pueda materializar una proyección de la intimidad del sujeto. En palabras del TS, referidas a la protección penal de los datos reservados, prevista en el art. 197 del CP, no es fácil precisar, a priori y en abstracto, cuando el desvelamiento de un dato personal o familiar produce ese perjuicio (de tercero). Baste ahora con decir que lo produce (el perjuicio de tercero) siempre que se trata de un dato que el hombre medio de nuestra cultura considera "sensible" por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no transciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar (STS de 18 de febrero de 1999)».

En cuanto a la alegación de error, la STS 237/2007, de 21-3, señala que «el tipo requiere del dolo, es decir, del conocimiento por el autor de los elementos del tipo objetivo, y además de un especial elemento subjetivo consistente en que la acción se ejecuta con la finalidad ("para") de descubrir los secretos o vulnerar la intimidad de otro. No solo, pues, dolo genérico. Es indiferente a los efectos de este primer apartado la finalidad ulterior del autor, aunque la existencia de un propósito lucrativo tiene su reflejo en el apartado sexto del mismo precepto. Los hechos consisten en la instalación de un programa que permite conocer los movimientos u operaciones realizados desde un determinado ordenador. En principio, en cuanto se trata de un acto de protección de la propiedad privada que no afecta a derechos de los demás, es un acto legítimo, pues parece claro que el propietario del ordenador puede instalar un programa que le permita verificar el uso que se da a ese instrumento, cuando sospecha razonablemente que está siendo utilizado de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

forma no autorizada. Es cierto, como argumenta, que en el momento de la instalación del referido programa no puede establecerse que su finalidad fuera conocer los mensajes o conversaciones de aquellos terceros que utilizaran el ordenador y la línea de Internet sin estar autorizados por quien era su propietario, pues no se declara probado que desde el primer momento supiera que el programa facilitara el contenido íntegro de las comunicaciones de una forma que hiciera inevitable su conocimiento. Esa acción no puede reputarse inicialmente ilícita. Pero esta valoración no permite ir más allá. Y desde luego no autoriza a invadir la privacidad ajena. De otro lado, es relevante la conducta del recurrente consistente en apoderarse del contenido de las conversaciones y comunicaciones privadas de su esposa, una vez que había comprobado que era ella quien utilizaba el citado ordenador para comunicarse con terceros. La cuestión no permite albergar duda alguna una vez que el recurrente conoció el contenido del primero de los correos, pues desde ese momento pudo tener, y sin duda tuvo, la seguridad de que se trataba de comunicaciones íntimas de su esposa, que afectaban al ámbito de su intimidad más estricta, a las que no podría pretender tener acceso legítimamente aun cuando se realizaran desde su ordenador personal, a pesar de lo cual continuó apoderándose de dichas comunicaciones. Es esta segunda fase de la conducta la que la sentencia ha considerado delictiva en cuanto comprendida en las previsiones del art. 197.1 del CP, pues la acción del acusado recurrente, una vez que conoció la naturaleza del contenido de las comunicaciones interceptadas e identificó a los comunicantes, se orientó con claridad al apoderamiento de datos relativos a la intimidad estricta de otra persona que constituían secretos de ésta en cuanto no resultaban accesibles a terceros de forma indiscriminada.

A los efectos del delito, es indiferente que el fin último del autor fuera utilizar el contenido de esas conversaciones, que él valoró como negativas para su esposa, en el procedimiento de separación matrimonial para con ello impedir que se acordara por el Juez la privación de la custodia de la hija. No existe duda alguna que la finalidad de la continuación en el uso del programa informático era precisamente continuar apoderándose de las comunicaciones privadas, aunque después pretendiera darles una u otra utilidad, de donde resulta el dolo específico referido a la finalidad de descubrir los secretos de otro o de vulnerar su intimidad».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

En este mismo sentido se ha pronunciado la STS 1641/2000, de 23 de octubre, que decía que «lo relevante a efectos de la configuración del tipo no es la apertura de la correspondencia, sino el apoderamiento de su contenido sin consentimiento, que es lo que constituye la conducta típica sancionada por el legislador, extremo éste que ha quedado acreditado por prueba de cargo demostrativa de que la acusada hizo suya la misiva enviada al marido por la Seguridad Social utilizándola como prueba contra éste en un proceso civil y en beneficio propio».

«Parece evidente que cualquier persona sabe que el acceso a las comunicaciones íntimas y personales de otra afecta a su intimidad, e igualmente, que la esfera más íntima del sujeto está protegida por la ley de la invasión de terceros no autorizados. Asimismo es notorio que las cuestiones relativas a la vida sexual de la persona constituyen parte del núcleo del concepto de intimidad. Es evidente también que la relación conyugal, o las equiparables a ella, incluso aunque no se encuentre en trámites previos a la separación, no autorizan el acceso a los secretos del otro integrante de la pareja. Desde este punto de vista no puede aceptarse la alegación del desconocimiento de la ilicitud. El recurrente afirma, por otro lado, que no era su intención invadir la intimidad sino proteger a la hija de ambos. El dolo de consecuencias necesarias es suficiente para el tipo subjetivo. El recurrente sabía que actuando de esa forma, es decir, accediendo al contenido de las comunicaciones privadas de su esposa, invadía su intimidad, de forma que su intención final no era relevante respecto del dolo. De otro lado ya ha sido tenida en cuenta por el Tribunal, que ha apreciado una atenuante como muy cualificada al estimar una menor culpabilidad en el hecho. Finalmente, afirma que se había asesorado técnicamente consultando a su abogado. No consta precisamente el contenido y alcance del asesoramiento. En cualquier caso, finalmente, la ilicitud de la conducta es de tal claridad que un eventual consejo de terceros no excluiría la culpabilidad del acusado. Por todo ello, el motivo se desestima».

La SAP de Badajoz, Sec. 3.ª, núm. 215/2007, 19-12, recoge la doctrina del TS en materia de error de prohibición; señala, que «para excluir el error resulta suficiente con que pueda racionalmente inferirse que el agente tenía conciencia de una alta probabilidad de ilicitud en su conducta. Es clara también tal doctrina

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

en cuanto a lo siguiente: a) que no cabe invocar el error cuando se utilizan vías de hecho desautorizadas por el ordenamiento jurídico que todo el mundo sabe y a todo el mundo consta que están prohibidas, y b) que para excluir el error no se requiere que el agente tenga seguridad respecto de un proceder antijurídico, pues basta con que tenga conciencia de una alta probabilidad de antijuridicidad, lo que por estimarse similar al dolo eventual no merece trato de benignidad alguno. También se señala la dificultad de determinar la existencia de error, por pertenecer al arcano íntimo de la conciencia de cada individuo, sin que baste su mera alegación, sino que deberá probarse, tanto en su existencia como en su carácter invencible; además "no cabe invocar el error cuando se utilizan vías de hecho desautorizadas por el ordenamiento jurídico, que todo el mundo sabe y a todos consta que están prohibidas", añadiendo que, en el caso de error iuris o error de prohibición, impera el principio ignorantia iuris non excusat, no permitiendo conjeturar o invocar tales errores en infracciones de carácter natural o elemental, cuya ilicitud es «notoriamente evidente y de comprensión y constancia generalizada. En el caso que estudia señala que precisamente en este aspecto, en el que la ilicitud de la conducta es evidente ya que no cabe siquiera imaginar que, no ya sólo el hombre medio, sino a todos los niveles, pueda pensar que dar a conocer de manera generalizada imágenes en que se muestran escenas de la vida sexual de terceros es una conducta amparada legalmente, pues no es arriesgado afirmar que todo el mundo sabe tal conducta está prohibida, de manera que no parece en modo alguno razonable considerar la posibilidad de error de clase alguna en un caso como el presente».

En cuanto a las modalidades, el art. 197.1 tipifica dos conductas: el apoderamiento para descubrir y la interceptación de las comunicaciones. La SAP Madrid, Sec. 7.ª, núm. 205/2008 de 17-7, recordando las SSTS de 10-12-2004, 20-6-2003, 14-5-2001 y 14-9-2000, señala que «el apartado 1 contempla el tipo básico, aunque en realidad contiene dos tipos básicos definidos por modalidades comisivas distintas, como son el apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, y la interceptación de las telecomunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

ATENCIÓN. Conclusión: el tipo básico del art. 197 CP regula dos modalidades comisivas distintas, la primera, en la que la conducta típica consiste en el apoderamiento de documentos o efectos personales; y, la segunda, en que la conducta típica consiste en el control ilícito de las señales de comunicación y en el control auditivo y visual clandestino.

La conducta consiste en apoderarse de los secretos para descubrir, sin necesidad de ulterior divulgación. Se consuma el delito con el mero apoderamiento para descubrir, y por tal ha entendido la jurisprudencia la aprehensión u obtención ilícita, así como también la retención de lo recibido por error. Es indiferente el fin último perseguido por el autor, incluido su voluntad de presentarlo en un juicio (STS 21 febrero 2007). Cabe la posibilidad de admitir la tentativa, siempre, claro, referida a la conducta de apoderamiento, no a la de conocer, en la medida que el precepto castiga tanto la clásica conducta de apoderarse para descubrir, como ahora también la de apoderarse para vulnerar la intimidad. En definitiva, basta con la intromisión no consentida en la intimidad de una persona física, para que la infracción quede completamente consumada.

En cuanto a la naturaleza de este ilícito, se define por la doctrina, como se dijo, en delito imperfecto mutilado de dos actos, que no requiere para la consumación el efectivo descubrimiento de los secretos o datos íntimos contenidos en los documentos, papeles, cartas o mensajes electrónicos. El sujeto debe apoderarse de estos objetos para descubrir los secretos o vulnerar la intimidad de otro; se acude así a la presencia de un elemento subjetivo del injusto para adelantar el momento de la consumación al acto de apoderamiento intencional, sin que sea precisa la efectiva toma de conocimiento de lo que contiene el documento para la perfección típica. El efectivo descubrimiento de la intimidad documental de otro, tan sólo juega un papel de engarce de este tipo básico con el tipo agravado de difusión o revelación tipificado en el núm. 4 del art. 197; pero debe subrayarse que ese efectivo conocimiento es un elemento que se sitúa extramuros de la perfección del tipo básico expresado en el art. 197.1 CP.

La SAP Madrid, Sec. 7.ª, de 17-7-2008 señala que «el apoderamiento de papeles no exige la aprehensión física de los mismos, pues basta su

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

aprehensión virtual, de manera que el sujeto activo del delito se haga con el contenido de cualquier forma técnica que permita su reproducción posterior, por lo que el delito se consuma tan pronto se acceda a los datos; se trata de un delito que no precisa para su consumación el efectivo descubrimiento del secreto o de la intimidad del sujeto pasivo, pues basta la apropiación del documento o la utilización del sistema de grabación o reproducción del sonido o de la imagen (elemento objetivo) junto con la finalidad señalada en el precepto de descubrir los secretos o vulnerar la intimidad (elemento subjetivo), debiendo ser dolosa la conducta típica, pues no se recoge expresamente la conducta imprudente, exigida conforme al art. 12 del CP, y ha de llevarse a cabo con la finalidad de descubrir secretos o vulnerar la intimidad, ya que la dicción literal del precepto emplea la preposición "para"; la acción del agente ha de estar encaminada a conocer secretos de la persona espiada sin el consentimiento de ésta, invadiendo y violentando el ámbito de su intimidad personal como medio de acceso a dichos secretos, entendiendo por éstos lo desconocido u oculto, es decir, todo conocimiento reservado que el sujeto activo no conozca o no esté seguro de conocer y que el sujeto pasivo no desea que se conozca».

La STSJ de Castilla-La Mancha, Sec. 1.ª, de 30-10-2008, en relación al acto de apoderamiento, menciona, que «este hace referencia a una idea de sustracción o desposesión del sujeto pasivo llevada a cabo por el sujeto activo sin su consentimiento, y que recae sobre las cartas, papeles, mensajes o documentos de éste. Como señalan las SSTS de 23 de octubre de 2000 y 21 de marzo de 2007 lo relevante a efectos de la configuración de la indicada modalidad delictiva "no es la apertura de la correspondencia, sino el apoderamiento de su contenido sin consentimiento". Ahora bien, aun cuando es verdad que el TS viene admitiendo además del apoderamiento físico o material de la correspondencia, documentos o efectos, como conductas equivalentes, la retención de la misma o la utilización de dicho material hecha con la finalidad de descubrir los secretos o vulnerar la intimidad, o la denominada aprehensión virtual, pudiendo citar además de la indicada las SSTS de 14 de septiembre de 2000 y 21 de marzo de 2001, en las que se afirma que fotocopiar un documento y utilizarlo equivale a su apoderamiento; sin embargo, en los hechos relatados en ningún caso se habla de desposesión o apoderamiento ni físico ni virtual o que de cualquier otro modo suponga una noción equivalente a

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

la recogida en el tipo, limitándose a describir una simple conducta de apertura y acceso a la correspondencia para conocer su contenido, lo que no basta para integrar la conducta típica. Dicha conducta podrá considerarse desde luego todo lo reprobable que se quiera pero no se incardina en el ilícito penal. Por otro lado, el delito imputado ha de recaer sobre cartas o documentos con el propósito de descubrir los secretos o vulnerar la intimidad de otro, lo que implica que no cualquier contenido documental está amparado por la protección penal que brinda el art. 197.1 del citado Código sino sólo aquellos que incorporen secretos o se refieran a la intimidad de otro, lo que hace preciso examinar qué se entiende por secretos o intimidad protegida penalmente».

Objeto del apoderamiento han de ser «papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales». Por consiguiente, ha de recaer sobre cartas o documentos con el propósito de descubrir los secretos o vulnerar la intimidad de otro, lo que implica que no cualquier contenido documental está amparado por la protección penal que brinda el art. 197.1 del citado Código sino sólo aquellos que incorporen secretos o se refieran a la intimidad de otro, lo que hace preciso examinar qué se entiende por secretos o intimidad protegida penalmente, en los términos ya expuestos.

Por último, ha de tenerse en cuenta en razón del principio de especialidad lo dispuesto en los arts. 583 y siguientes, para los casos en que se vea afectada la seguridad nacional, así como lo previsto en los arts. 278 y siguientes cuando se trata de secretos de empresa.

2.1.1.2. Interceptación de las comunicaciones

Tal conducta se recogía en el texto penal anterior en el antiguo art. 497 bis CP, si bien se amplía añadiendo ahora la imagen. Se cubre así una importante laguna en relación a los nuevos medios técnicos como pudieran ser el fax o el video. Sin embargo, la conducta más habitual consiste en interceptar las comunicaciones telefónicas.

En cuanto a la estructura y requisitos se reproduce lo dicho en relación a la anterior conducta, el ánimo de descubrir los secretos de otro o de vulnerar su intimidad, constituyen el auténtico elemento fundamental del precepto, pues la

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

interceptación o utilización ha de hacerse precisamente para ello. La estructura típica de ambas conductas es la misma, diferenciándose en los instrumentos utilizados.

Las escuchas telefónicas, acordadas judicialmente, y por tanto ajenas al ámbito de este delito, han sido objeto de numerosos pronunciamientos judiciales, particularmente en cuanto a los requisitos básicos para su adopción en el seno de la investigación criminal como en cuanto a su validez como prueba cuando se aportan al acto judicial y su incidencia en el derecho fundamental de la intimidad.

La STS 587/2007, de 28-6, recuerda que «el tenor del art. 18,3 CE hace patente que la garantía que él mismo establece con todo rigor, es de naturaleza formal y ampara esa clase de procesos en su totalidad, es decir, incluida la propia existencia del acto comunicativo como tal, la identidad de los que participan en él y, por supuesto, el contenido del mismo. El TC, ya en su bien conocida sentencia 114/1984, de 29 de noviembre, afirmó con rotundidad que "el concepto de secreto", que aparece en el art. 18-3 CE, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de ésta, como por ejemplo, la identidad subjetiva de los interlocutores»; recordando que la STEDH, de 2 de agosto de 1984, en el caso Malone, «reconoce expresamente la posibilidad de que el art. 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que, como el llamado comptage, permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación mismo». Que es por lo que «ponerlos en conocimiento de la policía, sin el consentimiento del abonado, se opone también al derecho confirmado por aquel precepto». En tal sentido se ha expresado el propio TC en su sentencia 123/2002, de 20 de mayo. Por tanto, también la obtención de los llamados "datos externos" al contenido de la comunicación, del tipo de los solicitados inicialmente en esta causa, tiene la naturaleza de verdadera y propia interceptación, a efectos constitucionales y legales, y está sujeta al mismo régimen, tanto en el plano de los requisitos como en el de las consecuencias asociadas a la infracción de éstos».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Además del sonido, se refiere también el precepto a la imagen, a la utilización de «artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación». La SAP de Las Palmas, Sec. 2.ª, núm. 358/2008 de 2-10, se refiere a la submodalidad delictiva del control audiovisual clandestino, que participa por completo de la naturaleza jurídica propia del delito, la estructura del tipo requiere de un elemento objetivo consistente en una acción de grabar que suponga una injerencia ilegítima en la intimidad ajena; y, de un elemento subjetivo, que implica que la finalidad del autor sea la de descubrir la referida privacidad ajena.

Pues bien, los hechos imputados al acusado en dicho procedimiento, SAP 358/2008, no son subsumibles en el tipo del art. 197 CP porque «no concurre el requisito objetivo exigido por el mismo, habida cuenta que la grabación, por muy clandestina que sea y cualquiera que sea su finalidad, de un personaje público y en un lugar público, no se puede entender como una intromisión ilegítima a su intimidad a la luz de la doctrina del TC al respecto de la configuración y límites del derecho fundamental a la intimidad. La recurrente pretende equiparar a los efectos del bien jurídico protegido la privacidad de las instalaciones de un hotel -la piscina- con las de un domicilio particular, pero tal equiparación está destinada al fracaso porque aquellas se tratan por definición de un lugar abierto al público y, por tanto, no de alguno de los sitios de la esfera donde la persona ejerce su ámbito más propio y restringido de intimidad. La sentencia impugnada basa el fallo absolutorio porque conforme a la doctrina del TC en materia de derechos fundamentales a la intimidad y a la información la acción de grabar en una piscina a una persona pública tomando el sol no es en sí un acto que pertenezca a la esfera íntima de una persona protegida penalmente por el tipo objeto de acusación, ni se ha practicado prueba acreditativa de que dicha acción estuviera orientada a descubrir los secretos ni a atentar contra la intimidad de la acusadora».

2.1.2. Los delitos cometidos a través de los medios informáticos

En el art. 197.2 CP se establece que:

«Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

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».

Las conductas consisten en apoderarse, utilizar o modificar, «en perjuicio de tercero», los datos reservados. Ha de tratarse de datos reservados de carácter personal o familiar, extendiéndose la sanción penal, en el último inciso, al que, sin estar autorizado, accediere por cualquier medio a tales datos y a quienes los altere o utilice en perjuicio de su titular o de un tercero.

Dicho párrafo segundo del art. 197 contempla la tutela penal de la libertad informática (habeas data; o «derecho a la autodeterminación informática» según lo denomina el Tribunal Constitucional alemán).

ATENCIÓN. El ATS de 11-2-2009, señala que «el art. 197.2 CP describe el tipo básico de los recientemente llamados por la doctrina delitos contra la libertad informática o habeas data, esto es, de los delitos que atentan contra la intimidad de las personas desvelando, o más ampliamente, haciendo un uso ilegítimo de los datos personales insertos en un programa informático», señalando que en cada una de las conductas descritas en los dos incisos de dicha norma la acción es prácticamente la misma: apoderarse, utilizar o modificar en el primer inciso y acceder por cualquier medio, utilizar o modificar en el segundo. El objeto de la acción delictiva es exactamente el mismo: «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».

El precepto, en cuanto a la conducta típica, está estructurado en dos partes. En ambas el objeto sobre el que ha de recaer las diversas modalidades de la conducta es idéntico: «datos reservados de carácter personal o familiar ajenos». El problema principal del objeto material en que recae la conducta típica del art. 197.2 se centra en determinar qué se entiende por «datos reservados». Un sector doctrinal amplio considera que todos los datos incorporados a un soporte informático son reservados. Para ello se basan en lo dispuesto por la LO 15/1999, de 13 de diciembre, de Protección de Datos de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Carácter Personal (LOPDCP), que otorga igual protección a todos los datos informatizados. Hay otro sector que opina, por el contrario, que los datos reservados son los que pertenecen exclusivamente al núcleo duro de la privacidad. Y es que, efectivamente, podría interpretarse que el legislador al utilizar la expresión «reservados», se refiere a los datos que directamente afectan a la privacy (incluso fuera del sistema informático -salud, ideología, creencias-), de forma que la tutela administrativa operaría para el resto de datos personales. Pero esta interpretación no puede prosperar a la luz del art. 197.5 CP, en el que se prevé un tipo agravado para los supuestos de abuso informático sobre datos personales pertenecientes al «núcleo duro de la privacidad» (SAP de Huelva, de 16 de junio de 2006). Aunque el precepto tampoco es una norma penal en blanco que haya de integrarse con norma administrativa alguna, por ello cabe mantener una interpretación similar a la mantenida para el término «secreto» del apartado anterior, es decir, como todo conocimiento restringido, no público, que afecte a cualquier extremo de la vida personal o de su familia que quiere mantenerse oculto.

Es requisito sine qua non que los datos estén incorporados a ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier tipo de archivo o registro público o privado (de tipo convencional y no automatizado). Si no existe dicha incorporación, como es el caso de recogida ilícita de datos personales con fines informáticos o creación clandestina de ficheros o bancos de datos personales con fines de automatización, nos encontramos fuera del ámbito del Derecho Penal, rigiendo en cualquier caso la sanción administrativa (arts. 42.2 c y d y 44.3 a b y c LOPDCP).

ATENCIÓN. El CP ha optado por reducir al ámbito de los ilícitos penales a las conductas de apoderamiento, utilización, modificación, acceso ilegítimo, alteración y cesión de los datos registrados, es decir, que la protección penal no abarca todo el proceso del tratamiento informatizado de los datos, se limita a la tutela de los datos ya registrados, excluyendo las fases de creación de los ficheros automatizados y de recogida de los datos personales, que se reconducen al ámbito de la responsabilidad administrativa, tal y como pone de manifiesto la Ley de Protección de Datos de Carácter Personal» (SAP Guipúzcoa -1.ª- 31/2000, de 21-3).

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

El intrusismo informático o Hacking, por ejemplo, no es una conducta constitutiva de delito. La SJP Badajoz, núm. 42/2006, de 15 febrero así lo expresa: «El acceso a datos informáticos de un tercero por mera curiosidad (intrusismo informático o Hacking), no es una actuación constitutiva de delito (SAP Tarragona de 23 de julio de 2001). Si bien es cierto que el acusado ha tenido acceso a los correos personales de los empleados de Wanadoo y a los archivos de los usuarios del juego; también lo es que no ha quedado acreditado que la acción se desarrollara "en perjuicio de tercero"; ni, por ende, que la intención del acusado fuera la de atentar contra la intimidad de los empleados de Wanadoo, o de los usuarios del videojuego (...). Por contra, más bien parece que la intención perseguida por el agente o intruso no ha sido otra que la de acceder sin más a las entrañas del sistema, franqueando cuantas barreras le fueron instaladas, conducta ésta típica del "hacker"».

El AAP de Barcelona, Sec. 6.ª, núm. 523/2008, de 8-10, dice: «En el número 2, final del art. 197, sanciona el Código a quien sin estar autorizado, acceda por cualquier medio a los datos personales y a quien los altere o utilice en perjuicio del titular o de un tercero. La acción típica se produce sobre datos personales ya registrados en el fichero, debe tener por objeto datos reservados de carácter personal o familiar de otro, siendo al parecer de muchos autores la expresión "reservados" notablemente redundante puesto que ni la LORTAD en su día, ni el art. 3.a) de la actual LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal atribuyen tal carácter a todos los datos personales incorporados a un fichero automatizado (sin que ello desmerezca su protección en tanto que personales), y sin que tampoco pueda interpretarse que la remisión a la reserva se refiera al denominado núcleo duro de la privacy (datos sobre la salud, ideología, creencias...), ya que el apartado 5 del mismo artículo prevé un tipo agravado para los supuestos de abuso informático sobre datos personales pertenecientes a dicho núcleo duro de la privacidad».

Señala que «para integrar las nociones de datos de carácter personal y fichero o soporte informático, electrónico o telemático habrá que acudir a los arts. 2: "La presente LO será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado" y 3 b) de la LO 15/1999: "A los efectos de la presente LO se entenderá por: b) Fichero:

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Incluye, por último, el tipo, al menos en su inciso primero, un elemento subjetivo del injusto, como es que la conducta típica se realice "en perjuicio de tercero". Inclusión en la que algunas opiniones han querido ver la intención del legislador de incriminar las conductas de dolo directo, excluyendo las de dolo eventual, pero que estimamos, en todo caso, se extiende a (en lo que al inciso final afecta) sólo a la alteración o utilización de datos, mas no al acceso a los mismos o a los ficheros que se contienen».

El ATSJ de Castilla-La Mancha, Sec. 1.ª, 30-10-2008, dice que «las características del art. 197.2 del CP aparecen expuestas de manera explícita en la STS de 18 de febrero de 1999 según la cual el art. 197.2 describe el tipo básico de los recientemente llamados por la doctrina delitos contra la libertad informática o habeas data, esto es, de los delitos que atentan contra la intimidad de las personas desvelando o, más ampliamente, haciendo un uso ilegítimo de los datos personales insertos en un programa informático. A primera vista, parecen recogidos en cada uno de los dos incisos de dicha norma dos tipos delictivos distintos, pero hay que reconocer que no resulta fácil precisar cuáles son sus elementos diferenciadores. La acción es, en ambos casos, prácticamente la misma: apoderarse, utilizar o modificar en el primer inciso y acceder, utilizar o modificar en el segundo, aunque puede apreciarse una diferencia de matiz en la intensidad de la acción entre apoderarse y acceder «por cualquier medio». El objeto de la acción delictiva es exactamente el mismo: «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». Alguna diferencia parece marcarse entre el sujeto pasivo del delito del primer inciso -"en perjuicio de tercero"- y el del segundo -"en perjuicio del titular de los datos o de un tercero"- pero es más que probable que no se le deba dar demasiada importancia a esta diversidad puesto que, lógicamente, el que con mayor frecuencia resulta perjudicado por la infracción es el titular de los datos aunque inexplicablemente se le haya silenciado en la definición legal del primer inciso. Por lo demás, tanto el elemento negativo del tipo -"sin estar autorizado"- como el resultado de la acción "en perjuicio de" aparecen expresados de la

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

misma manera en los dos tipos. Pese a esta sustancial identidad, la diferencia de matiz que existe, según hemos señalado, entre apoderarse y acceder por cualquier medio -la primera expresión evoca la acción de sustraer, en tanto la segunda conviene a toda forma ilícita, puesto que no se está autorizado, de llegar a conocer los datos reservados- autoriza a hablar de dos tipos delictivos, muy cercanos morfológicamente.

El bien jurídico protegido es la intimidad individual, aunque cabe matizar que parece razonable que no todos los datos reservados de carácter personal o familiar puedan ser objeto del delito contra la libertad informática, puesto que precisamente porque el delito se consuma tan pronto el sujeto activo "accede" a los datos, esto es, tan pronto los conoce y tiene a su disposición, es por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que puede afectar, como hemos visto, al titular de los datos o a un tercero, o es fácil, precisar a priori y en abstracto, cuando el desvelamiento de un dato personal o familiar produce ese perjuicio. Baste ahora con decir que lo produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera "sensible" por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no trasciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar...».

Las conductas consisten, como se ha dicho, en apoderarse, utilizar o modificar, «en perjuicio de tercero», los datos reservados. En consecuencia, se castiga toda acción de tomar, coger, o poner bajo su poder o control, copiar. En este sentido, debe reproducirse todo lo dicho en el apartado anterior en lo referente a su naturaleza de «delito mutilado en dos actos», así como en lo relativo a la consumación. La modalidad de «utilizar» debe entenderse como toda acción de aprovechamiento de dichos datos reservados. Por último, «modificar» significa cualquier comportamiento que cambie, altere o transforme los datos reservados. Pero las tres conductas típicas han de ejecutarse «en perjuicio de tercero». Esta exigencia constituye un elemento subjetivo del injusto, si bien esta afirmación no es pacífica y hay quien sostiene que este perjuicio debe entenderse objetivamente, sosteniéndose que este perjuicio es el quebrantamiento de la reserva o el descubrimiento del secreto. Sin embargo, el

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

perjuicio al que se alude es diferente del mero quebrantamiento de la reserva, inherente semánticamente a los verbos típicos.

En cuanto a este elemento, la SAP de Córdoba, Sec. 2.ª, núm. 297/2008, de 28-11, reitera que «el delito de descubrimiento de secretos es un delito tendencial, que se consuma tan pronto el sujeto activo accede a los datos, esto es, tan pronto los conoce y tiene a su disposición, pues solo con eso se quebranta la reserva que los cubre, por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de esa reserva integre el tipo, perjuicio que puede afectar al titular de los datos o a un tercero. Por lo tanto, ese elemento subjetivo que exige esta conducta debe existir en el momento del acceso a los correos electrónicos; precisamente el momento en el que el juez a quo expresa sus dudas sobre si estaba actuando con ese propósito o fue solo un encuentro casual. Para que la conducta sea típica debe realizarse con la finalidad de descubrir los secretos, circunstancia que precisamente no considera acreditada la sentencia apelada. La cuestión que aborda es el uso indebido del ordenador por parte de las perjudicadas que era de titularidad pública, tiene relevancia, no solo en la valoración probatoria de la concurrencia del elemento subjetivo del delito, sino que puede afectar a la propia tipicidad del hecho. La STS de 30-4-2007, en un caso similar en que el ordenador utilizado era de titularidad pública y adscrito a un organismo municipal, viene a resaltar que el descubrimiento de conversaciones privadas a través de esta herramienta, puede considerarse atípico. Argumenta esta sentencia que no es posible entender que en el ordenador en el que se almacenaban físicamente los datos y al que acceden los acusados fuera el lugar idóneo para el archivo o almacenamiento de datos relativos a la intimidad personal de los empleados porque se trataba de un instrumento de titularidad pública (en este caso, de titularidad de la empresa), lo que implica que su utilización solo podría estar orientada al cumplimiento de las funciones públicas (en este caso, las funciones comerciales y laborales asignadas a los empleados), para cuya mejor satisfacción se dota al organismo, y al tiempo a quienes lo sirven, de los necesarios medios técnicos. Haciendo referencia a la sentencia del mismo Tribunal núm. 666/06, mantiene que las comunicaciones del género de las interferidas no están destinadas institucionalmente a ser el regular cauce de contenidos de carácter íntimo. En este sentido, también le parece aplicable al caso, aunque se refiera a la jurisdicción laboral, la STSJ de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Cataluña de 11-3-2004, que niega que exista violación de los derechos fundamentales a la dignidad, al honor, a la intimidad personal y familiar a la propia imagen y al secreto de las comunicaciones, cuando se adoptan medidas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales en el sistema informático que maneja, en cuanto a que es un instrumento de trabajo que la empresa proporciona al trabajador para desarrollar sus cometidos laborales. En conclusión, se acoge la resolución de instancia en cuanto a la existencia de dudas sobre la concurrencia del necesario elemento subjetivo en la figura delictiva que se analiza, tanto para uno como otro inculpado, pero además entiende este Tribunal que ni siquiera el elemento objetivo podría ser predicable en su integridad, al incurrir en exceso las empleadas utilizando para fines privados una herramienta de trabajo proporcionada por la empresa. Ello lleva a la desestimación del recurso y a la confirmación de la sentencia que es objeto del mismo».

Como expone la STS de 18 de febrero de 1999, estamos ante un delito doloso, pero no ante un delito de tendencia.: «El Tribunal de Instancia ha considerado que la expresión "en perjuicio de" supone la exigencia de un ánimo o especial intención de perjudicar al titular de los datos o a un tercero y en tal exégesis descansa fundamentalmente su pronunciamiento absolutorio. Esta Sala no puede compartir esta lectura del precepto aunque no deja de reconocer que la preposición "en" ha sido interpretada frecuentemente en dicho sentido. En el tipo que analizamos, sin embargo, situado inmediatamente después del otro -el del art. 197.1- en que el ánimo específico aparece indicado con la inequívoca expresión "para", el perjuicio producido por la acción tiene que estar naturalmente abarcado por el dolo pero no tiene que ser el único ni el prioritario móvil de la acción. A esta conclusión debe conducir no solo el argumento sistemático a que acabamos de aludir, sino la propia relevancia constitucional del bien jurídico lesionado por el delito, cuya protección penal no puede estar condicionada, so pena de verse convertida prácticamente en ilusoria, por la improbable hipótesis de que se acredite, en quien atente contra él, el deliberado y especial propósito de lesionarlo. Estamos, pues, ante un delito doloso pero no ante un delito de tendencia».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Por tanto, cabe sostener que de producirse un perjuicio económico, pudiera apreciarse un concurso con estafa o apropiación indebida por ejemplo. La conducta se consuma sin necesidad de que éste se produzca. De suerte que si el perjuicio se materializa, existiría normalmente un concurso medial. Recuérdese que en este precepto se tutela exclusivamente la intimidad, y no contempla la lesión de otros bienes jurídicos. «En perjuicio» constituye un elemento subjetivo del injusto. Por «tercero» ha de entenderse aquí toda persona distinta al sujeto activo.

Pero además se requiere que el sujeto activo obre «sin estar autorizado»; cláusula que puede conceptuarse como un elemento normativo del tipo, sin cuya presencia se procedería a declarar la atipicidad de la conducta, o como una especial causa de justificación.

In fine se sanciona al que 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». Las conductas aquí expresadas «acceda», «altere» o «utilice» se proyectan no sobre los datos reservados -comportamientos ya tipificados en la primera parte de este mismo precepto- sino sobre los «ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado». En consecuencia, aquí se castiga a los que «acceden», esto es, a los que entran, o se introducen, y por tanto visualizan o escuchan, la información en ellos almacenada.

La SAP de Barcelona, Sec. 6.ª, núm. 72/2008, de 18-1, incide únicamente en la conducta relativa al acceso a los datos reservados de carácter personal, que se hallen automatizados de forma electrónica o que obren en cualquier otro tipo de archivo o registro público o privado, es decir, el inciso final del epígrafe, puesto que la posible captura de datos, consistente en el apoderamiento del mensaje de correo electrónico quedaría comprendida en el número primero del mismo artículo. Señala que «el moderno sistema de comunicación y transmisión de datos e información que conocemos como correo electrónico, hace referencia a una realidad compleja compuesta de al menos, y a los efectos que ahora nos importan, tres elementos diferentes. Primero, cada uno de los concretos mensajes que a través de este procedimiento informático circulan; segundo, los ficheros que incorporan las aplicaciones, donde se guarda el correo entrante, el

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

enviado, incluso aquellos mensajes que están preparados como borrador o ya han sido eliminados, y por último, la libreta de direcciones y el historial de tráfico registrado. Parecidamente a lo que ocurre con otros sistemas actuales como los teléfonos celulares portátiles, el correo electrónico, como sistema informático, contiene una ingente cantidad de datos de carácter personal, en diversa presentación y de diferentes características, que normalmente atañen a la esfera privada de las personas, y que encuentran variadas vías de protección en el art. 197 del Código Penal que hemos venido comentando. Protección que demanda un medio de comunicación y almacenaje de datos muy variados, muy vulnerables a la intromisión ajena, por diferentes medios muy eficaces, insidiosos y difícilmente detectables. Y esta tutela penal se puede extender, en principio a todo tipo de fichero, registro, soporte y mensaje, con independencia de que se contengan o circulen a través de equipos informáticos o aplicaciones de titularidad pública o privada, puesto que es de todo punto posible, y aun previsible, que al igual que desde un teléfono oficial se pueda mantener una conversación privada, desde un equipo informático público se pueda recibir o enviar un e-mail de contenido particular.

Efectivamente, la conducta consiste en actos de apoderamiento de un correo electrónico y de un acceso un fichero o soporte informático como es el listado de correo electrónico de una persona, la comprobación del tráfico por ésta sostenido y la selección de unos concretos mensajes y conversaciones por ésta mantenidos. No obstante, es preciso distinguir entre las dos acciones nucleares; apoderamiento del correo y acceso a la base de datos de correo electrónico, resultando de todo punto intrascendente respecto de ambas si para acceder a esta aplicación era o no necesaria una clave de entrada y cómo consiguieran la misma el acusado.

Resulta subsumible en el art. 197.2 del CP la conducta de quien sin estar autorizado, acceda por cualquier medio a 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. Y como también se analizó, el sistema de correo electrónico participa de la naturaleza de fichero o soporte de datos en tanto que conserva además de los mensajes concretos, listados de mensajes enviados o recibidos, libreta de direcciones, etc. El tipo presenta imperfecciones de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

redacción que provocan cierta oscuridad interpretativa, pudiéndonos plantear si lo que se penaliza es el mero acceso a los archivos, soportes o registros que contengan datos personales o sólo el acceso a estos últimos. En la práctica, más aún en este supuesto, será muy difícil deslindar ambas acciones típicas puesto que al acceder al archivo ya se está tomando conocimiento de un contenido privado y reservado (la relación de mensajes, las listas de correo, etc.) que luego se profundiza si además se van abriendo los diferentes mensajes concretos.

Ello nos sitúa, como marco de partida, ante la consideración apriorística de que la entrada inconsentida en la aplicación de correo electrónico de otra persona y el recorrido por las diferentes bases de datos que el sistema contiene, incluso sin abrir ningún mensaje, puede ser penalmente típica ya que con ella se está produciendo una intromisión en la intimidad y susceptible de facilitar una toma de conocimiento de datos muy sensibles y reservados. Además, pudiera sostenerse que el tipo del art. 197.2 in fine del Código Penal se presenta desprovisto de la necesaria concurrencia de otros elementos subjetivos del injusto adicionales como son el ánimo de descubrir los secretos o vulnerar la intimidad de otro, del número 1 del mismo artículo, o perjuicio de tercero que requiere el inciso primero del número 2, tal vez porque van implícitos en la propia acción.

Por lo tanto, el acusado al acceder a estos archivos asumió como mínimo con dolo eventual, o por mejor decir de indiferencia, recogido por el Tribunal Supremo en numerosas resoluciones (SSTS 02.12.04, 28.09.05 o 18.11.05, entre otras), que con su proceder podría vulnerar la legalidad penal, en tanto que el sistema de correo electrónico es un archivo, soporte o fichero que contiene datos, bases de datos e información que pueden ser reservados de carácter personal o familiar de otro.

Como consecuencia de lo anterior, podemos asentar que en el acusado al abrir el sistema de correo electrónico, concurría el elemento subjetivo de volición requerido, en su forma de dolo eventual, siendo suficiente situarse en una posición de indiferencia respecto del contenido posible de la aplicación del correo electrónico, y sin representación, ni posibilidad de acometer ningún acto de averiguación para poder prever el alcance de su conducta. Pero es que

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

además el acusado no accedió tan sólo al sistema de correo de la víctima, sino también procedió a remitir al marido de ésta un correo en el que le notificaba que ésta había mantenido conversaciones e intercambiado correos electrónicos con otra persona, siendo indiferente contrariamente a lo alegado por el recurrente que el contenido de lo revelado por el acusado fuera o no cierto, pues la intromisión en la intimidad de la denunciante y la revelación de ésta no ofrece duda alguna. El motivo debe, por tanto, ser desestimado».

La difusión vía whatsapp de fotografías que pertenecen al reducto de lo que, una persona media de nuestra cultura, pretende que no trascienda fuera de la esfera en que se desenvuelve su privacidad, más allá de la exclusiva tenencia por la persona a quien se le remiten inicialmente las mismas, es encuadrable en un delito de revelación de secretos, si se exhiben a terceros, sin contar con la anuencia del directamente interesado. SAP Ourense 131/2014, de 26 de marzo.

2.1.3. El acceso sin autorización a datos o programas informáticos

La reforma operada por LO 5/10 de 22 de junio, transpone la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, de forma que dentro del descubrimiento y revelación de secretos, y en el marco de los delitos informáticos, introduce un nuevo apartado 3 en el art. 197 donde se sanciona el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.

Dice el art. 197.3:

«El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el art. 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del art. 33».

Las conductas consisten en acceder sin autorización, o en mantenerse en contra de la voluntad de quien tenga legítimo derecho a excluirlo, y ha de realizarse vulnerando las medidas de seguridad establecidas. Si el responsable es una persona jurídica, la penalidad se establece en el párrafo segundo.

2.2. Tipos agravados

Por LO 5/10, de 22 de junio, los apartados 3, 4, 5 y 6 pasan a ser 4, 5, 6 y 7.

2.2.1. Difusión, revelación o cesión de los datos reservados a terceros

Establece el art. 197.4:

«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».

Se contienen dos modalidades, una en el apartado primero y la otra en el segundo:

- El art. 197.4.1.º es aplicable a todos los tipos básicos anteriores, y tiene su fundamento en que dichas acciones suponen incrementar la vulneración de la intimidad del sujeto pasivo. Presuponen la comisión de alguna de las modalidades básicas y comprende tres conductas: difusión, revelación y cesión, que en definitiva suponen la comunicación a una o más personas. La significación gramatical de los verbos utilizados parecen abarcar desde la transmisión por medio de comunicación, la comunicación a un número limitado de personas, o a un tercero para que use dicha información, de manera que el

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

legislador equipara difusión, revelación y cesión a terceros, aun cuando la primera suponga una mayor publicidad.

ATENCIÓN. Por tanto, en el párrafo primero del art. 197.4 CP se contiene una agravación de la pena, cuando además de realizarse la conducta ya descritas de apoderamiento de un secreto o interceptación de comunicaciones, se divulga a terceros. De esta forma la intimidad se ve doblemente atacada: primero se descubre ilícitamente un secreto, y después se transmite o comunica a otras personas. El sujeto activo de este delito ha de coincidir con el mismo que descubre los secretos de otro.

- En relación art. 197.4.2.º, se contiene un tipo atenuado en cuanto que el autor no ha cometido ni participado previamente en el delito de descubrir la intimidad, no ha sido autor ni cómplice. Se exige que el sujeto activo conozca la procedencia ilícita, que no necesariamente delictiva, de la información que luego va a difundir. La SAP de Murcia, Sec. 5.ª, núm. 104/2007, de 13-11, señala cuáles son los elementos necesarios para que pueda estimarse que concurre la conducta del art. 197.4.2.º del CP, estableciendo que del juego conjunto del art. 197.4.2.º en relación con el art. 197.1, se desprende que son elementos integrantes del tipo, de necesaria observancia, los siguientes:

a) acto previo de apoderamiento por un tercero de papeles o cartas del sujeto pasivo del delito (art. 197.1);

b) que dicho apoderamiento se hubiese realizado con la intención de descubrir secreto o vulnerar la intimidad del propio sujeto pasivo (art. 197.1);

c) difusión o revelación de tales datos a terceros (art. 197.4.1.º);

d) que el sujeto activo no haya participado en su descubrimiento (art. 197.4.2.º), y

e) que el sujeto activo tenga conocimiento del origen ilícito de los datos que difunde o revela (art. 197.4.2.º).

2.2.2. Por el especial deber del sujeto activo

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

El art. 197.5 CP establece:

«Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior».

Se establece una agravación para las personas encargadas de los soportes, ficheros o archivos, y otra agravación más si además difunden, ceden o revelan los datos reservados.

2.2.3. Datos sensibles o que afecten a menores o incapaces

Dice el art. 197.6:

«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 un incapaz, se impondrán las penas previstas en su mitad superior».

El apartado 6 del precepto incluye otro supuesto agravado cuyo fundamento tiene por objeto la especial protección de lo que se denomina el núcleo duro del derecho a la intimidad (núcleo duro de la privacy), además de los casos en que la víctima fuere un menor de edad o un incapaz, por su vulnerabilidad, que exaspera la pena que resulte de la aplicación de los preceptos anteriores, imponiéndola en su mitad superior.

Se refieren a la esfera más sensible de la intimidad como «la ideología, religión, creencias, salud, origen racial o vida sexual». El art. 7 de la LOPDCP se refiere a ellos como los datos especialmente protegidos.

ATENCIÓN. El art. 197.6 CP es un tipo agravado aplicable tanto al tipo básico del art. 197.1 y 2, como a la nueva modalidad del apartado 3, y al agravado del art. 197.4 CP; y refuerza la protección de un secreto de naturaleza especialmente sensible por venir referido a uno de los aspectos que constituyen el núcleo duro de la privacidad.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

La STS 302/2008, de 27-5, dice que «la referencia del art. 197.6.º a los datos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual no abarca la investigación ilícita de infidelidades o relaciones sexuales de cualquier índole, sino solamente aquellas que se refieran a la orientación sexual de la víctima poniendo de relieve tendencias que en el momento de la redacción del CP pudieran considerarse por algunos sectores al margen de la norma general, como las relaciones homosexuales, circunstancia que está superada por la legislación que homologa los vínculos entre sexos, sea cual sea el género de la persona. La redacción del precepto está en íntima conexión con el art. 16 de la CE, estableciéndose la agravante en función de la discriminación social, lo que es radicalmente distinto de la posible inquietud, ansiedad o desasosiego que pueda producir en una persona el hecho de que se conozcan sus relaciones extramatrimoniales».

2.2.4. Ánimo de lucro

Dice el 197.7:

«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 5, la pena a imponer será la de prisión de cuatro a siete años».

Se distingue según afecte a datos sensibles o no (los del apartado 6.º), con ánimo de lucro, en todo caso, razón de ser de la agravación.

Dice la STS 302/2008 de 27-5: «Por lo que se refiere al ánimo de lucro, éste no tiene la misma configuración que en los delitos patrimoniales, en que el lucro se define como la intención del sujeto de obtener una ventaja patrimonial mediante la incorporación a su patrimonio de una cosa ajena, por cuanto el lucro recae directamente sobre la cosa objeto de apoderamiento; ahora bien el concepto de ánimo de lucro se inserta en una concepción del lucro como beneficio patrimonial injusto, entendido como antijuridicidad material, y por tanto por la obtención de una ventaja patrimonial no amparada por el derecho por carecer de causa. Asimismo el ánimo de lucro o finalidad lucrativa para el caso del artículo 197.6 (ahora 7), ha de derivarse directamente de la utilización por el agente de los datos obtenidos ilícitamente. Así, en el supuesto de la STS

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

694/2003 en que la obtención de datos por un investigador lo es a cambio de remuneraciones económicas; el supuesto de la STS 1532/2000 en que se obtienen datos de personas minusválidas para usarlos para contactos sexuales, ofertas fraudulentas de trabajo y otras, o el de la STS 1219/2004, o en que la grabación de imágenes sexuales tiene, entre otras finalidades, la de ofrecer su venta a terceros».

En el caso de la STS 302/08, se trata del apoderamiento de una serie de documentación privada, y cuya utilización ha consistido en su presentación en juicio como prueba de la capacidad económica del marido; no hay un ánimo de lucro directo derivado del apoderamiento de tales documentos pues la ventaja patrimonial que pretende obtenerse no se deriva de la utilización ilícita de los mismos por parte de la acusada sino de la valoración del tribunal que emitió la sentencia, en el ámbito de un proceso contradictorio, y por tanto la consecución del lucro se encuentra fuera del dominio funcional del hecho por parte de la acusada, por más que la no aportación de dicha prueba documental, como es lógico, hubiera vedado su valoración por el tribunal de instancia.

2.2.5. Organización o grupos criminales

La LO 5/10 de 22 de junio introduce un nuevo apartado 8 en el art. 197 que dice:

«Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado».

2.3. Tipo especial impropio

Cuando se comete por autoridad o funcionario público, se regula en el art. 198 CP:

«La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Se trata de un delito especial impropio que solo puede ser cometido por la autoridad o funcionario público que ha de actuar fuera de los casos permitidos por la ley, sin mediar causa por delito, y prevaleciéndose de su cargo. Deben distinguirse de los delitos regulados en los arts. 534 a 536 CP, dentro de los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad, en que de igual forma que en las detenciones ilegales, actúan mediando causa por delito. Y esa es la diferencia, en el tipo analizado, el funcionario actúa como un particular, por tanto fuera completamente de sus competencias, mientras en los delitos contra las garantías constitucionales lo hacen en el ejercicio de las mismas pero se extralimitan gravemente.

2.4. Secreto profesional

Cuando el conocimiento del secreto lo es por razón del oficio o por las relaciones laborales, establece el art. 199 CP:

«1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años».

ATENCIÓN. El art. 199 CP se estructura en dos apartados: en el primero se castiga a los que revelen secretos ajenos que conozcan por razón de su oficio o sus relaciones laborales, y el segundo que regula el secreto profesional.

El bien jurídico es el mismo en ambos supuestos, la intimidad de un tercero. Y la conducta también, pues consiste en «revelar» o «divulgar» secretos conocidos en el desempeño de un oficio o relación laboral, o en el ejercicio de una profesión. Sirven aquí cuantas observaciones se hicieron al comentar el tipo básico del art. 197. Las diferencias, que se traducen en una mayor pena para el segundo apartado, se sitúan en la distinta naturaleza de la actividad por cuanto los profesionales incumplen el deber de secreto profesional.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Cabe considerar como confidentes necesarios a los Abogados y Procuradores (están obligados a guardar secretos sobre los hechos revelados por sus clientes, EGA, RD 658/2001, y EGP RD 1281/2004), médicos (art. 10.3 de la Ley 14/1986 General de Sanidad), detectives (RD 2364/1999 y Ley 23/1992 de Seguridad Privada), profesionales de banca (RDL 1298/1986 de 28 de junio, de entidades de crédito), informáticos, sacerdotes, periodistas.

2.5. Personas jurídicas

Cuando los datos reservados afecten a la intimidad de las personas jurídicas el art. 200 CP establece una cláusula de extensión, disponiendo que:

«Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código».

La cuestión que se plantea es si las personas jurídicas pueden ser titulares de derechos fundamentales, por cuanto el TC los declara personalísimos y ligados al individuo, de ahí que se sostenga que no son titulares del derecho a la intimidad, y su extensión a los miembros de las mismas o la intimidad de terceros. Algún autor sostiene que no hay inconveniente en sostener la intimidad de las personas jurídicas en aspectos tales como criterios de administración, jerarquía, control, previsiones, etc.

2.6. Requisito de perseguibilidad

Se establece, con carácter general, la necesidad de denuncia del agraviado para proceder por estos delitos y la relevancia del perdón del ofendido, en el art. 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, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el art. 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 5.º del apartado 1 del art. 130».

Excepcionalmente, cuando la persona agraviada -esto es el titular del bien jurídico lesionado- es menor de edad, incapaz o «persona desvalida», también podrá denunciar el Ministerio Fiscal. Se configura pues como una facultad y no como una obligación de éste, que tendrá que ponderar el derecho a la intimidad de la víctima con interés general de perseguir toda infracción.

No se exige denuncia previa, cuando el sujeto activo sea autoridad o funcionario público, afecte a los intereses generales o a una pluralidad de personas, configurándose en estos casos como delitos públicos perseguibles de oficio.

La SAP de Barcelona, Sec. 2.ª, núm. 986/2007,de 5-12, dice que, «el apartado 1 del art. 201 del CP a quien otorga legitimación para interponer la denuncia es al «agraviado» o, en su caso, a su representante legal, que es tanto como decir el «ofendido» por el delito (art. 201 apartado 3 CP) o, en último término, el sujeto pasivo del delito; que no cabe identificar al titular de los datos con todas las demás personas en cuyo perjuicio podría realizarse la acción típica». Perjudicado es la persona que como consecuencia de un delito o falta sufre un daño y/o perjuicio (art. 109.2 CP), en tanto ofendido es el sujeto pasivo del delito, si bien éste puede ocasionar perjuicios igualmente a terceras personas (arts. 109, 110 y 761.1 LECrim.). En consecuencia, a los efectos de lo dispuesto en el art. 201.1 del CP, debe entenderse que sólo el titular de los datos de que se trate está legitimado para denunciar, sin perjuicio de que, si así lo hace, cualquier tercero que pudiera haber sufrido un efectivo perjuicio como consecuencia del delito pueda mostrarse parte en la causa a los efectos de defender sus derechos e intereses legítimos.

3. ALLANAMIENTO DE MORADA

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

3.1. Introducción y bien jurídico protegido

El CP de 1995 contempla delitos de nueva creación en este capítulo, concretamente los arts. 203 y 204, al contemplarse el allanamiento de domicilio de personas jurídicas y establecimientos abiertos al público, como novedad principal, junto al ya clásico delito de allanamiento de morada.

En orden al bien jurídico protegido no existía unanimidad. Por su ubicación sistemática en al texto del CP de 1973 se sostuvo que era la seguridad, el bien jurídico protegido. Más concretamente la seguridad personal en relación a los espacios cerrados que las personas individuales, y las colectivas acotan para llevar a cabo sus actividades. También se dijo que era la libertad, en el sentido de decisión de las personas. Con la nueva rúbrica del Título X, parece claro que lo que se protege es la intimidad de las personas y así se reitera jurisprudencialmente.

El art. 18.2 CE reconoce como derecho fundamental la inviolabilidad del domicilio. Respecto del concepto de domicilio, la conocida STC de 17 de febrero de 1984 se refiere a espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima, siendo por tanto de mayor amplitud que el concepto jurídico privado o administrativo. Pero incluso en la vertiente penal cabe afirmar que es más amplio el concepto, dadas las referencias a despacho profesional o establecimientos mercantiles abiertos al público, donde parece que la razón de la norma es más bien el buen funcionamiento de tales establecimientos que la intimidad.

Por tanto, con carácter general, cabe sostener que en el delito de allanamiento de morada se protege la inviolabilidad de domicilio como parte de la intimidad, y que el concepto de domicilio o morada en Derecho Penal comprende tanto la residencia habitual como cualquier otra localización o establecimiento siempre que se more en él y con las salvedades referidas.

La STS de 17 de noviembre de 2000 dice que el delito de allanamiento de morada es una infracción contra la inviolabilidad del domicilio, que tutela tal derecho fundamental de la persona reconocido constitucionalmente, debiéndose entender por morada «el recinto, generalmente cerrado y techado,

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

en el que el sujeto pasivo y sus parientes próximos, habitan, desarrollan su vida íntima y familiar, comprendiéndose dentro de dicho recinto, dotado de especial protección, no sólo las estancias destinadas a la convivencia en intimidad, sino cuantos anejos, aledaños o dependencias constituyan el entorno de la vida privada de los moradores, indispensable para el desenvolvimiento de dicha intimidad familiar», señalando la STS de 5 de diciembre de 2005 que «el valor constitucional de la intimidad personal y familiar que explica el mayor rigor punitivo con que se protege en el CP vigente la inviolabilidad del domicilio de las personas físicas, sugiere que debe ser el derecho de éstas a la intimidad la clave con que debe ser interpretado el art. 202 CP, de suerte que el elemento objetivo del tipo descrito en esta norma debe entenderse «puesto» siempre que la privacidad resulte lesionada o gravemente amenazada, lo que inevitablemente ocurrirá cuando alguien entre en la vivienda de una persona, cualquiera que sea el móvil que a ello le induzca, sin su consentimiento expreso o tácito».

3.2. Tipo básico

Se sanciona en el art. 202.1 CP que dice:

«El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años».

3.2.1. Sujetos

Sujeto activo, solo puede ser un particular, que lo diferencia del cometido por autoridad o funcionario público de los arts. 204 o 534 CP cuando medie causa por delito y no se respeten las garantías constitucionales. El delito puede ser cometido por un cónyuge separado respecto de la morada del otro incluso siendo propietario si el otro tiene atribuido el uso y disfrute del inmueble, al igual que el arrendador respecto del arrendatario.

En este sentido, la SAP de Madrid (Sección 27.ª) núm. 886/2008 de 31 julio, señala que «aunque es cierto que el art. 202 del CP, con el fin de otorgar protección a la intimidad del hogar con fundamento en el derecho a la inviolabilidad del domicilio, tipifica como delito de allanamiento de morada la

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

acción de estar en morada ajena, tanto por irrupción como por permanencia, en condiciones de antijuridicidad, o sea contra la voluntad, expresa o tácitamente manifestada, del sujeto pasivo, representado por el morador que es quien tiene derecho a impedir la entrada o permanencia, y que, según establecen reiteradas resoluciones jurisprudenciales, el delito de allanamiento de morada puede ser cometido por el cónyuge que permanece o entra en la vivienda común contra la voluntad del morador, cuando éste es el otro cónyuge, ello lógicamente ha de estar, en todo caso, supeditado o a la existencia de sentencia o medida provisional de separación con asignación judicial de domicilio a uno de los cónyuges». Añade que en este supuesto «el resultado de la prueba evidencia que en efecto existía una separación de hecho, y que el recurrente, pese a no haberse divorciado aún de la denunciante, ya no vivía con ella en el domicilio, no teniendo, siquiera, la llave de la puerta, dado que irrumpe en ella, al oponerse la moradora a que entrara, saltando la valla exterior y rompiendo los pestillos de la puerta corredera de acceso al interior de la vivienda. Ello no obstante, no podemos entender que tal situación de hecho pueda ser equiparada a la decisión de adjudicación del uso exclusivo de la vivienda a uno de los cónyuges, con carácter provisional o definitivo, por un juez, a efectos de poder determinar la concurrencia del requisito típico referido a la morada ajena, por no haber sido atribuida la permanencia en el domicilio conyugal a uno de los cónyuges, lo que impide que la actuación del acusado pueda configurar el delito de allanamiento de morada que tipifica el art. 202 del CP, al faltar el requisito de la irrupción en morada ajena, ya que la misma en el momento de los hechos no merecía la consideración legal de tal, siendo por ello procedente a la revocación parcial de la sentencia dictada en el sentido de acordar su absolución respecto del delito de allanamiento de morada por el que había sido condenado, y manteniendo la condena por la falta de lesiones».

Sujeto pasivo es el morador, titular del bien jurídico protegido y que tiene el derecho de exclusión, lo que plantea problemas en caso de cotitularidad, si uno prohíbe y otro no, o en caso de convivencia familiar sobre admisión o exclusión de determinadas personas, sosteniéndose diversas posturas doctrinales entre las que destaca la de la primacía del veto sobre el consentimiento, y más dudosamente, la primacía del cabeza de familia sobre el resto. En cuanto a los empleados domésticos suele negarse el derecho de admisión. Por su parte, el domicilio del Rey y miembros de la Corona se protege en el art. 490 CP.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

3.2.2. Conducta típica

Se regulan dos modalidades delictivas alternativas: entrar o mantenerse en contra, y se precisa la existencia de tres elementos:

A) Elemento objetivo. La morada. No se define en el CP la morada, ni el concepto penal, como se adelantó, es asimilable con el domicilio civil, fiscal, administrativo o procesal, siendo incluso más amplio que el que ofrece el TC. Siguiendo a Suárez Montes puede considerarse como morada: «aquel espacio cerrado o en parte abierto, separado del mundo exterior, en condiciones tales que hagan patente la voluntad de los moradores de excluir de él a terceras personas, mueble e inmueble, destinado al desarrollo de actividades propias de la vida privada, y cuyo uso debe ser actual y legítimo».

Que el espacio este cerrado o en parte abierto, admite la posibilidad de allanamiento, en los casos en que la puerta este abierta o entornada. Que sea mueble o inmueble admite el concepto referido a una cueva donde se vive, el camarote de un barco, una tienda de campaña, una autocaravana o un remolque. Y que esté destinada a actividades propias de la vida privada, excluye un trastero, un zulo, un piso abandonado y deshabitado. La ocupación de viviendas deshabitadas no constituye este delito, pudiendo serlo de usurpación del art. 245 CP.

La SAP de Alicante (Sección 2.ª) núm. 196/2008 de 9 abril, no aprecia que los hechos sean constitutivos de un delito de allanamiento de morada del art. 202 CP, señala que para que el delito se cometa debe vulnerarse un inmueble, que se constituya en un espacio de intimidad personal o familiar, en los términos del art. 18.2 de la CE y en el caso enjuiciado, el inmueble violentado, es una caseta de campo sin luz eléctrica, que no se utiliza hace años por su propietario y que únicamente acude su propietario al lugar con una periodicidad semanal o quincenal, para realizar labores propias de una explotación agrícola.

Generalmente no se admite respecto de vehículos de los que se entiende no constituyen morada de una persona como reducto de su intimidad personal y familiar, siendo más discutible respecto de embarcaciones. Y en cuanto a las habitaciones de un hotel, una pensión o residencia cabe su asimilación. En

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

cuanto a las dependencias de casa habitada, la jurisprudencia defiende su inclusión en base al concepto de casa habitada del art. 20.4 CP.

B) Elemento activo de entrar o mantenerse y voluntad contraria del morador. La conducta alternativa ha de ser entrar o mantenerse en contra. Puede consistir en una u otra. Por tanto, una conducta activa de entrar en morada ajena por cualquier medio precisando la entrada física, o alternativamente, otra pasiva, de mantenerse, lo que presupone una previa aceptación por parte del morador que después cesa. El consentimiento del titular excluye la tipicidad de la conducta, de forma que la voluntad contraria del morador es requisito típico, puede ser expresa o tácita e incluso presunta. No basta la simple presunción de oposición, ha de ser clara.

La STS de 5 de diciembre de 2005 señala que «la conducta positiva de entrar o permanecer en morada ajena ha de realizarse contra la voluntad del morador o del que tiene derecho a excluir, voluntad que puede ser expresa, tácita y hasta presunta; no es necesario que sea expresa y directa, bastando que lógica y racionalmente pueda deducirse de las circunstancias del hecho de otros antecedentes, y que sólo se exigirá el dolo genérico de entrar o mantenerse en morada ajena contra la voluntad del morador, sin requerirse la presencia de ningún otro especial elemento subjetivo del injusto bastando con la conciencia de la ajeneidad de la morada y de la ilicitud de la acción».

C) Elemento subjetivo. Dolo. Generalmente se considera que es suficiente el conocimiento por parte del sujeto activo de la voluntad contraria del titular de la morada, no exigiéndose elemento subjetivo del injusto de violar la morada ajena aunque la jurisprudencia en ocasiones se ha referido a un dolo específico de violentar la morada ajena. Por tanto, es suficiente un dolo genérico consistente en entrar o permanecer contra la voluntad del morador. No es posible la comisión por imprudencia. La STS 1577/2005 de 21 diciembre, señala que el dolo exigible en este delito requiere la conciencia de la ajeneidad de la morada y de la ilicitud de la acción el acusado:

En el caso que aborda los hechos se refieren a que «tras introducirse el niño en la vivienda, entró en la misma, rebasando el quicio de la puerta que se encontraba abierta, sin darse cuenta ni querer entrar en vivienda ajena, de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

donde salió inmediatamente al darse cuenta de que había entrado en vivienda ajena».

La STS 1048/2000 de 14 junio recuerda que «el art. 202 del CP vigente ha venido a reforzar la protección penal de la inviolabilidad del domicilio de las personas físicas, elevando significativamente las penas que para el allanamiento de morada se establecían en el art. 490 del CP derogado. La agravación parece de todo punto lógica si se tiene en cuenta que la inviolabilidad del domicilio y la intimidad personal y familiar que mediante aquélla se trata de salvaguardar son valores y bienes jurídicos que el art. 18 de la CE ha elevado al máximo rango garantizándolos como derechos fundamentales. El valor constitucional de la intimidad personal y familiar que, explica el mayor rigor punitivo con que se protege en el CP vigente la inviolabilidad del domicilio de las personas físicas, sugiere que debe ser el derecho de éstas a la intimidad la clave con que debe ser interpretado el art. 202 CP, de suerte que el elemento objetivo del tipo descrito en esta norma debe entenderse "puesto" siempre que la privacidad resulte lesionada o gravemente amenazada, lo que inevitablemente ocurrirá cuando alguien entre en la vivienda de una persona, cualquiera que sea el móvil que a ello le induzca, sin su consentimiento expreso o tácito. E importa aclarar que el mero hecho de que la puerta de una vivienda esté abierta, como lo estaban las puertas de las casas invadidas por el acusado en los hechos enjuiciados, no puede ser interpretado, por sí solo, como un consentimiento tácito a la posible entrada de cualquier extraño, pues es llano que no es presumible el permiso cuando quien entra se propone, por ejemplo, llevar a cabo una sustracción u otra actividad ilícita. Para que el tipo subjetivo del allanamiento de morada de persona física se realice, es suficiente con que se "ponga" el tipo objetivo con conciencia de que se entra en un domicilio ajeno sin consentimiento de quienes pueden otorgarlo y sin motivo justificante que pueda subsanar la falta de autorización, pues dicha conciencia necesariamente comporta la de que se invade el espacio en que otras personas viven sin sujeción a los usos y convenciones sociales y ejerciendo su más íntima libertad».

3.3. Tipo agravado

Se contiene en el art. 202.2 CP:

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

«Si el hecho se ejecutare con violencia o intimidación la pena será de prisión de uno a cuatro años y multa de seis a doce meses».

La cuestión que suscita este precepto se contrae en la determinación de si la violencia o intimidación ha de recaer sobre las personas o se extiende también sobre las cosas. Interpretación extensiva que sostiene la jurisprudencia del TS que ha sido matizada en el sentido de que precisa que la vis in re sea medio o forma de ejecución del allanamiento. En este sentido, la STS 179/2007 de 7 marzo, establece que este subtipo agravado comprende aquellos supuestos en que la violencia o intimidación se hayan ejercitado para entrar o mantenerse en la morada ajena y comprende también los supuestos de vis in re, entendiendo la jurisprudencia equiparable la violencia o intimidación en las personas con la ejercitada in rebús siempre que la violencia material sobre las cosas sea el medio de ejecución de allanamiento, esto es, que se trate de fuerza material o real y no la prevista en los números 1 y 4 del art. 238.

3.4. Allanamiento de domicilio de personas jurídicas

Se regula en el art. 203 CP que establece un tipo básico y otro agravado en razón de la concurrencia o no de violencia o intimidación, al igual que en el precepto anterior. Señala que:

«1. Será castigado con las penas de prisión de seis meses a un año y multa de seis a diez meses el que entrare contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público fuera de las horas de apertura.

2. Será castigado con la pena de prisión de seis meses a tres años, el que con violencia o intimidación entrare o se mantuviere contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público».

El objeto del delito es el domicilio de «una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local». Dentro de las personas jurídicas públicas, se incluye al Estado, Municipio, CC.AA. y Entidades dependientes con personalidad jurídica propia. En cuanto a las

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

privadas, se refiere a Asociaciones, Fundaciones y Sociedades, cuyos Estatutos será preciso tener en cuenta a los efectos de la determinación del domicilio. Se incluyen, los despachos profesionales u oficinas, referidos a profesiones liberales y establecimientos mercantiles, con una amplitud que permite ubicar a lugares donde se ejerzan actividades mercantiles según dicha legislación. Y finalmente, locales abiertos al público, respecto de los que se planteó el problema de determinar si la referencia a fuera de las horas de apertura era autónoma o complementaria del resto de domicilios, como así ha sido interpretado. Local abierto al público se refiere a todo aquel donde se accede libremente por el público con independencia de las actividades a que se destinen, pudiendo ser recreativas, religiosas, culturales u otras.

ATENCIÓN. Respecto del tipo básico la conducta activa solo se refiere a la de naturaleza activa, de entrar. La otra conducta pasiva, la de mantenerse en los referidos domicilios contra la voluntad del titular, fuera de las horas de apertura se sanciona expresamente como falta en el art. 635 CP. De igual manera, entrar en esos domicilios dentro de las horas de apertura queda excluido del precepto como el ejercicio del derecho de admisión no convierte en típica la conducta de quien se niega a abandonar esos locales en horas de apertura.

Mayores problemas plantea esta figura en relación a la voluntad contraria del titular, dadas las particulares estructuras de los domicilios a los que se refiere el precepto, de manera que en cada caso habrá que acudir a la jerarquía establecida y determinar quién tiene facultad de consentir o excluir, incluso si existe delegación de tales facultades.

Respecto del tipo agravado, dos precisiones, se sanciona tanto la conducta de entrar como la de mantenerse, y no se refiere a horario de apertura sino tan solo a abierto al público, por lo que cabe incluir tanto a dentro como fuera de las horas de apertura.

3.5. Tipo especial

Sanciona el art. 204 CP:

«La autoridad o funcionario público que, fuera de los casos permitidos por la Ley y sin mediar causa legal por delito, cometiere cualquiera de los hechos

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

descritos en los dos artículos anteriores, será castigado con la pena prevista respectivamente en los mismos, en su mitad superior, e inhabilitación absoluta de seis a doce años».

Se trata de un delito especial impropio, por cuanto solo puede ser sujeto activo la autoridad o funcionario público. Al igual que en las detenciones ilegales (art. 164 CP) y en el descubrimiento y revelación de secretos (art. 198 CP), se exige que sea «fuera de los casos permitidos por la ley y sin mediar causa por delito», de manera que lo dicho en dichos preceptos vale aquí, recordando que en estos casos la autoridad o funcionario actúa como un particular, fuera de sus competencias, prevaliéndose de su condición.

En el art. 534 CP se sanciona a la autoridad o funcionario público que, mediando causa por delito, y sin respetar las garantías constitucionales o legales, entre en un domicilio sin el consentimiento del morador. Se trata de una entrada irregular en domicilio por no respetar las garantías establecidas.

3.6. Concursos

3.6.1. Con el hurto y otras infracciones

Dado el distinto bien jurídico que se protege, en el hurto y en el allanamiento de morada, son infracciones autónomas, y en caso de concurrencia habrá un concurso medial del art. 77 entre ambas infracciones, si el propósito de sustraer es anterior a la entrada en domicilio ajeno, o concurso real si el ánimo depredatorio es posterior o sobrevenido, particularmente después de haberse suprimido en el CP de 1995 la agravante genérica de morada, por lo que ya no es posible como lo era al amparo del texto anterior entender la existencia de hurto con agravante genérica de morada.

Estas consideraciones cabe extenderlas respecto a los daños, lesiones, amenazas, coacciones. No se apreciará como delito autónomo si forma parte integrante de otro delito como el robo en casa habitada.

3.6.2. Con el robo con fuerza en casa habitada

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

En los arts. 237, 238 y 241 al sancionarse expresamente la casa habitada no puede apreciarse nuevamente el elemento de morada para construir otro tipo, de manera que el robo en casa habitada absorbe el allanamiento.

En Junta General de 19 de octubre de 1998 se planteó el concurso entre el delito de allanamiento de establecimiento abierto al público del art. 203.2 CP y el delito de robo agravado de cometerse en local o edificio abierto al público. Tras el debate se acordó:

«1. Mantener el criterio interpretativo acordado por el Pleno de la Sala en reunión de 22 de mayo de 1997 sobre el concepto de local abierto al público, circunscribiéndolo exclusivamente a la apertura física del mismo

2. En los casos de delitos de robo cometidos en domicilio de personas jurídicas o establecimientos abiertos al público, solo procede aplicar el tipo correspondiente de robo, con exclusión del art. 203 CP

3. Cuando se acredite en el caso enjuiciado, que el ataque a la privacidad va más allá de lo que es inherente al delito de robo, cabría la posibilidad de una situación concursal entre el delito de robo y el delito de allanamiento de morada del art. 203 CP».

Tratándose de domicilio de persona jurídica, la STS 1048/2000 de 14 junio señala que la doctrina jurisprudencial viene sosteniendo en relación con los casos en que se comete un delito de robo con fuerza en las cosas en el domicilio de una persona jurídica, en un despacho profesional u oficina, o en un establecimiento mercantil o local abierto al público fuera de las horas de apertura, que sólo procede tener por cometido el delito de robo, excluyéndose el de allanamiento de morada creado ex novo por el art. 203.1 CP, «salvo que se acreditase que el ataque a la privacidad hubiera ido más allá de lo que es inherente al delito de robo, en cuyo caso cabría la posibilidad de una situación concursal entre ambos delitos». En consecuencia, lo que se expresa en esta doctrina de la Sala es que, protegiéndose en el art. 203 CP ciertas formas de intimidad profesional o mercantil, aunque con una menor intensidad punitiva que la empleada para la protección de la intimidad personal y familiar y siendo esta privacidad de menor rango la que debe servir para interpretar correctamente los delitos previstos en el art. 203 CP, la entrada en uno de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

aquellos locales con ánimo depredatorio, fuera de las horas de apertura, no integrará el nuevo delito de allanamiento sino cuando conscientemente se lesione o ponga en peligro la privacidad profesional, mercantil o de otra parecida índole que en dichos locales se encuentre reservada. Ahora bien, así como la lesión o amenaza a esta privacidad no es un resultado necesario de la entrada subrepticia en los locales mencionados, sí se producen necesariamente la lesión o amenaza a la intimidad personal cuando lo que se invade inconsentidamente es el domicilio de una persona física.

3.6.3. Con el robo con intimidación

Con anterioridad a la reforma operada por la LO 5/10 de 22 de junio se planteaban problemas concursales entre el allanamiento y el robo con violencia o intimidación. Así la STS 179/2007 de 7 marzo, apreciaba el delito de allanamiento de morada juntamente con el delito de robo con intimidación, aunque se suscitaba si este consume el primero. Se calificaban los hechos como constitutivos de robo con intimidación en las personas de los arts. 237 y 242.1 en concurso medial con un delito de allanamiento de morada del art. 202 CP, siguiendo la doctrina de la Sala 2.ª de la que era exponente la sentencia 12.12.2005, en virtud de la cual, cuando la acción se subsume en el robo con intimidación, que ha tenido lugar en la propia morada con entrada inconsentida en la misma, no existía el tipo complejo, aplicable en el robo con fuerza en las cosas en casa habitada del art. 241, ya que funcionaban autónomamente ambos desvalores por lo que era necesario imponer la pena de acuerdo con las normas del concurso, teniendo en cuenta que se trata de acciones distintas, entrar y apoderarse, si bien pueden considerarse ligadas por un vínculo instrumental o de preordenación.

Se entendía que existen diversos bienes jurídicos tutelados por la norma en los delitos de robo violento y allanamiento de morada, en cuanto el primero protege el patrimonio y el otro la intimidad y la inviolabilidad del domicilio, sin que el art. 202 del CP exija un específico ánimo subjetivo en la figura del allanamiento domiciliario, si bien alguna vez la doctrina jurisprudencial lo exigió, la doctrina mayoritaria se conformó con el dolo genérico como se ha señalado.

No obstante, con carácter general en estos casos el allanamiento de morada debía reconducirse al tipo genérico del art. 202.1, y no al subtipo agravado del

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

apartado 2 del mismo precepto, que establece una mayor pena «si el hecho se ejecutase con violencia o intimidación». El subtipo agravado comprende aquellos supuestos en que la violencia o intimidación se hayan ejercitado para entrar o mantenerse en la morada ajena y comprende también los supuestos de vis in re, entendiendo la jurisprudencia equiparable la violencia o intimidación en las personas con la ejercitada in rebus, siempre que la violencia material sobre las cosas sea el medio de ejecución de allanamiento, esto es, que se trate de fuerza material o real y no la prevista en los números 1 y 4 del art. 238. Por tanto, si la violencia ejercitada fue única y exclusivamente encaminada, no a permanecer en la vivienda, sino a la realización del delito contra la propiedad, estimar la misma, además, como cualificadora del subtipo agravado art. 202.2, supondría infracción del principio non bis in idem al valorarse doblemente la misma circunstancia.

La STS 144/2008 de 27 febrero, insistía en que los bienes jurídicos afectados son por el robo, el patrimonio, y por el allanamiento, la intimidad y la inviolabilidad del domicilio. Para abarcar la total antijuridicidad del acontecimiento no bastan las reglas del art. 8 CP, sino que es preciso acudir al art. 77 CP, en cuanto regula el concurso ideal. Otra cosa conduciría al absurdo -véase cómo lo explica la sentencia del 26/5/1999- consistente en que resultará irrelevante que el robo con violencia o intimidación se cometa o no en el domicilio de la víctima en tanto que sí lo sería en el caso de robo con fuerza en las cosas -art. 241.1-.

La Consulta 10/1997 de la FGE admitía la compatibilidad entre allanamiento de morada y robo violento.

Con la reforma del art. 242 CP, por la LO 5/10, ya no cabe la apreciación en concurso de ambas infracciones, toda vez que el legislador, al igual que en el robo con fuerza en las cosas en casa habitada, crea el tipo del robo violento en casa habitada, de manera que el allanamiento queda absorbido en el robo. Dice el nuevo art. 242:

«1. El culpable de robo con violencia o intimidación en las personas será castigado con la pena de prisión de dos a cinco años, sin perjuicio de la que pudiera corresponder a los actos de violencia física que realizase. 2. Cuando el

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

robo se cometa en casa habitada o en cualquiera de sus dependencias, se impondrá la pena de prisión de tres años y seis meses a cinco años...».

3.6.4. Con agresión sexual

La STS 667/2008, señala que «el delito de allanamiento morada del art. 202.1 CP no puede entenderse absorbido por el delito de agresión sexual. En el caso analizado se perpetraron un delito de allanamiento de morada y otro de agresión sexual, de los cuales el primero, era necesario para cometer la agresión sexual, constituyendo medio para llevar a efecto la violencia que forma el complejo delictivo descrito en los arts. 178 y 179 CP junto con el acceso carnal, ello implicaría, a lo más el no entender concurrente ninguna hipótesis de concurso de Leyes y si de una modalidad de concurso ideal de delitos -en su versión medial- penando separadamente los hechos punibles referidos, por cuanto sería la solución más favorable para el reo, tal como ha hecho la sentencia de instancia, si bien por las normas del concurso real».

La STS 458/2003 de 31.3, reitera que «cuando los hechos delictivos encajan en dos disposiciones penales y no es necesario aplicar las dos para abarcar la total antijuridicidad del suceso, nos hallamos ante un concurso de normas a resolver por lo regulado en el art. 8 CP, concretamente por la regla 3.ª que recoge el criterio de la absorción, a aplicar cuando el precepto penal más amplio consume o otro más simple». Pero la consunción de una norma solo puede admitirse cuando «ninguna parte injusta del hecho» queda sin respuesta penal, debiendo accederse en otro caso al concurso de delitos.

Pues bien, en modo alguno puede entenderse por la teoría de la consunción que el delito de allanamiento de morada pueda ser absorbido por el delito de agresión sexual, cuando son totalmente distintos, como distinto es el bien jurídico de una y otra infracción, siendo perfectamente autónomos e independientes sin que entre ellos exista la relación que haga posible un supuesto de progresión o se dé el caso de que uno de los preceptos en los que el hecho es subsumible en su injusto el todo, de modo que el supuesto fáctico previsto por una de las normas constituya parte integrante del previsto por otra, y si se admitiera la aplicación del principio de consunción no se produciría la integra desvalorización del hecho, si se penara solo la agresión sexual y no el allanamiento de morada, quedaría impune una parte injusta del hecho.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

La jurisprudencia ha extendido el supuesto concursal a la agresión sexual y allanamiento de morada en sentencias 18.5.90 y 7.2.87, precisando esta última que «cuando un solo comportamiento, es susceptible de incardinación o subsunción en distintos preceptos penales que se excluyen entre sí caso de ser compatibles su aplicación, se produciría una hipótesis de concurso ideal de delitos, en su modalidad pluriofensiva, se produce un concurso de leyes o conflicto aparente de las mismas, el cual se resuelve o dirime, bien por el criterio de la especialidad -lex especialis derogat legi generali-, bien por el de la gravedad o subsidiariedad -lex primaria derogat lex subsidiaria-, del cual hay manifestaciones múltiples a lo largo del CP y una plasmación general en el art. 8 CP bien por el de la absorción o consunción -ex consumens derogat legi compsuntae-, bien finalmente, por el de la alternatividad; pero si se trata de dos conductas distintas y no de una sola, puede ocurrir que las mismas no se hallen interrelacionadas sino que hayan nacido autónomamente o con independencia, en cuyo caso, se aplicarán las normas reguladoras del concurso real de delitos contenidas en los arts. 73 y 75, o que exista una relación de medio a fin, entre una y otra, en cuyo supuesto habrá un concurso ideal de delitos en su modalidad medial, instrumental o teleológica, prevista en el art. 77, la cual determinará la punición de la infracción de mayor gravedad en su grado máximo y hasta el límite que el dicho precepto establece, y si, ello, perjudica al reo o a los reos, se punirán las infracciones con independencia».

3.6.5. Con quebrantamiento de condena

La SAP de Alicante (Sección 1.ª) núm. 296/2008 de 30 abril, se plantea un problema técnico jurídico en el sentido de determinar si es posible sancionar también por el art. 202 CP adicionándolo al art. 468 CP. Dice que «es obvio destacar que el delito de allanamiento de morada se ha cometido sin que pueda entenderse embebido este delito en el del art. 468 CP, ya que se produce una adición del injusto o actuación ilícita, toda vez que además de quebrantar la orden de alejamiento acercándose al inmueble toma la decisión de entrar en la vivienda con una llave, pero a sabiendas de que tenía expresa prohibición de hacerlo. De no condenar por el delito del art. 202 CP se estaría condenando igual la conducta del que se acerca al inmueble de la víctima que la del que se acerca y entra en el mismo por la puerta con llave o por otro sistema, por lo que el hecho deber estar más sancionado en estas condiciones

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

que si la actuación se circunscribe tan solo al acercamiento al inmueble sin entrar en el mismo».

Pues bien, hay que reseñar que es sabida la gran dificultad que hay, en general, para distinguir entre concurso de leyes o normas y concurso de delitos, particularmente cuando se trata de examinar si se produjo absorción de un delito más simple en otro de mayor complejidad (art. 8.3.1 CP). En estos casos se ha dicho (SSTS 875/2004 de 19.6, 1706/2002 de 9.10), de acuerdo con la doctrina, que solo cabe un criterio de valoración jurídica sumamente impreciso: si la aplicación de una norma cubre la totalidad de la significación antijurídica del hecho nos encontramos ante un concurso de normas; si para abarcar toda esa significación antijurídica es preciso acudir al castigo conforme a las dos leyes en juego, estamos ante un concurso de delitos, real o ideal, según las características de cada hecho.

La SAP de Alicante (Sección 1.ª) núm. 296/2008 de 30 abril, establece que los hechos son legalmente constitutivos de un delito de allanamiento de morada, previsto y penado en el art. 202.1, además del art. 468 CP. No existe concurso ideal del art. 77 CP al no ser uno de los delitos medio para cometer el otro, sino que existe un concurso real. Hace notar que no estamos en el caso de que haya entrado en la vivienda para cometer otro delito con el que concurriría en concurso medial, sino que se trata de dos delitos distintos y de configuración y bien jurídico protegido distintos. En la misma línea de aplicar el concurso real en la concurrencia del quebrantamiento de condena y allanamiento de morada se pronuncian la Audiencia Provincial de Málaga, Sección 2.ª, Sentencia de 31 marzo 2004, la Audiencia Provincial de Asturias, Sección 3.ª, Sentencia de 26 enero 2006.

3.6.6. Con la usurpación

No hay problema alguno, al tener distinta estructura típica y distinto bien jurídico protegido. La SAP de Madrid (Sección 17.ª) núm. 270/2007 de 12 marzo, señala que el apoderamiento de los inmuebles está reservado para otro tipo delictivo distinto, el de «usurpación». Distingue las siguientes hipótesis, con un tratamiento distinto según el bien jurídico comprometido:

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

a) El allanamiento de morada, sin propósito expropiativo, se tipifica y castiga en el art. 202 del CP, como un delito contra la inviolabilidad de domicilio.

b) La ocupación expropiativa violenta o intimidativa de un bien inmueble o de un derecho real inmobiliario se tipifica y sanciona como delito contra la propiedad en el apartado 1 del art. 245, en concurso ideal con el anterior, si se tratase de una morada ajena.

c) La ocupación no violenta de un bien inmueble que no constituya morada, cualquiera que sea su finalidad, se tipifica y castiga por el art. 245.2 como un delito contra la pacífica posesión de aquél.

4. REFERENCIA A LOS LLAMADOS DELITOS INFORMÁTICOS

4.1. Clasificación

Con la denominación de «delitos informáticos», «ciberdelitos», o «delitos telemáticos», se pueden encuadrar los hechos que de alguna forma tienen dos componentes básicos: existencia de delito y uso de la informática. En el CP no existe ningún título ni capítulo dedicado específicamente a ellos, sino que dispersos por el mismo existen toda una serie de delitos que podrían encuadrarse bajo esta denominación. La doctrina solía reservar el número 2.º del art. 197, a los llamados «delitos informáticos» stricto sensu, lo que resulta totalmente incompleto, más aún a partir de la reforma operada por la LO 5/10 de 22 de junio.

ATENCIÓN. La reforma operada por LO 5/10 de 22 de junio, en el marco de los denominados delitos informáticos, para cumplimentar la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, incardina las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, en el nuevo art. 264 CP donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El segundo apartado se refiere al descubrimiento y revelación de secretos, en el nuevo apartado 3 del art. 197 CP, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

datos o programas informáticos contenidos en un sistema o en parte del mismo.

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en noviembre de 2001 se firmó en Budapest el «Convenio de Ciberdelincuencia del Consejo de Europa». Este convenio ha sido ratificado por España el 3 de junio de 2010, con entrada en vigor el 1 de octubre de dicho año. En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

1.1. Acceso ilícito a sistemas informáticos.

1.2. Interceptación ilícita de datos informáticos.

1.3. Interferencia en el funcionamiento de un sistema informático.

1.4. Abuso de dispositivos que faciliten la comisión de delitos.

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

2. Delitos informáticos:

2.1. Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

2.2. Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

2.3. El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

3. Delitos relacionados con el contenido: Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, el 28 de enero de 2003 se promulgó el «Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa» que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

• Difusión de material xenófobo o racista.

• Insultos o amenazas con motivación racista o xenófoba.

• Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

El Convenio sobre Cibercrimen, el primero internacional en esa materia, se abrió a la firma en 2001 y entró en vigor en 2004. A día de hoy lo han adoptado numerosos países miembros del Consejo de Europa, además de Estados Unidos, España, Alemania, Reino Unido e Italia.

Como se ha dicho, las referencias a los delitos informáticos se hallan dispersas en el vigente CP y podrían encuadrarse bajo tal rúbrica los siguientes artículos:

a) El art. 26, respecto al concepto de documento, en el que tiene cabida el documento magnético en cuanto supone un soporte material que expresa o incorpora datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

b) El art. 197 que tipifica el descubrimiento y revelación de secretos, el apoderamiento de mensajes de correo electrónico o datos reservados de carácter personal o familiar o de otro que se hallen registrados en ficheros o soportes informáticos, o el acceso no autorizado a los mismos, o su alteración

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

o utilización en perjuicio de tercero. En el nuevo apartado 3 del art. 197 el acceso sin autorización a datos o programas informáticos.

c) El art. 239 que considera llave falsa a los efectos del tipo de robo con fuerza en las cosas, las tarjetas, magnéticas o perforadas.

d) El art. 248.2 que contempla expresamente la estafa por computación, castigando la producción dolosa de un perjuicio causado por una manipulación informática o artificio semejante. Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

e) El art. 256 que castiga el uso de cualquier terminal de telecomunicaciones sin el consentimiento del titular, ocasionando un perjuicio superior a 400 €.

f) El art. 264 que considera como delito de daños. 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave será castigado con la pena de prisión de seis meses a dos años. 2. El que por cualquier medio, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

g) El art. 270 que protege la propiedad intelectual de la obra literaria, artística o científica fijada en cualquier tipo de soporte.

h) El art. 278 que castiga el descubrimiento de secretos de empresa mediante apoderamiento de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos.

La FGE en relación a los delitos informáticos en sintonía con el Convenio antes referido, distingue:

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

• Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, en definitiva ataques que se producen contra el derecho a la intimidad: incluyendo los delitos de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos (Arts. del 197 al 201 del CP), incluyendo el robo de identidades y la conexión a redes no autorizadas.

• Delitos informáticos que comprenden los tipos penales de los arts. 248 y ss., arts. 263 y concordantes y art. 400 en relación con el art. 386 y ss. Se incluyen:

- Sabotajes informáticos: Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (Art. 263 y otros del CP).

- Fraudes informáticos: Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Arts. 248 y ss. del CP).

- Falsedades: Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad (Arts. 386 y ss. del CP).

• Delitos relacionados con el contenido:

- Amenazas: Realizadas por cualquier medio de comunicación (Arts. 169 y ss. del CP).

- Calumnias e injurias: Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión (Arts. 205 y s y 211 del CP).

- Pornografía infantil: Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz (Art. 187).

La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido (Art. 189).

El facilitamiento de las conductas anteriores (el que facilitare la producción, venta, distribución, exhibición...) (Art. 189).

La posesión de dicho material para la realización de dichas conductas (Art. 189).

• Delitos relacionados con infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor: Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas (Arts. 270 y otros del Código Penal). Esto es, la piratería informática.

• Como consecuencia del protocolo adicional al Convenio Ciber habría que incluir la difusión de material xenófobo o racista y minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad (art. 607.2 CP) e insultos y amenazas con motivación xenófoba o racista.

4.2. Estafa informática. Pharming y phising

Se tipifica como un delito de estafa en el art. 248.2 apartado a) del CP que establece, en redacción dada por LO 5/10 de 22 de junio que modifica el precepto e introduce los apartados b y c):

«2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero».

Dicha tipificación el CP de 1995 llena la laguna legal existente en la materia, modificándose por la citada LO 5/10 de 22 de junio. El concepto general de estafa requería la existencia de engaño capaz de producir error en otro provocando un acto de disposición patrimonial, lo que suponía la inadmisión del engaño a una máquina.

El art. 248, en su apartado 2 a), tipifica la estafa informática, fraude informático o estafa por computación, que debe producir un perjuicio económico, y si es inferior a 400 € puede considerarse la falta de estafa del art. 623.4 CP, al igual que el tipo tradicional de la estafa, si bien difiere en el engaño bastante y en la dinámica comisiva tradicional, por cuanto este y el error de disposición se sustituyen por «alguna manipulación informática o artificio semejante», las cuales pueden consistir en la alteración del software o la introducción de datos falsos en el ordenador, en la alteración del orden del proceso o en el falseamiento del resultado. La doctrina suele distinguir entre manipulaciones externas e internas según sean dentro o fuera del sistema operativo.

En cualquier caso se trata de un delito de resultado que exige para su consumación el efectivo perjuicio económico a través de una transferencia no consentida de un determinado activo patrimonial.

Una modalidad es el llamado phising. La palabra pharming deriva del término farm (granja en inglés), está relacionada con el término phishing, utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. El origen de la palabra se halla en que una vez que el atacante ha conseguido acceso a un servidor DNS y tomado control de este, es como si poseyera una «granja» donde puede hacer uso a placer de los recursos que allí se encuentran. El término phishing proviene de la palabra inglesa«fishing» (pesca), que hace alusión al intento de hacer que los usuarios «piquen en el anzuelo». A quien lo practica se le llama phisher y los métodos que utilizan son variados. Los intentos más recientes de phishing han tomado como objetivo a clientes de

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

bancos y servicios de pago en línea. Los sitios de Internet con fines sociales se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad, otra de las técnicas utilizadas.

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño de páginas web o correos para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor o URLs mal escritas solicitando la verificación de los datos bancarios o de identidad que luego utilizan con ánimo de lucro. E incluso para agotar el delito, bajo apariencia de empresas ficticias, intentan reclutar teletrabajadores por medio de e-mails, chats y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios. Aquellas personas que aceptan la oferta y reciben los fondos que reenvían a cuentas de otros países pueden incurrir en un delito de blanqueo de capitales por imprudencia.

ATENCIÓN. Anzuelo o Estafa electrónica (en inglés phishing) es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). La modalidad denominada phishing o estafa telemática, suele consistir en que mediante el envío de correos electrónicos, se solicita a los clientes de entidades bancarias se pongan en contacto con la misma, a fin de que el usuario realice sus operaciones en una página de la referida entidad que resulta ser un duplicado de la oficial que ejecuta el ciberdelincuente.

4.3. Sabotaje informático. Cracking

Sabotaje informático en un sentido amplio comprende la destrucción de sistemas informáticos completos como los programas, equipos, datos y documentos electrónicos. El término cracking se reserva a los daños informáticos que se producen accediendo a sistemas informáticos ajenos a través de Internet o redes de transmisión de datos.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

La LO 5/10 de 22 de junio modifica el art. 264, que queda redactado:

«1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.º Se hubiese cometido en el marco de una organización criminal.

2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas:

a) Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años.

b) Multa del doble al triple del perjuicio causado, en el resto de los casos.

Atendidas las reglas establecidas en el art. 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del art. 33».

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

El derogado art. 264.2 CP establecía que «la misma pena (de uno a tres años de prisión y multa de 12 a 24 meses) se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

En cuanto a la naturaleza de este delito se sostiene por cierto sector en base al tenor literal del precepto y a su ubicación sistemática, que se trata de un delito contra el patrimonio, de daños cualificados en elementos informáticos lógicos del sistema y no en los elementos físicos del sistema informático. En esta interpretación se contemplan como objeto material la red, el soporte o el sistema informático, donde se almacenan esos datos o programas. Cuando el ataque se produzca sobre un disco u ordenador, soporte físico de esos datos o programas que también se dañan, tal destrucción debería castigarse, además conforme al tipo básico del delito de daños, distinguiéndose, pues, los elementos lógicos y los físicos. La destrucción de los elementos lógicos se sancionaría conforme al 264.1 y los físicos conforme al 263 CP.

Otro sector considera al tipo de referencia como delito autónomo que protege la integridad y la disponibilidad de los datos. Desde esta perspectiva si se causaren daños en los elementos físicos se produciría un concurso ideal, además carecería de relevancia la cuantía económica del daño causado para la determinación del delito al no protegerse la propiedad sino la integridad de los datos.

ATENCIÓN. Cuando los daños afectan a los elementos o soportes físicos (cosas corporales) se debe aplicar el tipo del art. 263 CP, cuando se refieran a los elementos o soportes lógicos (cosas no corporales ni materiales) es de aplicación el 264.2 CP.

Se prevén en el tipo dos conductas básicas, dos subtipos agravados comunes y la responsabilidad penal de una persona jurídica. Las conductas son:

A) Daños a datos, programas informáticos o documentos electrónicos ajenos (art. 264.1 CP). En cuanto a los elementos del delito, el objeto material comprende los daños que se causen a «datos, programas o documentos electrónicos ajenos». En el caso de daño a los elementos lógicos de un sistema

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

informático el objeto de ataque es un fichero o archivo donde se contienen los datos, programas o documentos. Datos son las unidades básicas de información cualquiera que sea su contenido. Documento electrónico es todo conjunto de datos o de información creado informativamente o susceptible de procesamiento informático. Y programas son el cuerpo sistemático de instrucciones legibles por la computadora que permiten realizar una tarea concreta.

En relación a la conducta típica, los verbos utilizados son el apartado 1, borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles, planteándose la cuestión de si es suficiente el ataque al valor de uso o es necesario alterar la estructura material del objeto, cuestión que no es pacífica por el propio concepto del daño que implica menoscabo. De la dicción literal del precepto cabe afirmar que los daños deben recaer sobre los datos, programas o documentos electrónicos, no es necesario que se deteriore la red, los soportes o los sistemas informáticos. La incorporación de un nuevo fichero o programa no produce ninguna modificación o alteración de los existentes que permita sostener la tipicidad de tal conducta.

Como se anticipó, se discute si rige la cuantía mínima de 400 € aplicable al tipo base del delito de daños. Sobre la base de la autonomía de este delito y las dificultades de valoración económica de los datos y por afirmarse que no cabe derecho de propiedad alguno sobre ellos, se niega la exigencia de ese elemento objetivo, de forma que cierto sector doctrinal considera la comisión del delito con independencia del perjuicio, afirmándose que puede ser un daño no tangible, el llamado daño funcional que no es valorable económicamente. Sin embargo, la posición jurisprudencial exigía ese valor para la apreciación del delito. La reforma operada por LO 5/10 en las conductas de los apartados 1 y 2 del art. 264 exige en ambos casos «cuando el resultado producido fuera grave», sin exigir cuantía alguna.

Desde otro lado, se exige la ajeneidad de esos datos, programas o documentos de forma que el propietario no puede ser sujeto activo del delito, bastando en el pasivo la conciencia de que no son propios. Los problemas se plantean en caso de usos compartidos.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

B) Obstaculización o interrupción del funcionamiento de un sistema informático ajeno (art. 264.2 CP). En el apartado 2 los verbos son introducir, transmitir, dañar, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos. Tanto esta conducta como la anterior exigen falta de autorización y que la conducta sea grave. Dada la naturaleza coactiva de la conducta, no cabe exigir cuantía alguna, solo gravedad.

ATENCIÓN. Se prevén en el tipo del art. 264 CP, dos conductas básicas, dos subtipos agravados comunes (apartado 3), y regula la responsabilidad penal de las personas jurídicas (apartado 4). Las conductas son: A. Daños a datos, programas informáticos o documentos electrónicos ajenos (art. 264.1 CP). B. Obstaculización o interrupción del funcionamiento de un sistema informático ajeno (art. 264.2 CP). Los subtipos agravados a ambas conductas son: 1.º Se hubiese cometido en el marco de una organización criminal. 2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

En cuanto a los procedimientos, se encuentran los que implican destrucción o deterioro soporte intencionado, y los propiamente informáticos, entre los que cabe mencionar:

- Eliminación de ficheros. Borrado de datos, programas o documentos mediante los comandos (borrar o delete) o procedimientos de manejo. En los casos en que los documentos permanezcan ocultos o sea posible su reinstalación o recuperación, la conducta es atípica al no haber alteración. Son típicas, además de las acciones de eliminación completa o parcial de un fichero, programa o documento electrónico, la adición, eliminación o sustitución de los datos de un fichero alterándolo y haciéndolo distinto al original, la supresión o modificación de enlaces o vínculos que alteren o inutilicen un programa los cambios en el nombre del fichero, el establecimiento de claves desconocidas para el titular, encriptación y otros procedimientos que lo hagan irrecuperable.

- Virus, gusanos y bombas lógicas. Se trata de procedimientos de destrucción de los elementos lógicos a través de su reproducción. El software malicioso, conocido como malware, es un programa que se instala en un sistema de información causando daños en ese u otros sistemas o utilizándolos para usos diferentes de los previstos por sus propietarios.

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Los virus se replican de un sistema informático a otro para situarse en los ordenadores de forma que puedan destruir o modificar programas y ficheros de datos, presentar un determinado mensaje, provocar fallos en el sistema operativo o interferir los procesos normales de dicho sistema. Las bombas lógicas son programas autoejecutables que se activan cuando el usuario realiza una acción predeterminada o se cumplen determinados parámetros (por ejemplo una fecha). Los gusanos (works) se transmiten por el correo electrónico y se autoejecutan sin necesidad de que el receptor realice acción alguna, explorando la red a la que está conectado para buscar vías de penetración, colapsando las redes locales o servidores, consumiendo la memoria.

De todos ellos solo entran en la conducta típica los virus que supongan destrucción, inutilización, alteración o daño de dato, programa o documento. Los otros al no suponer daño no encuadran en la descripción típica al ser alteraciones del funcionamiento del sistema.

- La denegación de servicio. También llamados ataques «Dds», donde se solicitan datos o servicios a un servidor sin aceptar lo demandado lo que provoca múltiples intento de envío saturando las posibilidades del equipo o dirigiendo correos con direcciones de IP falsas a un servidor que al intentar establecer conexión y no poder hacerlo, termina por bloquearse. Estos métodos no suponen necesariamente supresión o modificación de documento alguno, si se produjera sería de aplicación el tipo de referencia.

- Cracking, al que ya nos hemos referido como el intruso que accede a sistemas informáticos ajenos para borrar ficheros, romper sistemas, introducir virus y en general causar daños.

4.4. Hacking

Con el término hacker (o la acción realizada por este, hacking), se viene a definir la persona que utiliza determinadas técnicas para acceder, sin la debida autorización, a sistemas informáticos ajenos. El hacking o «intrusismo informático» debe diferenciarse del cracking o cracker por ser éstos los términos que identifican a la persona o acción de dedicarse intencionalmente a eliminar o borrar ficheros o sistemas informáticos, a introducir virus en los

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

mismos o, en general, a dañarlos. Tal conducta, según hemos apuntado, tiene una previsión típica en el delito de daños del art. 264 CP.

Nuestro CP no tipifica expresa y autónomamente el delito de hacking. El acceso ilícito a un sistema informático no constituye el delito de daños del art. 264 CP, a diferencia del craking. El intrusismo informático será punible en la medida de que sea medio comisivo para alguno de los delitos que puedan cometerse a través de medios informáticos. En la órbita del derecho comparado aparece criminalizada la figura, el art. 202 a) StGb alemán castiga al que: «sin autorización se procurare para sí o para tercero datos que no estén destinados a él y se encuentren especialmente protegidos contra un acceso no autorizado».

Es posible subsumir los supuestos de Hacking en el tipo de descubrimiento y revelación de secretos, concretamente en la interceptación de telecomunicaciones y acceso inconsentido a datos que existen en soportes informáticos, a los que alude el primer párrafo y el último inciso del párrafo segundo del art. 197 CP.

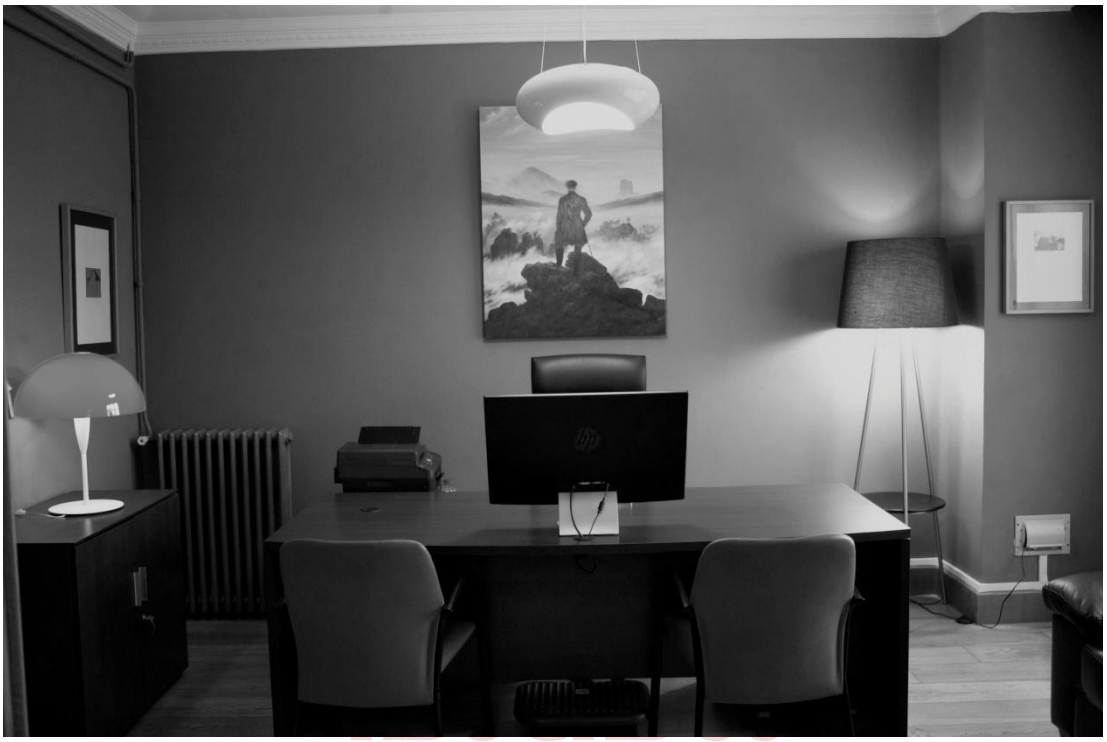
No obstante, se propugna doctrinalmente que debería interpretarse restrictivamente la acción de «acceder», como la averiguación efectiva de las claves de acceso, que es el primer secreto ajeno que se descubre y el que además dará paso al resto del sistema protegido.

4.5. Utilización ilegítima de equipos informáticos

El art. 256 CP castiga el uso de cualquier terminal de telecomunicaciones sin el consentimiento del titular, ocasionando un perjuicio superior a 400 €, donde podrían ubicarse conductas tales como el acceso ilícito mediante un ordenador propio a redes o sistemas informáticos ajenos.

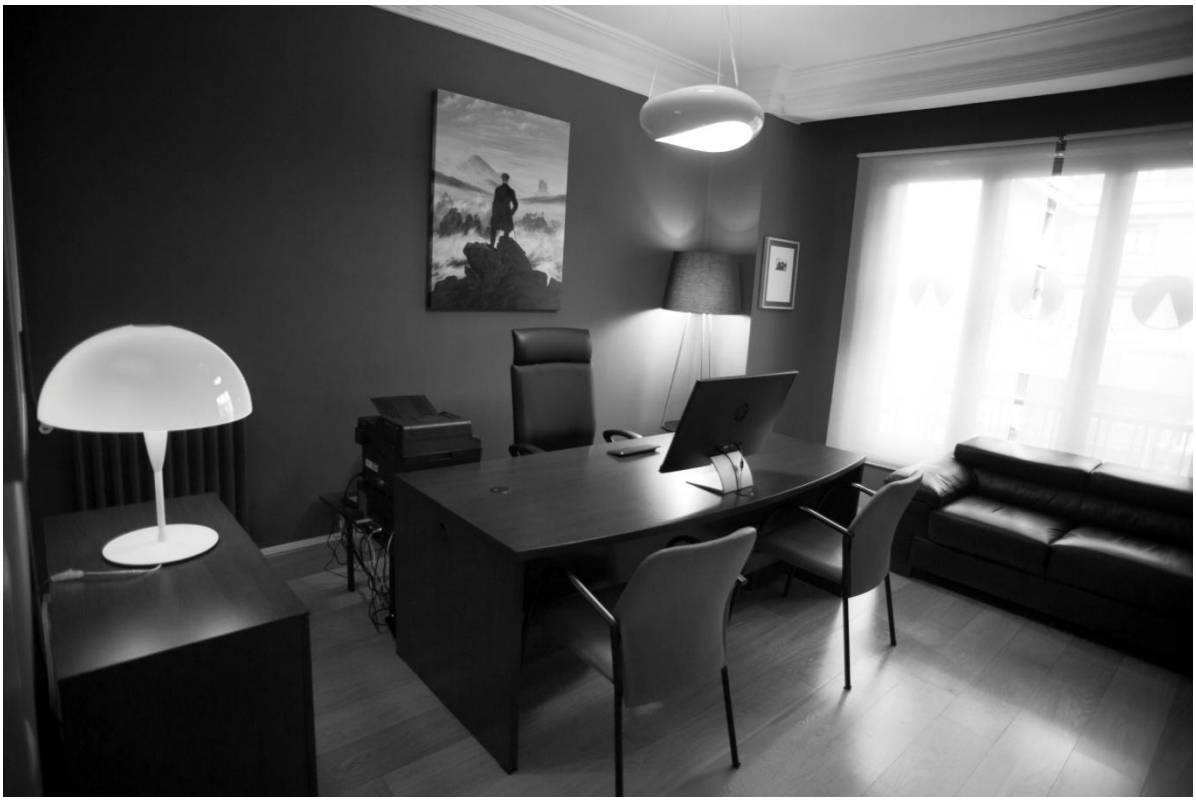
Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

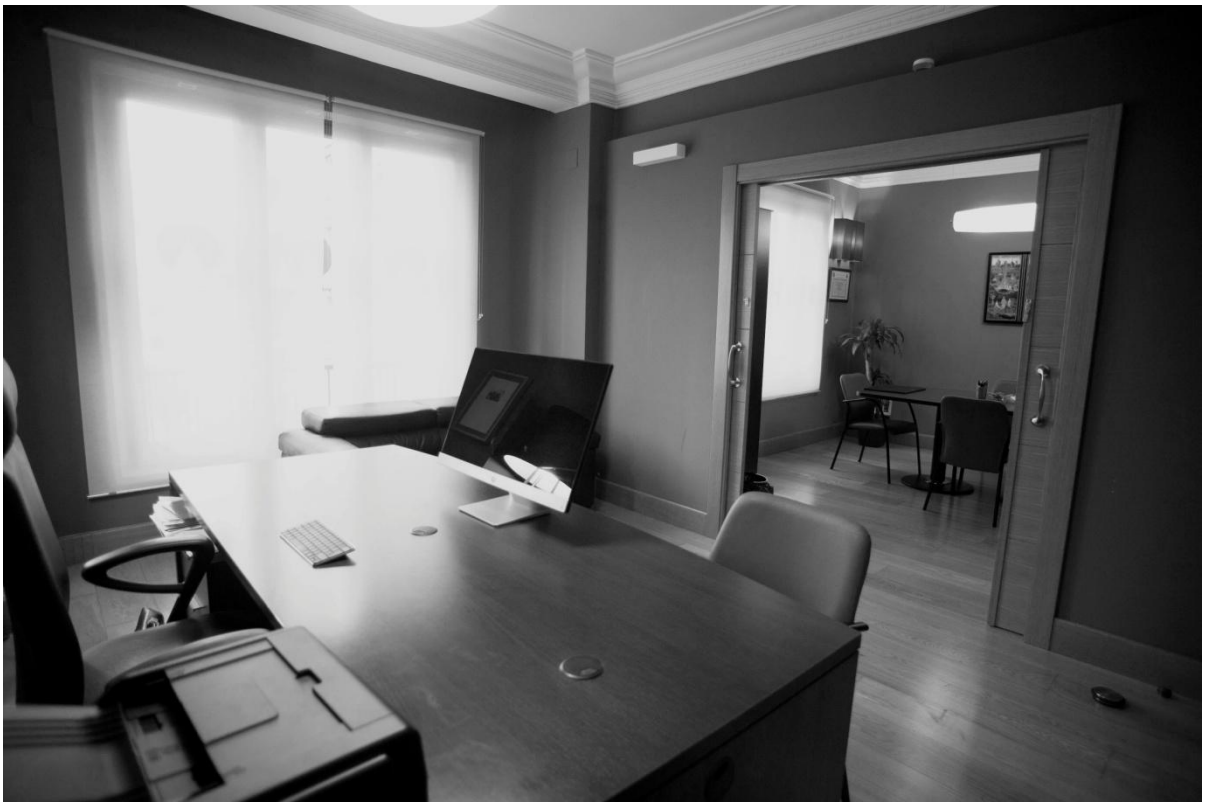


Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

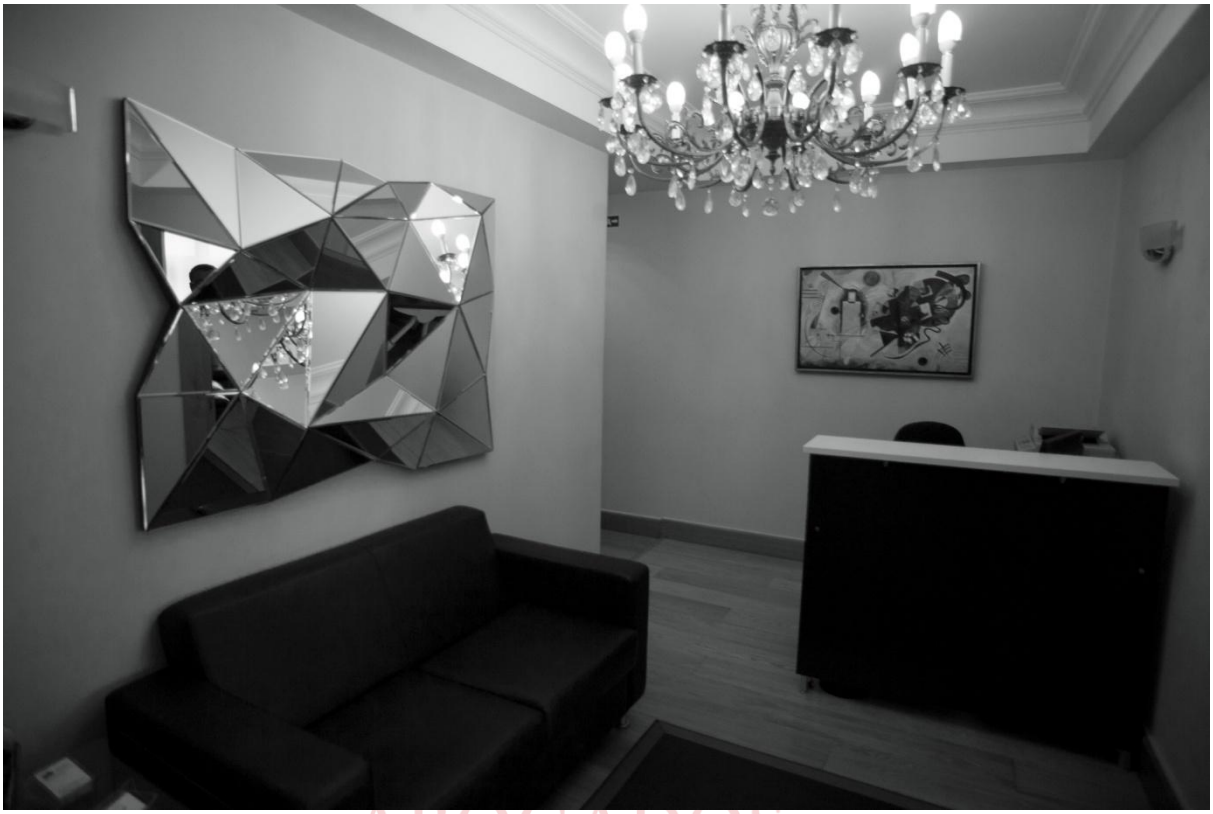
Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com



Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com



Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com



Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com

Campoamor 9 2º 33001 OVIEDO
984 186 927
984 081 875f
www.alfredogarcialopez.es/com