EL DELITO DE INTRUSISMO INFORMÁTICO TRAS LA REFORMA DEL CP ESPAÑOL DE 2015

CYBERCRIME AFTER THE REFORM OF THE SPANISH CP MARCH 2015

Revista Boliviana de Derecho Nº 21, Enero 2016, ISSN: 2070-8157, pp. 210-229

Asunción
COLÁS
TURÉGANO

ARTÍCULO RECIBIDO: 19 de agosto de 2015
ARTÍCULO APROBADO: 26 de agosto de 2015

RESUMEN: En el trabajo se realiza un análisis de las novedades y cuestiones más controvertidas de los delitos de intrusismo informático tras la reforma del CP español de marzo de 2015.

PALABRAS CLAVE: Delitos contra la intimidad, delitos contra la seguridad informática, delitos de intrusismo informático, hacking informático.

ABSTRACT: It is performed a study about the latest developments and most controversial issues of cybercrime after the reform of the Spanish CP March 2015.

KEY WORDS: Crimes against privacy, computer security crimes, crimes of computer intrusion, computer hacking.

I. CONSIDERACIONES PREVIAS

No es aventurado afirmar que el siglo XXI es el del progreso informático. La informática, que se desarrolla en las postrimerías del siglo XX, ha alcanzado un avance vital en el momento presente constituyendo un elemento esencial de las modernas sociedades. La informática y todo lo que ella implica -sobre todo el desarrollo de internet y las redes sociales- ha revolucionado nuestra vida. La tecnología, que aparece como instrumento de ordenación de la información, con el complemento de internet y todo lo que la red supone, origina unas consecuencias importantísimas en el quehacer cotidiano de la ciudadanía. Desde el punto de vista de la tutela jurídica, el abuso de las tecnologías puede llevar a afectaciones relevantes de los derechos ciudadanos, como así ha sido recogido en los ordenamientos penales. El vigente CP español, desde su redacción original de 1995 y con las sucesivas reformas ha ido recogiendo y ampliando conductas, unidas por el denominador común de ser realizadas mediante las nuevas tecnologías, dando lugar a los llamados "ciberdelitos". Sin pretensiones de exhaustividad, pensemos en los ataques que mediante el uso de la red se puede infligir en la intimidad, la propiedad, la indemnidad sexual, etc.

Esta verdadera revolución informática y los efectos que la misma está procurando - también en el ámbito de la realidad criminal-, ha propiciado la preocupación por la aparición de una serie de conductas realizadas mediante la utilización de la informática y las redes sociales con las que se innova en las modalidades de ataque a bienes jurídicos tradicionales y también se erige, como hipotético nuevo interés digno de tutela penal, la propia seguridad en el uso de los sistemas informáticos. De esta manera la ciberdelincuencia surge como nueva modalidad de actuación criminal.

• Asunción Colás Turégano

Asunción Colás Turégano es Doctora en Derecho por la Universidad de Valencia, en enero de 1996 defendió su Tesis Doctoral dirigida por el profesor D. Tomás Vives Antón sobre los problemas de constitucionalidad planteados por los delitos contra el medio ambiente. Desde 1993 imparte clases de Derecho penal en la Universidad de Valencia, siendo profesora titular de derecho penal desde enero de 1999. Ha participado en diferentes proyectos de investigación y tiene monografías y artículos científicos en materias como protección penal del medio ambiente, delincuencia juvenil, diversidad cultural y derecho penal, violencia contra la mujer, delitos contra la intimidad y la propia imagen. Correo electrónico: asuncion.colas@uv.es.

Ante dicha perspectiva, los ordenamientos jurídicos han venido incorporando nuevas modalidades informáticas de ataque a los bienes jurídicos tradicionales, así como figuras específicas de tutela de la seguridad informática, siguiendo una estrategia preventiva de adelantamiento de la línea de defensa de los intereses penales.

En España se habían venido introduciendo algunas conductas caracterizadas por el uso de medios informáticos, como por ejemplo ocurrió con el delito de estafa ya desde la aprobación del CP de 1995. Sin embargo el número de figuras ha ido incrementándose destacando la reforma llevada a cabo en junio de 2010 que recoge de manera específica la figura del intrusismo informático y la recientemente aprobada en marzo de 2015 que ha entrado en vigor el 1 de julio de este mismo año que amplía el elenco de delitos cometidos por medios informáticos[1].

Sin embargo, si hay un ámbito en el que se demuestra la insuficiencia de la intervención aislada de los Estados es el de la criminalidad informática, espacio en el que resulta precisa la colaboración supranacional[2]. Ello ha propiciado la aprobación de diversos convenios y resoluciones de organismos supranacionales de los que España forma parte. En cumplimiento de los mismos se introduce y, posteriormente se amplía la regulación de las conductas en nuestro CP.

Llama la atención la especial fidelidad del legislador español a dichos instrumentos internacionales, pues se realiza frecuentemente una trasposición, casi literal, de las figuras punitivas en ellos recogidas como indicaciones a los diferentes Estados. Circunstancia que abre un debate que no podemos abordar por exceder de las pretensiones de este trabajo y es el referente al respeto a las garantías penales cuando el legislador nacional, en cumplimiento de pretendidas exigencias supranacionales, incorpora al ordenamiento penal nuevos delitos. Como muy gráficamente ha afirmado Galán Muñoz[3] el legislador se escuda en el cumplimiento de dichas exigencias internacionales para justificar el castigo de conductas alejadas de la efectiva lesión del bien jurídico, aunque dichas conductas resulten difícilmente compatibles con los principios y garantías penales como los de intervención mínima, subsidiariedad y proporcionalidad.

En este contexto, la reforma del Código penal aprobada en junio de 2010 introduce en nuestro ordenamiento el delito de intrusismo informático, modificación

1 Relación de delitos recogidos en el CP español cometidos mediante la informática o en los que la difusión informática opera como agravante: art. 183 *ter* (*grooming*), art. 189 (pornografía infantil), art. 248 (estafa informática) art. 264 y ss. (daños informáticos), art. 197.3 (intrusismo informático), art. 270 (propiedad intelectual), art. 510 (provocación a la discriminación, odio o violencia contra grupos), art. 575 (delito de adiestramiento terrorista), art. 578 (enaltecimiento o justificación de los delitos de terrorismo).

2 Galán Muñoz, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", *Revista Penal* (2009) nº 24, p. 90.

3 Galán Muñoz, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", cit., p. 92.

que vino impuesta por los compromisos internacionales contraídos por España dirigidos a la tutela de la denominada "seguridad informática". Así el Convenio sobre la Ciberdelincuencia del Consejo de Europa[4] (Convenio de Budapest de 23 de noviembre de 2001), apela a la necesidad de "aplicar, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia…". Idea que fue concretada en la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. En cumplimiento de la misma se introduce en nuestro CP, en el capítulo de los delitos contra la intimidad y la propia imagen una figura por la que se castigan las conductas de acceso y mantenimiento a los datos y programas alojados en un sistema informático (art. 197.3 CP).

La Decisión marco 2005/222/JAI fue sustituida en 2013 por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, que incorpora nuevas exigencias en materia de protección de los sistemas de información así como para la coordinación de las autoridades competentes. La reforma del CP de 2015 ha venido a ampliar la regulación del 2010 incorporando las nuevas exigencias derivadas de la Directiva, ha mantenido la regulación dentro del capítulo dedicado a la tutela de la intimidad, ampliándose con la introducción de nuevas figuras.

De esta manera, en primer lugar se vuelve a incluir dentro de los delitos contra la intimidad el llamado delito de intrusismo informático, con alguna pero importante modificación y se incorporan dos nuevos delitos: el delito de interceptación de trasmisiones no públicas de datos informáticos. Art. 197 *bis*. 2 y el delito que castiga la producción o facilitación de instrumentos para la realización de los delitos 197 1, 2 y 197 bis. Art. 197 ter

Al análisis de las cuestiones más discutidas sobre las nuevas figuras se van a dedicar las páginas que siguen.

II. EL DELITO DE INTRUSISMO INFORMÁTICO. ART. 197.BIS 1

La figura recoge la conducta de aquel sujeto que emplea su experiencia y conocimientos informáticos para quebrantar las medidas de seguridad de un sistema de información. Aunque estamos ante un delito común que, en principio, no exige ninguna condición especial desde un punto de vista formal, en la práctica la autoría se va a circunscribir a aquellas personas dotadas de unos conocimientos y habilidades especiales en el ámbito de la informática, el usuario medio difícilmente va a tener la habilidad precisa para llevar a cabo la conducta típica. Desde dicha perspectiva sí

4 Ratificado por instrumento de 20 de mayo de 2010 (BOE nº 226, de 17 de septiembre; corrección de errores en BOE nº 249, de 14 de octubre).

podemos afirmar que estamos ante un delito cuyo autor ha de ser un especialista informático. El llamado *hacking blanco,* la conducta del sujeto que para demostrar su habilidad informática o para descubrir fallos en un sistema accede sin autorización al mismo resultaba atípico hasta la reforma de 2010. Sí incriminaba el CP conductas de *hacking negro,* a los conocidos en el lenguaje especializado como *crackers,* quienes utilizando sus conocimientos informáticos realizaban conductas lesivas como causar daños en el propio sistema informático o en los datos o programas en él alojados, atacar la intimidad o el patrimonio, éste último mediante la llamada estafa informática…supuestos que ya eran sancionados.

Una de las cuestiones más controvertidas que plantea la nueva figura es la dificultad de determinar cuál es el valor que con la misma se quiere tutelar, más allá de la genérica referencia a la seguridad de los sistemas de información referido en la Directiva y recogido en la exposición de motivos de la ley de reforma. La complejidad en la determinación del valor tutelado y la parificación del castigo de conductas de mera complicidad muestran un claro adelantamiento de la tutela penal de tan poco preciso bien jurídico.

Es un ejemplo más de este nuevo derecho penal de la seguridad que persigue conjurar cualquier peligro que pueda proyectarse sobre los ciudadanos, mediante el instrumento penal aun a costa del sacrificio de los derechos más esenciales. En cualquier caso no parece que los riesgos fueran tan perentorios puesto que transcurridos cinco años desde la introducción de la figura en el CP, nuestros tribunales apenas han tenido oportunidad de pronunciarse al respecto[5].

1. Bien jurídico protegido

La introducción del llamado delito de intrusismo informático planteó en la doctrina la duda respecto al bien jurídico que se pretendía proteger con el mismo. La figura se incluyó, no en un capítulo nuevo, sino dentro del capítulo dedicado a la tutela de la intimidad lo que provocó que nos encontráramos con dos corrientes doctrinales a la hora de analizar el objeto de tutela, influenciadas por la ubicación elegida por el legislador.

Ciertamente la mayoría de los autores que analizaron la figura se inclinaron por considerar que con su introducción el legislador había pretendido dar *ex novo* una protección de la seguridad de los sistemas informáticos; no obstante la ubicación elegida, dentro de los delitos contra la intimidad, llevó a algún autor a considerar que

5 Son escasas las sentencias en las que se haya condenado por el anterior art. 197.3 (actual 197. *bis)*. En la base de datos Aranzadi Westlaw se han encontrado dos sentencias: SAP Álava de 7 de marzo de 2013. JUR 2014\147603 (acceso no consentido a una cuenta ajena de Facebook) y SAP Murcia de 20 de febrero de 2015 JUR 2015\97040 (acceso no consentido correos electrónicos empleados empresa).

también se pretendía la tutela de dicho bien jurídico, por lo que nos encontramos con una cierta división en este aspecto.

De esta forma, mientras un sector minoritario de la doctrina apostó por considerar, a la vista de la ubicación elegida por el legislador para la nueva figura y por la evidencia de que en muchos casos la realización de la conducta supondrá una indudable afectación al bien jurídico intimidad, que éste era el valor que se pretendía proteger, si bien, la nueva regulación propiciaba un evidente adelantamiento en la protección de la intimidad que se podía ver potencialmente afectada con la realización de las conductas descritas. En apoyo de dicha interpretación, además de los motivos expuestos, jugaba la específica descripción de las conductas, paralelas a las recogidas en el delito de allanamiento de morada: Entrar y mantenerse, por lo que se afirmaba que en este caso se tutelaba aquella parcela de la privacidad ligada al domicilio informático. Desde dicha postura MORALES[6] consideró que lo que se pretende tutelar es "la información vital que se sitúa en estos espacios…reserva de dicho espacio en términos de intimidad". Postura que también mantuvo Bolea Bardón[7] al referir que el bien jurídico es la intimidad al afirmar que el "adelantamiento de las barreras de protección de la intimidad que parte de la consideración que la mera intromisión informática pone en peligro la privacidad del titular del sistema".

Sin embargo, otro sector doctrinal optó por considerar que lo tutelado en este caso es la seguridad de los sistemas informáticos, apuntando las dificultades que la ubicación elegida por el legislador acarrea en la interpretación. En dicha dirección afirma Tomás- Valiente Lanuza[8], que lo que se pretende proteger con la nueva figura es la seguridad de los sistemas informáticos por el importantísimo valor actual de la informática para la organización social, criticando la ubicación dentro de los delitos contra la intimidad a lo que se añade la complejidad de interpretar la figura como adelantamiento de la tutela de este último bien jurídico por los problemas de delimitación con el art. 197. Interpretación que, además, como señala la autora, dejaría fuera del ámbito típico el acceso a sistemas informáticos en los que no estuviera alojado ningún dato íntimo. Con base en ello y a la menor pena con la que está castigada esta conducta frente a las figuras básicas contra la intimidad, considera que "lo que se está protegiendo no es la intimidad en sentido estricto…sino un bien jurídico de carácter instrumental no necesariamente vinculado a ella".

6 Morales García, O.: "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios* (dir. G. Quintero Olivares). Cizur Menor (2010): Aranzadi, p. 185.

7 Bolea Bardón, C.: *Comentarios al código penal. Reforma LO 5/2010* (dir. M. Corcoy –Bidasolo, S. Mir Puig). Valencia (2011): Tirant lo Blanch, p. 468.

8 Tomás Valiente Lanuza, C.: *Comentarios al código penal* (dir.: M. Gómez Tomillo), 2ª ed. Valladolid (2011): Lex Nova, pp. 802-803

En parecidos términos se manifiesta Carrasco Andrino[9], al estimar que "el bien jurídico debe buscarse en el ámbito de la seguridad de las redes o sistemas de información…valores de primer orden en la actual sociedad de la información" por lo que afirma que la finalidad del legislador es "…preservar la seguridad en el tráfico informático y, en particular, la integridad y confidencialidad de los datos y programas informáticos como elementos de los sistemas informáticos". También Morales Prats[10] estima que el delito va dirigido a proteger la seguridad de los sistemas informáticos, si bien matiza que va dirigido como fin último a la tutela de la *privacy* informática de las personas. Finalmente, Anarte/Doval[11] también mantienen que el bien jurídico es la seguridad de los sistemas informáticos, si bien subrayan como problema la falta de contenido del objeto protegido, por lo que sugieren conectarlo con la intimidad por lo que definen la figura como delito de peligro abstracto para la intimidad.

Así pues, en líneas generales la mayoría de la doctrina consideró que con la figura el legislador había introducido una figura de peligro abstracto para la seguridad de las redes informáticas, que podían hipotéticamente suponer un riesgo para la intimidad. Si bien algún autor[12] rechazó dicha interpretación ligada a la seguridad "por su difícil convivencia con el principio de lesividad".

Esa cercanía al derecho a la intimidad y su postura crítica respecto a que se esté tutelando un bien jurídico colectivo lleva a Galán Muñoz[13] a considerar que lo que se tutelaría es "el derecho a la inviolabilidad informática, entendiendo por tal a aquel derecho instrumental y puramente formal que permite o faculta a toda persona a mantener sus sistemas informáticos y, sobre todo, a los datos y a los programas contenidos en los mismos al margen de intromisiones ajenas no deseadas".

En dichos parámetros se había posicionado la doctrina ante una figura compleja por la materia que regula y que implica nuevos retos al jurista en la tutela de nuevos intereses ligados al desarrollo de la informática y la importancia que la misma tiene en las sociedades contemporáneas. Con la nueva regulación nos volvemos a encontrar ante una figura de peligro, que se vuelve a ubicar entre los delitos contra la intimidad por lo que cabrá encajar la tutela de ambos bienes jurídicos: intimidad y seguridad de los sistemas informáticos.

9 Carrasco Andrino, M.: "El delito de acceso ilícito a los sistemas informáticos, en *Comentarios a la reforma penal de 2010* (dir. F.J. Álvarez García, J.L. González Cussac). Valencia (2010): Tirant lo Blanch, p. 250.

10 Morales Prats, F.: *Comentarios a la parte especial del derecho penal* (dir. G. Quintero Olivares, coord. F. Morales Prats). Cizur Menor (2011): Aranzadi, p. 483.

11 Anarte Borrallo, E., Doval País, A.: *Derecho penal. Parte especial. Vol. I. La protección penal de los intereses jurídicos personales* (dir. J. Boix Reig). Madrid (2010): Iustel, pp. 455-456.

12 Morales García, O.: "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", cit., p. 183.

13 Galán Muñoz, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", cit., p. 95.

Resulta evidente que en el momento actual, el generalizado uso de los ordenadores, lleva a convertir tales dispositivos en depositarios de buena parte de nuestra intimidad. No obstante dicha parcela de la privacidad ya estaba tutelada en el CP que castiga con la pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses (art. 197.2) toda una serie de conductas que van desde el simple acceso al sistema informático en el que se encuentran alojados tales datos íntimos hasta su utilización o modificación. Es por ello que la nueva figura de acceso y mantenimiento en un sistema informático, debe implicar algo diferente a lo ya recogido.

La nueva redacción implica, además, un nuevo adelantamiento en la línea de defensa del bien jurídico al dejar de exigirse que el acceso o mantenimiento sea a los datos o programas informáticos alojados en el sistema informático, bastando que el sujeto activo acceda o se mantenga en un sistema de información.

Parece que lo que el legislador se ha propuesto es dar una tutela específica a la seguridad de los sistemas informáticos o de información por la importancia que los mismos tienen en las sociedades actuales, suponiendo dichas conductas un cierto peligro para la intimidad de los ciudadanos, y de entidades, en tanto en algunas ocasiones el acceso a tales equipos o sistemas puede suponer un riesgo evidente para determinados datos privados alojados en dichos equipos o sistemas, lo que justificaría su ubicación en el Código. No obstante de darse efectivamente y actuarse con dicha finalidad entrarán en aplicación las figuras específicas contra la intimidad (art. 197.2).

2. Conducta típica

Como se apuntaba al analizar el bien jurídico protegido, las conductas castigadas por el art. 197.3 antes de la reforma de marzo de 2015 eran coincidentes con las previstas en el delito de allanamiento de morada al castigarse a quien "por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantuviera dentro del mismo en contra de la voluntad de quien tuviera el legítimo derecho a excluirlo…". Lo que como se ha señalado propició interpretaciones del tipo en clave de afectación a la privacidad informática.

Así pues y como venía interpretando la doctrina, el acceso típico requería la vulneración de las medidas de seguridad fijadas para impedirlo, por lo que devenía atípico el acceso a sistemas no protegidos. Siendo también atípico el acceso autorizado por el titular del sistema. La mayor controversia doctrinal se generó respecto a la necesidad o no de acceso licito inicial, en relación a la conducta consistente en mantenerse en el sistema. Si bien la mayoría de la doctrina considera, en atención

a la literalidad del precepto y aplicando la doctrina surgida en la interpretación del delito de allanamiento de morada -con el que el paralelismo es evidente-, que aquí se recogen los supuestos en que el acceso ha sido lícito, surgiendo la ilicitud cuando el sujeto es requerido para que abandone el sistema, negándose y manteniéndose en el mismo[14].

La reforma de 2015 introduce una serie de cambios, unos de redacción y otros de mayor calado en el delito de intrusismo informático. La nueva redacción de la figura recogida en el actual art. 197.1 bis, establece:

"El que por cualquier medio o procedimiento vulnerando las medidas de seguridad establecidas para impedirlo, *y sin estar debidamente autorizado, acceda o facilite a otro el acceso* al conjunto o una parte de un sistema de información o se mantenga en él contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

En primer lugar, respecto a las conductas ya contempladas desde la reforma de 2010, se mantiene como límite de la tipicidad la exigencia de falta de autorización y de vulneración de las medidas de seguridad establecidas para impedir el acceso. Se recogen las dos conductas ya conocidas: acceder y mantenerse, pero se incorpora como novedad la referencia explícita a un supuesto de colaboración, al tipificarse la conducta del que facilita a un tercero el acceso al conjunto o a una parte de un sistema de información.

Con relación a esta última modalidad, tendrán cabida dentro de la misma la conducta de todo aquel que haga posible o ayude al acceso de un tercero, produciéndose de esta forma una cierta y criticable ampliación del ámbito de lo punible, pues se eleva a la categoría de autoría lo que hasta el momento solo podía ser calificado como acto de participación, pudiendo abarcar desde supuestos de colaboración necesaria, hasta supuestos de mera complicidad, lo que resulta especialmente criticable por la desproporción punitiva a la que conduce, castigando con la misma pena supuestos de diferente lesividad.

En todo caso, para considerar consumada la conducta del facilitador, se ha de producir el efectivo acceso al sistema de información. No parece adecuado considerar suficiente para la consumación el simple facilitar el acceso, sin que éste se produzca en el caso concreto. Supondría una inadmisible ampliación del ámbito punible, y además plantearía problemas de delimitación con las nuevas conductas de facilitación de instrumentos para acceder a un sistema informático, recogidas en el

14 Morales García, O.: "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", cit., p.185; Bolea Bardón, C.: *Comentarios al código penal. Reforma LO 5/2010*, cit., p. 468; Tomás Valiente Lanuza, C.: *Comentarios al código penal.* cit., p. 803; Carrasco Andrino, M.: "El delito de acceso ilícito a los sistemas informáticos" cit., p. 251-254.

nuevo art. 197 ter. La exigencia del efectivo acceso al sistema de información para el supuesto del facilitador permite delimitar los supuestos incluidos en una u otra figura. Con efectivo acceso en el 197 bis, sin necesidad de éste en el 197 ter.

Se mantiene la necesidad de vulneración de las medidas de seguridad, por lo que el acceso a sistemas de información o parte de ellos, no protegidos, no constituirá ilícito penal. Respecto a dicha exigencia, la doctrina[15] había considerado que tales medidas de seguridad debían ser "las adecuadas al estado de la técnica, usos y costumbres de la comunidad, no más allá de lo razonable para un usuario medio".

En cualquier caso nos encontramos ante un delito doloso por lo que el sujeto ha de actuar guiado por la finalidad de vulnerar la seguridad de los sistemas de información, por lo que si el acceso es producto de un descuido o negligencia sin la intencionalidad requerida por el tipo, el hecho será atípico.

3. Objeto material

Se modifica también el objeto de la acción dado que en la anterior redacción el acceso o el mantenimiento solo se convertía en típico cuando se proyectaba *sobre datos o programas informáticos contenidos en un sistema informático o en parte del mismo.* Sin embargo, en la nueva redacción dada al precepto las conductas han de proyectarse sobre *el conjunto o una parte de un sistema de información,* sin requerirse el efectivo acceso a los datos o programas en él alojados, dándose un adelantamiento en la barrera de protección del bien jurídico que se pretende tutelar: la seguridad de los sistemas informáticos. Se castiga, por tanto, el simple acceso al sistema informático, sin necesidad de acceder a los datos o programas en él alojados.

De acuerdo con la definición recogida en la Directiva, un sistema de información es: "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automatizado de datos informáticos, así como los datos informáticos almacenados, tratados o recuperados o trasmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento".

Distinguiendo el concepto del de datos informáticos: "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función".

Por tanto, desde una perspectiva conceptual, en la Directiva se distingue entre el sistema de información, referido al aparato o conjunto de aparatos en los que

15 Morales García, O.: "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", cit., p. 187.

se alojan los programas y los datos informáticos, que son procesados mediante los programas informáticos.

Se acentúa de esta forma la especial dirección de la figura hacia la tutela de la seguridad alejándose, al propio tiempo, del otro bien jurídico que se pudiera ver afectado con las conductas descritas, la intimidad, al no precisarse que el acceso o mantenimiento lo sea a los datos o programas alojados en un sistema informático.

En la propia exposición de motivos se enfatiza esa dirección de la figura hacia la tutela de la propia seguridad de los sistemas informáticos frente a la tutela de la intimidad en cumplimiento de la Directiva pues, como se indica de manera expresa, "se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos".

Sin embargo tal adelantamiento provoca serias dudas respecto al contenido de injusto de la figura, Galán Muñoz[16] postula que estamos ante un bien jurídico individual concretado en el derecho a la inviolabilidad informática, considera que el acceso no autorizado a un sistema completamente vacío, sin datos ni programas debería ser una conducta totalmente atípica por ser completamente inocua para el bien jurídico.

4. Sujetos

Nos encontramos ante un delito común que puede ser realizado por cualquier persona, si bien por las particularidades de la conducta el hecho va a ser realizado por un experto en el uso de la informática. Sólo aquella persona con conocimientos informáticos avanzados va a poder, de manera intencionada, acceder en un sistema de información ajeno, es por ello que el círculo de posibles sujetos activos se circunscribe a los sujetos con dichas habilidades.

Respecto al sujeto pasivo, lo será todo aquel que sea titular de un sistema de información, pudiendo ser el titular tanto una persona física como jurídica, previsión que se contempla expresamente en el CP[17].

16 Galán Muñoz, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", cit., pp. 95-96

17 Art. 200 CP: "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".

5. Penalidad

Finalmente, en cuanto a la penalidad, no hay ningún cambio, se mantiene la pena de prisión de seis meses a dos años, sensiblemente inferior a la prevista para los supuestos de acceso a la intimidad informática en el art. 197.2, castigados con la pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

III. INTERCEPTACIÓN DE TRASMISIONES NO PÚBLICAS DE DATOS INFORMÁTICOS. ART. 197 BIS. 2

Nos encontramos ante una figura nueva, impuesta por las exigencias de la Directiva 2013/40/UE, habiéndose limitado el legislador español a trascribir fielmente el contenido de la misma. La principal dificultad que plantea la figura va a ser la delimitación con la conducta de interceptación de telecomunicaciones ya recogida en el propio art 197.1, si bien referida ésta a la tutela de la intimidad.

Establece el nuevo precepto 197 bis 1: "El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

Mediante esta nueva conducta, -copia casi literal del art. 6 de la Directiva 2013/40/UE- se penaliza la utilización de artificios o instrumentos técnicos para interceptar transmisiones "no públicas" de datos informáticos.

Para concretar el alcance de la figura es preciso establecer las diferencias con la modalidad de interceptación recogida en el ap. 1 del art. 197 donde, como sabemos, se castiga al que "para descubrir los secretos o vulnerar la intimidad de otro…. intercepta sus telecomunicaciones…" Respecto a la misma, se ha considerado equivalente a la "intromisión clandestina en una telecomunicación privada"[18]. Bien entendido que sólo van a tener relevancia penal aquellas conductas que interfieran para conocer una telecomunicación, por tanto, como establece el Diccionario de la RAE "un sistema de comunicación telefónica, telegráfica, radio telegráfica o demás análogas**",** no el simple escuchar detrás v.gr. de un puerta o pared la conversación de terceros. Reprochables moralmente pero sin ninguna trascendencia penal.

Se exige por tanto la utilización de medios tecnológicos. Por la experiencia jurisprudencial se ha exigido una cierta tecnicidad de los mismos al no haberse

18 Romeo Casabona, C.:"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet", *Derecho y Conocimiento: Anuario Jurídico sobre la sociedad de la información y del conocimiento* (2002), nº 2, pp. 137-138.

admitido como supuesto típico el escuchar una conversación ajena a través de un teléfono supletorio (AAP Huesca de 21 de septiembre de 2001, TOL 108.591). Exige, pues, la interceptación la utilización de medios técnicos, también en el caso comentado al exigir el tipo la utilización de "artificios o instrumentos técnicos".

En el supuesto ahora incorporado al art. 197 bis. 2 se penaliza la interceptación de transmisiones no públicas de datos informáticos. Las diferencias básicas que encontramos con la interceptación de telecomunicaciones del art. 197.1, son:

1ª) El art 197 bis.2 no exige el elemento subjetivo de actuar "para descubrir los secretos o vulnerar la intimidad", pues con la conducta que ahora se comenta no se pretende lesionar la intimidad de la persona; como se indica en el preámbulo de la ley, las conductas dirigidas a atacar la intimidad ya se encuentran recogidas en el ap. 1. En este caso, la conducta va dirigida a la tutela de otro bien jurídico, la seguridad de los sistemas informáticos. Así pues con la nueva conducta se recogen los supuestos en los que hay una intromisión ilegítima en una trasmisión de datos informáticos, siempre que no se trate de una telecomunicación privada, y se haga con la finalidad de descubrir los secretos o intimidad de otro, en cuyo caso tendríamos que aplicar el art. 197.1.

2ª) Por otro lado el art. 197.1 exige que se intercepten las telecomunicaciones de otro en tanto el art. 197 bis.2 habla de interceptación de transmisiones no públicas de datos informáticos. Por tanto la conducta del art. 197.1 es más amplia al incluir todo tipo de telecomunicaciones: teléfono, fax, e-mail. En tanto el art. 197 bis.2 se ciñe a las transmisiones de datos informáticos.

3ª) Finalmente, la necesidad de que la interceptación se dirija a vulnerar la intimidad en el supuesto contemplado en el art. 197.1 lleva a limitar las telecomunicaciones intervenidas a las puramente privadas; en el otro supuesto se exige que se trate de "trasmisiones no públicas". Por lo tanto, si nos atenemos a la acepción gramatical del término hablaremos de trasmisiones "Notorias, patentes, manifiestas, vistas o sabidas por todos" por contraposición a trasmisiones reservadas. Trasmisiones en las que no se contemplan datos íntimos, pues en dicho caso, siempre que el sujeto haya actuado con la intención de vulnerar la intimidad, tendríamos que calificar por la vía del art. 197.1, el margen de aplicación es, por tanto, bastante limitado. Quizás pueda arrojar algo de luz la lectura del preámbulo de la ley en el que se establece que con la nueva conducta se quiere contemplar la interceptación de "transmisiones automáticas —no personales— entre equipos". Pues la interceptación de comunicaciones personales, ya hemos visto, estaba contemplada.

En cualquier caso habrá que estar al desarrollo jurisprudencial para ver la aplicación que se hace de la figura y su delimitación con la contemplada en el art. 197.1.

IV. PRODUCCIÓN O FACILITACIÓN DE INSTRUMENTOS PARA LA REALIZACIÓN DE LOS DELITOS. ART. 197 1, 2 Y 197 BIS. ART. 197 TER

Finalmente el nuevo art. 197 ter, en cumplimiento de lo dispuesto en el art. 7 de la Directiva 2013/40/UE, prevé el castigo de conductas relacionadas con la producción o facilitación a terceros de instrumentos para la realizar los delitos previstos en los dos primeros apartados del art. 197 (delitos contra la intimidad y contra el *habeas data,* así como los supuestos de intrusismo informático recogidos en el art. 197 bis 1º y de interceptación de transmisiones no públicas del art. 197 bis 2º). De esta forma establece el nuevo Art. 197 ter**,** que:

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

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

Supone un nuevo adelantamiento de la línea de defensa de los bienes jurídicos implicados, intimidad y seguridad de los sistemas informáticos. El delito es doloso por lo que sólo será punible en los supuestos en que se pueda demostrar que la facilitación de tales instrumentos está intencionalmente orientada a la actividad delictiva en concreto.

Una de las principales dificultades que plantea la figura es su delimitación con la también nueva conducta de facilitación del acceso ilegal a tercero recogida en el nuevo art. 197 bis, pues nos encontramos ante un inadecuado solapamiento de ambas figuras. Al analizar este último ya se han destacado los problemas de delimitación con la nueva conducta consistente en facilitar a tercero el acceso ilegal a un sistema de información. Una manera de trazar una línea de distinción entre ambos supuestos, podría ser como ya se ha señalado, exigir que en aquel supuesto se produzca un acceso efectivo al sistema de información por parte de aquel al que se le ha facilitado el acceso. Exigencia que no se requiere en la figura que ahora nos ocupa.

Llama en cualquier caso la atención la parificación punitiva entre ambos supuestos, al menos por lo que se refiere a la pena de prisión, en ambos casos de 6 meses a 2 años. Es cierto que en el delito que ahora analizamos se plantea como alternativa a

la pena de prisión la multa de tres a dieciocho meses, lo que permitirá atemperar la pena en los supuestos de menor lesividad.

V. DISPOSICIONES COMUNES

Para finalizar el análisis de la nueva configuración del intrusismo informático, es necesario referir la serie de disposiciones comunes contempladas en el capítulo

1. Agravación por actuar en el seno de una organización o grupo criminal. Art. 197 quater

Se corresponde el texto del nuevo art. 197 quater con el texto del antiguo artículo 197.8, respecto del que encontramos una ligera diferencia respecto a la aplicación del supuesto.

Establece el nuevo precepto: "Si los hechos descritos *en este Capítulo* se *hubieran cometido* en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado".

De acuerdo con la redacción del ahora derogado art. 197.8 la cualificación se proyectaba sobre los delitos de descubrimiento y revelación de secretos y sobre el intrusismo informático; con la nueva redacción será aplicable también a la figuras de quebranto del secreto laboral o profesional en el caso de que las conductas en ellas previstas se lleven a cabo en el marco de una organización criminal.

2. Responsabilidad penal de la persona jurídica. Art. 197 quinquies

El nuevo art. 197 quinquies reproduce el contenido del párrafo segundo del derogado art. 197.3, que contemplaba la responsabilidad penal de las personas jurídicas por cualquiera de los delitos comprendidos en el antiguo art. 197.

Establece el nuevo precepto: "Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los *artículos 197, 197* bis *y 197* ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33".

No supone ninguna variación respecto a la regulación anterior, más allá de la derivada de la introducción de nuevas figuras delictivas en el ámbito de los delitos contra la intimidad y la seguridad de los sistemas informáticos, a los que también les será de aplicación la cláusula de responsabilidad penal de los entes societarios.

3. Responsabilidad del funcionario público. Art. 198

Prevé el art. 198 una responsabilidad específica para el funcionario público que, "fuera de los casos permitidos por la ley, sin mediar causa por delito y prevaliéndose de su cargo…" realiza cualquiera de los delitos contra la intimidad o contra la seguridad de los sistemas informáticos.

En su caso se prevé la aplicación de la pena prevista en cada supuesto en su mitad superior y además inhabilitación absoluta de seis a doce años.

4. Delito semipúblico

De acuerdo con la previsión contemplada en el art. 201 para proceder por los delitos de intrusismo informático será precisa la denuncia de la persona afectada o de su representante legal de ser ésta menor de edad o discapacitada, en estos casos podrá también denunciar el Ministerio fiscal. Denuncia que no será necesaria si los hechos se atribuyen a un funcionario público de acuerdo con lo dispuesto en el art. 198 CP ni tampoco cuando el delito afecte a los intereses generales o a una pluralidad de personas.

En consecuencia con su carácter semipúblico, el perdón del ofendido o de su representante legal extingue la acción penal, salvo en relación al perdón otorgado por los representantes legales de un menor o discapacitado ya que en este caso el juez puede rechazar la eficacia del perdón, interviniendo el Ministerio fiscal en defensa de los intereses del menor o discapacitado (art. 130. 1. 5º)

VI. VALORACIÓN FINAL

Señalábamos al comienzo de este trabajo los importantes retos que la revolución informática ha planteado a las sociedades actuales. Uno de los más preocupantes, sin duda, el desarrollo de la ciberdelincuencia. En las páginas anteriores hemos referido la nueva regulación de los delitos de intrusismo informático, quizás el núcleo de las figuras que tienen como modalidad comisiva los medios informáticos. Nos encontramos ante un grupo de delitos que tienen como punto de conexión el ser un claro ejemplo de lo que se ha denominado "moderno Derecho Penal del riesgo" propio de las actuales sociedades globalizadas. El legislador, aplicando el principio de precaución, pretende adelantarse a los ataques ampliando cada vez más la influencia del Derecho penal en el control de los nuevos riesgos, sin embargo, es una tarea extremadamente compleja y difícil de atajar mediante un derecho penal de muy pobres resultados. En dicha tendencia expansiva se busca la complicidad de la norma europea para justificar la dudosa necesidad de introducir el nuevo delito aun a costa de sacrificar los principios básicos del Derecho Penal. Cabría cuestionarse si es el Derecho penal la vía adecuada para hacer frente a cualquier amenaza en el ámbito

de la seguridad informática o bien, si no sería más oportuno reservar la amenaza penal para el fin que le es más propio, las ofensas más graves a los bienes jurídicos más importantes, relegando a otros sectores del ordenamiento jurídico la ofensas leves a dichos bienes jurídicos.

BIBLIOGRAFÍA

ANARTE BORRALLO, E., DOVAL PAÍS, A.: *Derecho penal. Parte especial. Vol. I. La protección penal de los intereses jurídicos personales* (dir. J. BOIX REIG). Madrid (2010): Iustel.

BOLEA BARDÓN, C.: *Comentarios al código penal. Reforma LO 5/2010* (dir. M. CORCOY –BIDASOLO, S. MIR PUIG). Valencia (2011): Tirant lo Blanch.

CARRASCO ANDRINO, M.: "El delito de acceso ilícito a los sistemas informáticos**,** en *Comentarios a la reforma penal de 2010* (dir. F.J. ÁLVAREZ GARCÍA, J.L. GONZÁLEZ CUSSAC). Valencia (2010): Tirant lo Blanch.

CARLOS TUREGANO, A.: "Nuevas conductas delictivas contra la intimidad (art. 197, 197 bis, 197 ter)" en *Comentarios a la reforma penal de 2015*. Valencia (2015): Tirant Lo Blanch.

GALÁN MUÑOZ, A.: "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales**"**, *Revista Penal* (2009) nº 24.

MORALES GARCÍA, O.: **"**Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios* (dir. G. QUINTERO OLIVARES). Cizur Menor (2010): Aranzadi.

MORALES PRATS, F.: *Comentarios a la parte especial del derecho penal* (dir. G. QUINTERO OLIVARES, coord. F. MORALES PRATS). Cizur Menor (2011): Aranzadi.

MORALES PRATS, F.: *Comentario a la reforma penal de 2015* (dir. G. QUINTERO OLIVARES). Cizur Menor (2015): Aranzadi.

RAGUÉS I VALLÉS, R., ROBLES PLANAS, R.: "La reforma de los delitos informáticos: incriminación de los ataques a los sistemas de información", pp. 367 a 376. En *El nuevo Código Penal. Comentarios a la reforma* (dir. J.M. Silva Sánchez, coord. N. Pastor Muñoz). Madrid (2012): La Ley.

ROMEO CASABONA, C.:"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet", *Derecho y Conocimiento: Anuario Jurídico sobre la sociedad de la información y del conocimiento* (2002), nº 2.

TOMÁS VALIENTE LANUZA, C.: *Comentarios al código penal* (dir.: M. Gómez Tomillo), 2ª ed. Valladolid (2011): Lex Nova.