Revista Penal México 9
Doctrina
núm. 9, septiembre de 2015-febrero de 2016

La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española (*)

Jorge Alexandre González Hurtado *Universidad Complutense de Madrid*

Resumen: *El ordenamiento jurídico penal español ha venido actualizando sus disposiciones en materia de delincuencia informática de forma acorde a la mayor parte de preceptos internacionales en la materia. En cambio lo ha hecho sin plantearse la idoneidad de agrupar sistemáticamente dichos tipos penales de forma unitaria en el Código Penal. Podemos preguntarnos si llegado el momento actual, esta política criminal sigue siendo la más acertada, mas cuando otros países, como es el caso de México, así han decidido hacerlo.*

Palabras clave: *Delitos informáticos, cibercrimen, Código Penal, bien jurídico protegido.*

Abstract: *The Spanish penal law has been updating its provisions on cybercrime according to most of the international conventions in this area. However, it has not considered gathering such offenses in a unique field in the Criminal Code. We may wonder whether the present time, this criminal policy continues to be the most successful, especially when other countries, such as Mexico, has decided to change this view radically.*

Key Words: *Computer-related crimes, cybercrime, criminal code, legal interest protected.*

Rec: 8-12-2014 | **Rev:** 24-05-2015 | **Fav:** 04-06-2015

(*) El presente artículo toma como referencia la idea planteada a lo largo de mi tesis doctoral 'Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma' que fue calificada en su defensa pública con la nota de sobresaliente *cum laude* por unanimidad.

1. Estado de la cuestión

El legislador español, siguiendo la preocupación de la Comunidad Internacional, así como de la Unión Europea en materias relacionadas con el uso de las nuevas tecnologías,[1] ha manifestado su lógica adhesión a la misma tipificando las acciones que suponen un atentado contra la seguridad en los sistemas informáticos, dando cabida a la mayor parte de las exigencias internacionales en nuestro Código Penal. Sin embargo, en la actualidad ello no ha supuesto la verdadera consagración de este valor —la seguridad en los sistemas de información— como un bien jurídico superior digno de protección penal. Así, en España, los delitos informáticos en sentido amplio —delitos cometidos contra o través de medios informáticos— por su ubicación en el Código, protegen principalmente diversos bienes jurídicos, lo que plantea problemas de interpretación al quedar vinculados sus elementos típicos por los parámetros comunes de interpretación de los delitos con los que se encuentran agrupados.

En consonancia con la preocupación que en el ámbito internacional existe, parece haberse iniciado un camino —al menos en el ámbito doctrinal— en el que se entiende que este tipo de delitos tienen por objeto de protección un bien jurídico de primer orden relacionado con las nuevas tecnologías, pudiendo proteger, además, otros bienes jurídicos que se manifiesten con menor intensidad (intimidad, patrimonio, etc.). Posicionamiento éste que sería inverso a la visión actual del legislador español y de la doctrina tradicional, en la que el bien jurídico protegido principal es aquel relativo al lugar donde se encuentran ubicados en el Código y, en menor medida, son tipos protectores de un bien jurídico indeterminado pero vinculado a la informática. Por todo ello, parece recomendable un análisis del punto de vista que sobre este asunto se tiene en la actualidad en España y, eventualmente, la proposición de un nuevo modelo que, en nuestra opinión, resolvería algunos problemas y mostraría de forma más acertada las preocupaciones existentes en el ámbito público internacional, pero fundamentalmente reflejaría de mejor manera la realidad social actual. A este asunto dedicaremos las siguientes páginas.

2. Delincuencia informática desde un punto de vista contrario a la anclada legislación española

A) Delitos informáticos y teoría del bien jurídico protegido

Tal como ha sido redactado el Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001 y, en menor medida, como están descritas las acciones merecedoras de reproche penal en 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, puede extraerse la idea de que los delitos informáticos en sentido amplio, tanto si son delitos cometidos a través de la informática como si son delitos cometidos contra sistemas informáticos, responden a una clasificación relativamente cerrada. Tales conductas ya no se pueden considerar nuevas, pues al menos en el ámbito práctico y el ámbito extra penal vienen reflejándose de forma constante desde finales de la década de 1980, siempre agrupadas de una forma muy similar.[2] En el ámbito penal, consecuencia de ello, se abre el debate sobre la naturaleza de los tipos penales a través de los que se introducen estos abusos de los sistemas de información, sobre su objeto de protección general y sobre la necesidad, o no, de regular de alguna forma específica aquellos delitos en los que participan con mayor o menor intensidad los sistemas informáticos.

Ya se ha dejado entrever al comienzo que por delitos informáticos, en sentido amplio, se pueden llegar a entender casi cualquier delito clásico en el que se haya usado un sistema informático,[3] lo que en la práctica se traduce en una importante complicación de cara a regular los delitos informáticos de forma unitaria en la legislación penal. En cambio, como ya hemos indicado, desde las instituciones internacionales sí se ha introducido un grupo cerrado de acciones que son en las que, en un sentido menos generalista, se pueden subsumir los delitos informáticos en sentido amplio. Estas con-

[1] Véanse: Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001, Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011; y Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013.

[2] Tanto en los principales trabajos de la OCDE (1986, 1992 y 2002) como en los de las Naciones Unidas (1994) se realizan agrupaciones similares: daños informáticos, acceso ilícito a sistemas informáticos, falsificaciones informáticas, fraudes informáticos, delitos contra la propiedad intelectual e industrial y más recientemente delitos relacionados con la pornografía infantil.

[3] Por ejemplo delitos de injurias o calumnias, o en un caso extremo un delito contra la inviolabilidad de las Cortes (ataque a los sistemas informáticos del Congreso que impiden que se vote alguna medida, por ejemplo).

ductas serían las que engloban delitos en los que los sistemas informáticos son la herramienta fundamental para la comisión del delito —estafa y falsificación informática—, delitos en los que el sistema informático es el objeto del delito —acceso ilícito y daños informáticos—, y delitos relacionados con el contenido, en los que los sistemas informáticos facilitan de forma sustancial la comisión de los mismos —propiedad intelectual o pornografía infantil—.

Tal listado respeta sustancialmente las diversas clasificaciones de los estamentos internacionales, y al respecto cabe preguntarse si sobre el mismo sería posible extraer algunas conclusiones comunes en los delitos que pueda justificar la idea de aglutinarlos en el Código Penal español (en adelante CPesp) dentro de un Título (o quizá dentro de un Capítulo en el Título XXIII del Libro II, vinculado al orden socioeconómico como realiza el Código Penal francés, u en otro Título, como veremos a continuación) que se pudiese denominar "de los delitos informáticos".[4]

Pero, a fin de comenzar por el principio, es obligación recordar que la mayor parte de la doctrina española[5] ha venido a consagrar la idea de exclusiva protección de bienes jurídicos como barrera al poder punitivo del Estado,[6] y es con base en la misma conforme a la que se han ordenado, en términos generales, los delitos en el Libro II del Código Penal español. La teoría clásica de protección de bienes jurídicos como legitimación para la actuación del Estado en materia punitiva[7] ha supuesto la base sobre la que se ha construido nuestro sistema penal vigente y básicamente el de todos los países de nuestra cultura jurídica. Doctrina que exige, para la justificación de los tipos penales, que las conductas en ellos descritas provoquen —o puedan hacerlo— la lesión de un bien jurídico[8]. Queda así excluida del poder punitivo del Estado la regulación de meras inmoralidades[9] o, como se ha señalado más recientemente, de intereses sociales mayoritarios,[10] que no siempre deben ser identificados con un bien jurídico existente. De todo ello se deduce que, si bien se ha manifestado en varias ocasiones la idea de que la seguridad en el campo de la informática y las telecomunicaciones es un campo relevante con un interés social innegable, este hecho no es suficiente para elevar dicho concepto a la categoría de bien jurídico, para lo cual serán necesarios otros requisitos.

Sin embargo, a pesar del conocimiento de lo que un bien jurídico no es, lo cierto es que tampoco existe una definición pacífica en la doctrina que limite el alcance del propio concepto de bien jurídico.[11] La doctrina constitucionalista ha venido a señalar que el punto de partida para la conceptualización de un bien jurídico debe tener origen en la Constitución;[12] sin embargo, reconocer la vinculación de la Constitución y el bien

[4] URBANO CASTRILLO, E., "Los delitos informáticos tras la reforma del CP de 2010", en *Delincuencia informática. Tiempos de cautela y amparo,* Thomson Reuters/Aranzadi, Navarra, 2012, p. 29, defiende que debería existir un Título diferenciado que distribuya en diferentes capítulos, en los que primaría un bien jurídico protegido único, y unas disposiciones comunes finales a todos los tipos penales. Incluso negando este cambio radical, al menos debería completarse un capítulo de delitos informáticos con aquellos propiamente informáticos y una agravante genérica en los demás, cuando para la comisión del tipo se aprovechasen de la facilidad que otorga el medio informático.

[5] GARCÍA-PABLOS DE MOLINA, A., *Introducción al Derecho penal*, 4ª ed., Universitaria Ramón Areces, Madrid, 2006, pp. 173 y ss.; o QUINTERO OLIVARES, G., *Parte General del Derecho penal,* 4ª ed., Thomson Reuters, Navarra, 2010, pp. 67 y ss.

[6] BACIGALUPO ZAPATER, E., *Derecho penal. Parte General*, 2ª ed., Hammurabi, 1999, pp. 43 y 44, señala que "el Derecho penal moderno (a partir de Binding) se ha desarrollado desde la idea de protección de bienes jurídicos. De acuerdo con ella, el legislador amenaza con pena las acciones que vulneran (o ponen en peligro) determinados intereses de una sociedad determinada".

[7] ROXIN, C., *Derecho penal. Parte General. I*, Thomson Civitas, Navarra, 1997 (reimpresión de 2008), p. 51.

[8] GARCÍA-PABLOS DE MOLINA, A., *Introducción…,* ob. cit., p. 174, "no se trata de prohibir por prohibir, de castigar por castigar, sino de hacer posible la convivencia y la paz social".

[9] ROXIN, C., *Derecho…,* ob. cit., pp. 52 y 53. En España, MIR PUIG, S., "Bien jurídico y bien jurídico-penal como límites del *ius puniendi*", en *Estudios Penales y Criminológicos*, núm. 14, 1991, pp. 205 y ss.

[10] Señalado por GIMBERNAT ORDEIG, E., en la presentación de HEFENDEHL, R., *La teoría del bien jurídico. ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Marcial Pons, Madrid, 2007, pp. 12 y ss. En MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho Penal, Parte General,* 8ª ed., Tirant lo Blanch, Valencia, 2010, p. 60, se denomina la "perversión del concepto de bien jurídico".

[11] ROXIN, C., *Derecho…,* ob. cit., p. 54. En España, GARCÍA-PABLOS DE MOLINA, A., *Introducción…,* ob. cit., p. 175; o MIR PUIG, S., *Introducción a las bases del Derecho penal: concepto y método*, 2ª ed., Catapulta, Buenos Aires, 2003, pp. 128 y ss.

[12] ROXIN, C., *Derecho…,* ob. cit., p. 55, "el punto de partida correcto consiste en reconocer que la única restricción previamente dada para el legislador se encuentra en los principios de la Constitución"; en el mismo sentido en España, SILVA SÁNCHEZ, J.M., *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, 2ª ed., Civitas, Madrid, 2001, pp. 92 y ss. Sin embargo, hay manifestaciones en contra de la idoneidad de esta vinculación, WOHLERS, W., "Las jornadas desde la perspectiva de un escéptico del bien jurídico", en HEFENDEHL, R., *La teoría del bien jurídico. ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Marcial Pons, Madrid, 2007, pp. 404 y ss.

jurídico protegido puede ser, en ocasiones, abstracto y complicado.[13] Este hecho le ha costado críticas reseñables a dicha teoría,[14] pero debemos reconocer que al tiempo la configura de forma que los bienes jurídicos pueden ser revisados y su catálogo ampliado. Esta característica se antoja fundamental si queremos verificar la existencia de un bien jurídico digno de protección penal relacionado con los sistemas de información, pues la concepción actual del bien jurídico abarca tanto estados previos a la concreción del Derecho como deberes de cumplimiento creados por éste, siendo el caso de la informática el segundo.[15] Pero tanto la mutabilidad del concepto como la sujeción —que no limitación— a los valores constitucionales no debe llevarnos a la conclusión de que no existen límites al concepto de bien jurídico. En general, el bien jurídico penal es aquel presupuesto necesario para el desarrollo personal y la realización de los individuos en la sociedad, donde encontramos, principalmente la vida o la salud como manifestaciones de lo primero, y la libertad o la intimidad de lo segundo.[16] Estos bienes, además, podrán ser individuales o colectivos,[17] siendo estos segundos especialmente relevantes en el ámbito que nos ocupa, pues están vinculados al orden social o comunitario del individuo. Ahora bien, entender que la seguridad de los sistemas de información responde adecuadamente a la teoría del bien jurídico será, en una parte fundamental, una "cuestión valorativa".[18] Hecha esta apreciación, cabe destacarse que parece adecuado suponer que para que podamos hablar de bien jurídico protegido debemos encontrarnos, al menos, ante valores vinculados al reconocimiento constitucional. Además, debe verificarse la existencia de un interés social de protección, entendido en el sentido de cuál será la afectación para el individuo en caso de ser vulnerado y, vinculado con lo anterior, es necesario graduar el riesgo de afectación del bien jurídico, y por tanto la necesidad de estipular su protección en las normas penales del Estado.

En la búsqueda de un bien jurídico relativo a la seguridad en los sistemas de información debemos realizar igualmente la asociación de los presupuestos anteriores a la realidad de los sistemas informáticos en la actualidad. En el caso español, la vinculación de la seguridad en los sistemas de información y los valores constitucionales aparece en primer lugar en el artículo 1º de la propia Constitución Española de 1978 (en adelante CEsp) al señalar como uno de los valores fundamentales la libertad y la justicia. Así, en el Título preliminar se establece que los poderes públicos deberán remover "los obstáculos que impidan o dificulten su plenitud" (artículo 9.2 CEsp). En el Título primero, el artículo 10 CEsp consagra el libre desarrollo de la personalidad. Si bien el desarrollo de la libre personalidad es un concepto sumamente general, no escapa a la lógica entender que cuando los sistemas informáticos han pasado a formar parte de la realidad cotidiana de la vida de los ciudadanos, un ataque contra estos sistemas afectará, en función de la intensidad del mismo, al desarrollo de la personalidad.[19] En todo caso parece correcto afirmar que la libertad reconocida en la Constitución Española va más allá de la mera libertad de circulación o establecimiento, y se configura como una verdadera facultad de autodeterminación personal, en todos los ámbitos propios de la vida de la persona.[20]

---

[13] Es destacable la compleja construcción doctrinal realizada por GIMBERNAT ORDEIG, E., en la presentación de HEFENDEHL, R., *La teoría*…, ob. cit., pp. 17 y 18, para encajar los delitos relativos a la tortura animal, dentro de los valores constitucionales establecidos, en orden a establecer así el bien jurídico que protegen tales tipos penales en nuestro ordenamiento.

[14] JAKOBS, G., *Derecho penal. Parte General. Fundamentos y teoría de la imputación*, 2ª ed. corregida, Marcial Pons, Madrid, 1997, pp. 47 y 48.

[15] Las normas penales que regulan la seguridad en los sistemas de información no podían responder a la protección de bienes constitucionalmente recogidos, pues en muchos casos son muy posteriores a estos textos constitucionales; sin embargo, ello no obsta para que, una vez producida la aparición de la informática, las normas que la protegen no puedan basar su existencia en nuevos bienes jurídicos sobrevenidos, tan dignos de protección como los originales. ROXIN, C., *Derecho…,* ob. cit., pp. 54 y ss., ejemplifica esta situación con la protección de bienes jurídicos que suponen ciertos delitos tributarios o la provocación de ruidos.

[16] MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho…,* ob. cit., p. 59.

[17] GARCÍA-PABLOS DE MOLINA, A., *Introducción…,* ob. cit., p. 174, aunque sobre la idoneidad de la teoría del bien jurídico para proteger bienes colectivos señalaremos más adelante algunas voces discrepantes.

[18] MIR PUIG, S., *Delincuencia informática*, PPU, Barcelona, 1992, pp. 205 y ss., "la apreciación de cuándo un interés es fundamental para la vida social y cuándo no lo es […] se trata de una cuestión valorativa".

[19] Piénsese en un ataque general contra los sistemas informáticos que gestionan las redes de comunicaciones e Internet que inutilice todos los sistemas de telefonía y de comunicación electrónica en general. Por no hablar de ataques contra el sistema de regulación del tráfico de una ciudad o los sistemas informáticos de plantas de suministro de electricidad.

[20] DE ESTEBAN ALONSO, J., y GONZÁLEZ-TREVIJANO SÁNCHEZ, P., *Tratado de Derecho constitucional, II,* 2ª ed., Universidad Complutense Madrid, Madrid, 2004, p. 76.

Siguiendo esta línea de razonamiento debemos buscar la conexión entre la libertad constitucionalmente establecida y la utilización de sistemas informáticos, y verificar si el uso de éstos es una manifestación de la libertad constitucionalmente reconocida, de tal modo que el nexo constitucional requerido para la apreciación del bien jurídico quede establecido. Según nuestra posición, la libertad para utilizar los medios informáticos sin más límite que el derecho de los demás debe, efectivamente, entenderse subsumido en el concepto constitucional tanto del artículo 1.1 como del 9.2 de la Constitución Española, pues la utilización de estos medios informáticos no es sino una manifestación moderna de la libertad clásica. No se debe confundir esta libertad general, en todo caso, con los ámbitos de la libertad y seguridad establecidos en el artículo 17 de la Constitución, referidos específicamente al derecho de no ser privado de libertad en su manifestación física.[21]

También, desde un ámbito constitucional de la seguridad en relación con los sistemas informáticos, el Estado garantiza el secreto de las comunicaciones (artículo 18.3 CEsp), lo que desde la óptica que ahora interesa parece ser imposible si no se garantiza la seguridad de las redes de comunicaciones y los sistemas informáticos que en ellas participan. La seguridad —como ocurre con la libertad— viene reflejada en la Constitución Española desde diversos prismas: seguridad jurídica (artículo 9.2), seguridad personal (artículo 17.1), seguridad social (artículo 41), seguridad ciudadana (artículo 104.1) y seguridad pública (artículo 149.1.29), siendo estas dos últimas las que a nuestro estudio interesan, pues se vinculan estrechamente con la posibilidad de ejercer el derecho a la libertad informática ya señalado y que el Tribunal Constitucional de España ha interpretado indicando que "la seguridad pública, entendida como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano, según pusimos de relieve en las SSTC 33/1982, 117/1984, 123/1984 y 59/1985, engloba, como se deduce de estos pronunciamientos, un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad intuitiva del bien jurídico así definido".[22] Por tanto, seguimos pudiendo apreciar la posibilidad de vincular la libertad y la seguridad en los sistemas de información con el mandato constitucional dado. La libertad es un derecho general que requiere del establecimiento de un marco de seguridad para su protección.[23] Éste ámbito de la seguridad ha encontrado diverso desarrollo legislativo, en España principalmente en la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado,[24] que establece, en lo que ahora interesa, la organización básica del Cuerpo Nacional de Policía y de la Guardia Civil. En el caso del Cuerpo Nacional de Policía, establece en sus artículos 29 a 36 la estructura básica de la Policía Judicial, donde se señala que corresponde al Ministerio del Interior "organizar Unidades de Policía Judicial", atendiendo a criterios "de especialización delictual" (artículo 30.1). Pues bien, con el fin de seguir tal mandato, en la actualidad la estructura orgánica del Cuerpo Nacional de Policía[25] establece en su jerarquía la Unidad de Investigación Tecnológica (UIT), creada en 2012, y que supone deslindar definitivamente la investigación en asuntos relacionados con la informática de la delincuencia económica, Unidad en la que se encuadraban las investigaciones de este tipo hasta la creación de la UIT. Dentro de la UIT quedan por tanto ubicadas tanto la Brigada Central de Investigación Tecnológica (BIT)[26] como la Brigada Central de Seguridad Informática (BSI), cuyas funciones son "la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e

[21] SSTC 71/1994, de 3 de marzo, 86/1996, de 21 de mayo y 120/1999, de 27 de junio.

[22] STC 104/1989, de 8 de junio, FJ. 3.

[23] DE ESTEBAN ALONSO, J., y GONZÁLEZ-TREVIJANO SÁNCHEZ, P., *Tratado*…, ob. cit., p. 79, "este derecho [la seguridad] hay que entenderlo como la garantía jurídica del individuo frente al poder, para evitar no sólo la privación de su libertad, sino también cualquier forma arbitraria de represión".

[24] Manifestación de esta máxima constitucional debe entenderse también la LO 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, si bien en la misma no se hace referencia a los sistemas informáticos, por lo que la excluimos de nuestro estudio.

[25] Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

[26] La BIT, antes perteneciente a la Unidad Central de Delincuencia Económica y Fiscal (UDEF Central), enmarcada bajo la Comisaría General de Policía Judicial, ahora depende jerárquicamente de la UIT. Una breve reseña se encuentra en LÓPEZ, A., "La investigación policial en Internet: estructuras de cooperación internacional", en *Revista de Internet, Derecho y Política. Revista d'internet, dret i política*, núm. 5, 2007, p. 67; y FERNÁNDEZ LÁZARO, F., "La Brigada de Investigación Tecnológica: la investigación policial", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial/ Cuadernos de Derecho Judicial, Madrid, 2006, pp. 133 y ss.

industrial y los fraudes en las telecomunicaciones y la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes".[27] También en España, la otra gran Fuerza de Seguridad, la Guardia Civil, en su estructura[28] y de forma análoga, cuenta con el Grupo de Delitos Telemáticos (GDT),[29] competente en la investigación "que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como cibercrimen".[30]

Es decir, tanto la UIT como el GDT tienen como función proveer de la seguridad pública[31] necesaria para el ejercicio de lo que podríamos denominar "las libertades informáticas", lo que nos da una idea tanto de la autonomía de esta libertad respecto de otras como de la relevancia asignada por el Estado a este campo.

En todo caso, lo cierto es que el único precepto constitucional que en España se refiere expresamente a la informática es el artículo 18.4 CEsp, que señala que "la ley limitará el uso de la informática" con el fin de garantizar el honor y la intimidad personal y familiar de los ciudadanos, y más importante que ello, el pleno ejercicio de sus derechos a éstos.[32] La ubicación y redacción de este precepto en la Constitución Española genera dudas en cuanto a los límites a los que se refiere al establecer que la ley regulará el uso de la informática. Si se está hablando en todo caso de garantizar el honor, la intimidad, las relaciones familiares y otros derechos análogos, o si cuando se refiere a "pleno ejercicio de los derechos" debe entenderse cualquier otro derecho. A este respecto se ha manifestado la doctrina al vincular el artículo 18.4 CEsp con el artículo 197 CPesp en su plano tecnológico,[33] y se ha llegado incluso a utilizar la expresión de libertad informática, vinculada a la autodeterminación informática —no siempre referidas exactamente a la misma idea— sobre la idea de la protección en el tratamiento informático de datos personales.[34] Esta idea de libertad informática, con la que nuestra posición es coincidente, no agota, en todo caso, el sentido de la libertad informática entendida como la libertad de utilizar los sistemas de información para el completo desarrollo de la persona, sino que es una parte integrante de la misma.

En todo caso, puede preverse el valor constitucional que tiene la utilización de la informática, aunque posiblemente los usos y peligros que sobre ella se ciernen hayan sido sobradamente excedidos respecto de lo que pudo suponer el constituyente español de 1978.

Por último, también se ha tratado de relacionar la seguridad en los sistemas de información con el ámbito de protección constitucional desde el ámbito del artículo 20.1.d de la Constitución Española, en el que siguiendo la Declaración Universal de Derechos Humanos[35] se

---

[27] Página web de la UIT: http://www.policia.es/org_central/judicial/estructura/funciones.html.

[28] Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

[29] El GDT pertenece a la Unidad Central Operativa, dentro de la Jefatura de Policía Judicial, bajo la Dirección Adjunta Operativa de la Guardia Civil. Sobre su labor, expresada por el ex jefe del órgano (2000-2011), se puede ver SALOM CLOTET, J., "Delito informático y su investigación", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial, Cuadernos de Derecho Judicial, Madrid, 2006, pp. 103 y ss.

[30] Página web del GDT: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[31] Denominación que acuñó el Tribunal Constitucional en la STC 104/1989, de 8 de junio.

[32] En un sentido limitado lo ha entendido parte de la doctrina, DE ESTEBAN ALONSO, J., y GONZÁLEZ-TREVIJANO SÁNCHEZ, P., *Tratado*…, ob. cit., p. 124. En nuestra opinión, aceptando la idea de que su ubicación no es la más adecuada, debemos apoyar la idea de que la Constitución se refiere, por un lado, a la ley en sentido general (ley penal, civil, etc.), y por otro, a que los ejercicios que debe garantizar con la limitación del uso de la informática son todos los existentes y no sólo los relativos al honor, la intimidad y las relaciones familiares. En este sentido existen voces novedosas que pretenden una visión más amplia de dicho precepto constitucional; ADÁN DEL RÍO, C., "La persecución y sanción de los delitos informáticos", en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. 20, 2006, p. 153, "aunque el acento se coloque en garantizar la intimidad, se está reconociendo la dificultad de delimitar todos los bienes jurídicos afectados, por lo que el texto constitucional en realidad ha extendido la protección a todos los derechos"; también HERRÁN ORTIZ, A.I., *El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pp. 99 y ss. En realidad siguen la pauta abierta mucho tiempo atrás en PÉREZ LUÑO, A.E., "La protección de la intimidad frente a la informática en la Constitución española de 1978", en *Revista de Estudios Políticos*, núm. 9, 1979, pp. 59 y ss.

[33] REQUEJO NAVEROS, M.T., *El delito de revelación de secreto médico y la protección penal de la información genética,* Colex, Madrid, 2006, pp. 32 y ss.

[34] HUERTA TOCILDO, S., y ANDRÉS DOMÍNGUEZ, C., "Intimidad e informática", en *Revista de Derecho penal*, núm. 6, 2002, pp. 16 y ss., señalan, además, que "como hemos visto, el propio Tribunal Constitucional parece avalar esta tesis diferenciadora al considerar que la llamada 'libertad informática' es un 'derecho autónomo' (SSTC 11/1998 y 30/1999) dirigido a controlar el flujo de informaciones relativas a uno mismo aunque no pertenezcan al ámbito más estricto de la intimidad".

[35] Artículo 19 de la DUDH que establece el derecho universal recibir y difundir información, sin limitaciones y por cualquier medio de expresión.

reconoce el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión", de tal manera que, como se señala en la Declaración de Ginebra de 2003, tal derecho deba revisarse en favor de la realidad tecnológica a la que nos enfrentamos hoy en día[36] y adquiera especial relevancia la protección de los sistemas informáticos que permiten el desarrollo de este derecho universal.[37]

Por tanto, y como ya se ha señalado, la aparición de la informática en la Constitución Española y el resto del ordenamiento es, directa o indirectamente, recurrente. De todo ello, creemos que podemos responder afirmativamente a la pregunta sobre si es adecuada la inclusión de la libertad de utilizar sistemas informáticos, y la seguridad que el Estado debe proveer para ello, como un valor constitucionalmente protegido; cuestión fundamental para continuar con la búsqueda de un bien jurídico relacionado con los sistemas de información. Por otro lado, a la pregunta sobre si la vulneración de este posible bien colectivo de la seguridad informática puede suponer una afectación sobre el individuo y el desarrollo de su personalidad y su desenvolvimiento en la sociedad actual, creemos que se debe responder de manera totalmente afirmativa. En la totalidad de los países de nuestro entorno la utilización masiva de tecnología y sistemas informáticos de forma individual por los ciudadanos es máxima, no se trata simplemente de una forma de ocio, sino que realmente existe un uso social completo en todos los ámbitos del desarrollo de la individualidad del sujeto (económico, laboral, contractual, administrativo, cultural, médico, etc.). Así, el interés colectivo trasciende del mero interés "de la mayoría", al suponer su vulneración la producción de un daño en esferas propias de cada individuo.

Por último, la construcción del bien jurídico exige que el riesgo sobre el mismo sea real para justificar la creación de los tipos penales destinados a protegerlo. En nuestra opinión, este punto es el menos discutible de esta parte de la investigación. El peligro real de ataques sobre sistemas de información no sólo es un riesgo, es una realidad.[38] Si existe una característica constatable en nuestro Derecho penal en relación con los delitos informáticos es que su aparición ha sido muy posterior a éstos, y ya son bien conocidos no sólo los riesgos, sino los posibles efectos de las acciones delictivas.

Precisamente la relevancia del riesgo para la aceptación del bien jurídico característico de los delitos informáticos radica en otro ámbito. La intensidad del riesgo sobre el bien jurídico va a ser uno de los elementos más relevantes a la hora de hacer una selección adecuada de los tipos penales que integran la protección del mismo; en efecto, tal riesgo no se manifestará con la misma intensidad en los delitos de daños informáticos que en los de estafa informática, o en los delitos relativos al contenido (pornografía infantil o propiedad intelectual); pues no en todos ellos aparecerá un riesgo para el bien jurídico de entidad suficiente, y por lo tanto su ubicación sistemática en el Código deberá mantenerse inalterada incluso aceptando la necesidad de incluir un nuevo Título relativo a los delitos informáticos. En ciertos delitos informáticos, el bien jurídico protegido principal no será el relacionado con la seguridad informática, sino con los ya existentes, siendo en todo caso este nuevo bien el afectado de forma secundaria. Al contrario, algunos tipos penales, como veremos, tendrán como objeto primordial la defensa de esta seguridad informática, y de forma secundaria, la protección de otros bienes jurídicos también relevantes.[39]

B) Construcción del bien jurídico protegido en los delitos informáticos: la seguridad en los sistemas de información

En la actualidad debemos entender que el Derecho penal español, y de forma análoga el Derecho penal de la mayor parte de países de europeos con un sistema codificado, no consagran un bien jurídico prote-

[36] COTINO HUESO, L., *Libertad en Internet. La red y las libertades de expresión e información,* Tirant lo Blanch, Valencia, 2007, p. 58.

[37] Sobre la vinculación de la protección del derecho a la información y la seguridad informática se manifiesta COTINO HUESO, L., *Libertad…,* ob. cit., pp. 76 y ss., al inclinarse por entroncar la defensa de los sistemas de información con la libertad de expresión e información, al ser estos "cauces superdesarrollados" de transmitir y difundir información. Por lo tanto, velar por la seguridad de los mismos se convierte en una obligación pública, que debe destinar de cuantos medios disponga (se entiende, por tanto, también el Derecho penal) a este fin.

[38] Se pueden consultar a este respecto los datos que aparecen en las Memorias Anuales de la Fiscalía General de España desde el año 2010.

[39] GALÁN MUÑOZ, A., "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en *Revista de Derecho y Proceso Penal*, núm. 15, 2006, p. 23, señala con razón que "este concepto [criminalidad informática] se delimita atendiendo al hecho de que todos los delitos que se incluyen en su seno afectarían a un bien jurídico colectivo común, con independencia del concreto valor individual que también se pudiese lesionar o poner en peligro por tal conducta".

gido relacionado con la informática o los sistemas de telecomunicaciones.[40] En principio todos los delitos informáticos en sentido amplio protegen bienes jurídicos diversos. En España, el delito de acceso ilícito regulado en el artículo 197 bis y ss. CPesp se encuentra ubicado en los delitos de revelación de secretos, lo que indica que el bien jurídico protegido es la intimidad. El delito de estafa informática del artículo 248.2.a CPesp o los actuales daños informáticos (264 y ss. CPesp) protegen el bien jurídico patrimonio, la falsedad informática (donde se protege la seguridad en el tráfico jurídico)[41] o los delitos relativos al contenido (propiedad intelectual o pornografía infantil) en los que se protege el derecho patrimonial que el autor tiene sobre su creación literaria, artística o científica (artículos 273 a 277 CPesp),[42] y por otro lado la seguridad del menor o su derecho a la propia imagen (artículo 189 CPesp).[43]

Se deduce por tanto que el Código penal español no establece la existencia de un bien jurídico vinculado a la informática que merezca protección, y en el momento actual en el que nos encontramos, en el que los sistemas informáticos han copado absolutamente todas las facetas de la vida en la sociedad, cabría, al menos, preguntarse si eso es o no es correcto,[44]y en su caso tratar de definir ese bien jurídico digno de protección relacionado con los sistemas informáticos, así como analizarlo convenientemente para resolver las incógnitas subyacentes.

B.1. La seguridad en los sistemas de información ¿bien jurídico digno de protección penal?

Comenzando con el análisis de los instrumentos internacionales más relevantes desde una perspectiva europea, es decir, el Convenio sobre la Ciberdelincuencia aprobado en Budapest en 2001, la Decisión Marco de 2005 y su sucesora, la Directiva de 2013, debemos señalar que si bien el concepto de bien jurídico no aparece en sus diversas exposiciones de motivos, sí hacen referencia a la trascendencia de los sistemas informáticos en la sociedad actual, y la necesidad de su protección. El Convenio sobre la Ciberdelincuencia de Budapest de 2001 señala en su preámbulo como uno de los motivos que lo originan "los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas". Pero en lo que ahora nos interesa es muy importante la vinculación de estos cambios con el mantenimiento del nivel de libertad de los individuos al señalar la necesidad de garantizar "la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad", lo que da buena cuenta del nexo, ya señalado en esta investigación, de la aparición de una posible libertad informática, como manifestación de la libertad clásica. Sin embargo, aparte de estas menciones, pronto comienza el articulado del mismo sin hacer más puntualizaciones a este respecto.

En cuanto a la Decisión Marco 2005/222/JAI del Consejo, se expresa en una línea similar, algo más detallada, en la que se pone de manifiesto la vinculación de estos ataques contra sistemas informáticos con objetivos terroristas, al haberse convertido las infraestructuras de la información en elementos vitales de los Estados, y así expresa que "esto pone en peligro la realización de una sociedad de la información segura

[40] MATA Y MARTÍN, R.M., "Criminalidad informática: una introducción al cibercrimen", en *Actualidad penal*, núm. 36, 2003, p. 34, expone sustancialmente esta visión negativa sobre la existencia de un bien jurídico inherente a la informática cuando determina que lo importante para que una actividad informática deba ser entendida como delictiva es que se pueda vincular a un bien jurídico preexistente manifestado por el legislador.

[41] Debemos entenderlo en su sentido más amplio, pues partiendo de las interpretaciones del Tribunal Supremo encontramos muy diversas concreciones del bien sobre las que ahora no interesa debatir. La STS de 27 de mayo de 1988 establece que el objeto de protección es "el ataque a la fe pública o a la confianza de la sociedad en el valor probatorio de los documentos". En otras sentencias se hace referencia a bienes similares, SSTS de 13 de diciembre de 1990, de 27 de junio de 1991, y de 27 de abril de 1992.

[42] Cuestión pacífica tanto en la doctrina como en la jurisprudencia. QUINTANO RIPOLLÉS, A., *Tratado de la Parte especial de Derecho penal*, tomo III, 2ª ed., Revista Derecho Privado, Madrid, 1978, p. 658; RODRÍGUEZ RAMOS, L., "Protección penal de la propiedad industrial", en VV.AA., *Propiedad industrial. Teoría y práctica*, Editorial Centro de Estudios Ramón Areces, Madrid, 2001, p. 361; o BAJO FERNÁNDEZ, M., y BACIGALUPO SAGGESE, S., *Derecho penal económico*, 2ª ed., Editorial Universitaria Ramón Areces, Madrid, 2010, pp. 482 y 483; también STS 1479/2000, de 22 de septiembre. Aunque BERDUGO GÓMEZ DE LA TORRE, I., "La reforma de los delitos contra la propiedad industrial", en *Documentación Jurídica*, núms. 37-40, 1985, p. 740, entendía que debe observarse un bien de naturaleza colectiva.

[43] Doctrina que procede de la STS 22 de junio de 2010, en la que modificaba su anterior criterio, en el que señalaba que el bien jurídico protegido era "la libertad o indemnidad sexual del menor".

[44] Tal lógica evolución ya se señala a mediados de la década de los años noventa en PÉREZ LUÑO, A.E., *Manual de informática y derecho,* Ariel, Barcelona, 1996, p. 70.

y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea" justificando así la regulación penal aprobada.[45] No se puede afirmar que desde los organismos internacionales se esté aceptando la existencia de un nuevo bien jurídico superior. Sin embargo, atendiendo a su enunciado, especialmente en la Decisión Marco, parece quedar suficientemente acreditado que la seguridad informática que se propugna con la regulación se basa en la protección de la libertad informática, que sí queda reconocida. En esta línea sigue la evolución europea del problema, ya que en la Directiva 2013/40/UE hace hincapié en su preámbulo que alguna de las acciones contra los sistemas informáticos "puede por sí sola constituir un grave peligro para el interés público".[46] Podemos por tanto confirmar la tendencia a incardinar la relevancia de la seguridad de los sistemas informáticos, tanto en la libertad individual de los ciudadanos como en la protección de valores colectivos de la sociedad. Lo que convierte a la propia seguridad informática en un elemento de peso considerable en la configuración de una sociedad libre y segura.

Por su parte, el legislador español, en la exposición de motivos de la LO 5/2010 de 22 de junio, de reforma del Código Penal, que introdujo últimamente novedades sustanciales en materia de delincuencia informática (especialmente en lo referente al acceso ilícito y a los daños informáticos), excluye toda posible concepción de un nuevo bien jurídico al señalar en el preámbulo de la ley de reforma que "se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos".[47] A este respecto, la reforma de 2015, a través de la LO 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, no ha variado en nada esta concepción, si bien ha completado algunas lagunas en los tipos penales introducidos en 2010, principalmente tipificando el abuso de dispositivos.[48] En todo caso, y en lo que ahora nos interesa, no parece caber interpretación al respecto, aunque también es cierto que la exposición de motivos en ambas reformas, en lo relativo a estos aspectos, brilla por su brevedad y simplicidad, al limitarse a señalar que tal modificación se debe a la imposición europea y parece desprenderse del escaso interés mostrado tanto en fase prelegislativa como en la legislativa que abrir un debate doctrinal sobre la conveniencia de la ubicación de estos delitos y la posible existencia de un nuevo bien jurídico no era en ningún caso prioritario.[49] De ello se resuelve hacer la transposición desde un ámbito de literalidad, sin entrar en otros debates, lo que desde un punto de política legislativa puede entenderse por la amplitud de las reformas penales llevadas a cabo en 2010 y 2015, pero que no debe ser excusa para que no se plantee en un futuro este debate.

Por tanto, entre la velada referencia a un posible bien jurídico relacionado con los sistemas informáticos, y la negativa visión a este respecto del legislador español, debemos señalar que nuestra posición no sólo está de acuerdo con aquello que se intuye desde el ámbito internacional, sino que va a más allá de éste, al afirmar la existencia de este bien jurídico, no compartiéndose, por tanto, desde nuestro punto de vista, la visión simplista del legislador español.[50]

---

[45] SÁNCHEZ MEDERO, G., "Internet: Un espacio para el cibercrimen y el ciberterrorismo", en *Crisis analógica, futuro digital. Actas del IV Congreso Online del Observatorio para la Cibersociedad, celebrado del 12 al 29 de noviembre de 2009*, Meddia, Cultura i Comunicació (edición electrónica sin numerar), establece la relación entre el paso de la ciberdelincuencia hacia el ciberterrorismo trazando una como la evolución de la otra.

[46] FERNÁNDEZ FERNÁNDEZ, C., "Delitos informáticos", en *Base Informática*, núm. 43, 2009, p. 15, señala como ejemplo que "uno de los motivos que está parando el crecimiento del comercio electrónico es la desconfianza debido a la inseguridad de los consumidores que no se "fían" de utilizar la red para realizar las compras de una forma más cómoda, como puede ser desde casa sin tener que desplazarse, hablamos de la seguridad técnica en el pago electrónico".

[47] Preámbulo de la LO 5/2010, de 22 de junio, Apartado XIV.

[48] Debe destacarse a este respecto que en la tramitación parlamentaria de esta reforma el Grupo Parlamentario de Unión Progreso y Democracia en el Congreso de los Diputados asumió la tesis aquí expuesta, presentando una reforma integral de los delitos informáticos. Dicha propuesta fue finalmente rechazada, desgraciadamente sin siquiera ser debatida, gracias a la mayoría absoluta del grupo que apoyaba al gobierno. http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-66-2.PDF#page=1 (Enmiendas 577 y siguientes).

[49] URBANO CASTRILLO, E., "Los delitos…", ob. cit., p. 18. También en URBANO CASTRILLO, E., "Infracciones patrimoniales por medios informáticos y contra la información, como bien económico", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial/Cuadernos de Derecho Judicial, Madrid, 2006, p. 155, ya se señala que "no parece discutible que el mundo de la informática y de las nuevas tecnologías requiere un tratamiento jurídico propio, penal incluido […] La inexistencia de un apartado concreto sobre 'delitos informáticos' es un hecho. Sin embargo, parece defendible que existiera, dada la especificidad de estas conductas".

Ya hemos señalado al hacer el estudio de la teoría del bien jurídico que, si bien la discusión doctrinal sobre éste no es pacífica, no cabe duda de que las premisas principales existen: la vinculación a la Constitución a través de la libertad y la seguridad no sólo es una cuestión interpretativa, sino que en la normativa internacional queda recogida explícitamente. Y de esta importante manifestación se puede deducir la obvia influencia de la afectación de estos derechos de libertad y seguridad en la esfera personal, aún a pesar de encontrarnos ante un peligro presentado de forma colectiva. El riesgo de vulnerar este posible bien jurídico, al igual que su vinculación constitucional, queda de nuevo manifestado en la normativa internacional, pues el Convenio de 2001 lo recoge explícitamente al señalar como motivo de la aprobación del mismo "el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos",[51] pero más allá va, si cabe, la Decisión de 2005, en la que, amén de utilizar la palabra "peligro"[52] en lugar de riesgo, señala que "se ha comprobado la existencia de ataques contra los sistemas de información […]", lo que supone hablar no ya de riesgo, sino de la concreción de ese riesgo en acciones que ponen en peligro la libertad y seguridad en los sistemas de información.

De todo lo expuesto, creemos correcto afirmar que existe dicho bien jurídico relativo a los sistemas de información, y que su formulación más adecuada sería la de "**seguridad en los sistemas de información**",[53] nomenclatura que hemos venido utilizando de forma abstracta, pero que se puede considerar que recoge sustancialmente las preocupaciones de la mayor parte de la doctrina moderna; esto es, la protección unitaria de los sistemas de información, y, por ende, de su utilización, siendo una visión mucho más avanzada que aquella que sigue pretendiendo establecer que los bienes jurídicos actuales son capaces de integrar todo tipo de nuevos delitos, incluidos los de naturaleza informática. Esta posición, aunque contraria al criterio del legislador español y la mayor parte de países europeos, parece ser respaldada mayoritariamente, como hemos señalado, y al menos en su concepción general, por la doctrina más moderna.[54] Creemos adecuado establecer que el bien digno de protección penal debe ser la seguridad porque es un concepto más general y que no sólo protege la libertad informática, que puede ser considerada como una facultad individual, sino que se configura como un verdadero bien colectivo, ya que los delitos que protegen la seguridad en los sistemas de información tienen un factor general que se extiende más de allá de la mera libertad individual.[55]

El siguiente paso que debe afrontar la doctrina, pues, es ajustar dicho bien jurídico a los tipos penales actualmente existentes para conocer cuáles de ellos deben ser integrados en un eventual nuevo Título del Código Penal español, y cuáles, por el contrario, pueden mantenerse dentro de los límites actuales junto con otros delitos tradicionales.

---

[52] En esta línea se manifiesta MORILLAS CUEVA, L., "Nuevas tendencias del Derecho penal: Una reflexión dirigida a la cibercriminalidad", en *Cuadernos de Política Criminal*, núm. 94, 2008, pp. 18 y ss., se refiere a la "aparición de modernos bienes jurídicos y del surgimiento de nuevos riesgos". También AROCENA, G.A., "De los delitos informáticos", en *Revista de la Facultad de Derecho UNC*, vol. 5, núm. 1, 1997, pp. 44 y ss.; y DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", en *REDUR*, núm. 8, diciembre de 2010, pp. 181 y ss. En palabras de éste último, "cualquier solución pasa por una visión conjunta de todos ellos. Son pues las peculiaridades que plantean los nuevos delitos las que justifican su análisis particular; luego es necesario agrupar los tipos con rasgos y problemas comunes para un tratamiento adecuado y armonioso […] La autonomía de los delitos informáticos debe ser afianzada y desligada de los tipos comisivos tradicionales. Ello, por una razón tanto teórica (si bien las modalidades comisivas informáticas pueden asociarse a tipos ya existentes, la función de las nuevas figuras delictuales sería la protección de la información y no del bien jurídico tradicional) como funcional (garantizar una adecuada persecución de estas conductas).

[53] DE LA MATA BARRANCO, N.J., y HERNÁNDEZ DÍAZ, L., "El delito de daños informáticos. Una tipificación defectuosa", en *Estudios Penales y Criminológicos*, núm. 29, 2009, p. 329, señalan que, según pretende afirmar el Convenio, "no se trata de entender que se protege la información contenida en soportes informáticos porque tenga más valor en sí misma que otra información contenida en otros soportes, pero sí que ello se hace por la importancia que tiene individual y socialmente su integridad y accesibilidad al estar situada en redes o sistemas informáticos de los que hoy en día dependen todos los ámbitos públicos y privados, más allá del daño al dato o sistema concretos".

[54] "Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia." También utiliza la palabra "amenaza" con el mismo significado: "para responder con eficacia a esas amenazas es necesario un planteamiento global en materia de seguridad de las redes y de la información […]".

[55] Se sigue la tesis de GALÁN MUÑOZ, A., "Expansión…", ob. cit., p. 23, que determina que "el injusto típico de estos nuevos delitos se configura atendiendo a la afectación de un bien jurídico colectivo e institucional de perfiles poco definidos: La seguridad y la confidencialidad de los sistemas informáticos". Cercana a esa línea sobre la seguridad informática como núcleo de protección se manifiesta ADÁN DEL RÍO, C., "La persecución…", ob. cit., p. 156, cuando señala que "se puede desarrollar y potenciar el reconocimiento de un nuevo grupo de delitos autónomos en el Código Penal, que tengan en cuenta principios nuevos, una suerte de seguridad o de privacidad informática o de otro modo, pero que no dependan en su interpretación del ámbito patrimonial o de la intimidad o cualesquiera otros bienes jurídicos tradicionales".

B.2. Delitos informáticos que pueden integrar el nuevo bien jurídico

Podemos señalar que, si bien desde nuestra posición es correcta la creencia en la existencia de un valor superior merecedor de protección penal, que además es de primer orden y refleja valores constitucionales tal y como se ha desarrollado la sociedad y que posee las características de ser sustancialmente autónomo, general y colectivo, dicho valor ni es inequívoco ni se han fijado por ahora unos límites al mismo. Por ello, es ahora el momento de tratar de acotar ese bien jurídico digno de protección, y con base en el mismo analizar si existe, y con qué intensidad, en los diferentes tipos de delitos informáticos señalados en el ámbito internacional.[56]

Como hemos señalado, la seguridad en los sistemas de información no se va a manifestar con igual intensidad en todos los delitos informáticos. Conocer cuáles de ellos integran el núcleo de los delitos contra la seguridad en los sistemas de información es esencial para poder llevar a cabo una proposición de reforma coherente.

En principio, salvo mejor criterio, deberán integrar tales delitos aquellos que ponen en peligro el correcto funcionamiento de las redes de información, así como los elementos que forman parte de las mismas. Se entiende, por tanto, que aunque el bien jurídico es común, el objeto material puede diferir en los diferentes tipos penales, de forma que el grupo de estos objetos va a quedar relativamente restringido. Así, éstos se clasificarían de la siguiente manera: a) datos informáticos, que incluye tanto a los programas informáticos como a los documentos electrónicos, en general; podemos usar la expresión "información informática" para referirnos a todos ellos; b) sistemas informáticos, que incluye tanto a ordenadores como dispositivos de telefonía móvil, videoconsolas, equipos médicos informatizados, etc.; y c) redes informáticas, los ca-

[56] Entendemos que el reconocimiento de este nuevo bien jurídico de ámbito colectivo responde a las dudas planteadas por la doctrina, que ha ido aceptando en los últimos años la dualidad entre delitos informáticos en sentido abstracto (todos aquellos en los que aparecen elementos informáticos, y que pueden ser eventualmente cualquier delito tradicional) y delitos informáticos en sentido estricto (aquellos en los que el objeto material del delito es el propio sistema informático o sus elementos lógicos, y cuya aparición en el Código es escasa y muy determinada). A favor de contemplar la posibilidad de la existencia de un nuevo bien jurídico protegido de tratamiento autónomo que afecta a un reducido número de tipos penales se muestran: REYNA ALFARO, L.M., "La criminalidad informática: cuestiones para una reflexión inicial", en *Actualidad Penal,* núm. 21, 2002, p. 545; URBANO CASTRILLO, E., "Infracciones…", ob. cit., pp. 155 y 156, "otra razón que aconsejan ese tratamiento separado y específico de la criminalidad informática, es su incidencia en las categorías y conceptos jurídicos clásicos"; NAVA GARCÉS, A.E., *Delitos informáticos*, 2ª ed., Porrúa, México, 2007, p. 97, señala que "cabe destacar que los delitos informáticos [refiriéndose exclusivamente a los delitos de acceso ilícito, daño y sabotaje informático y estafa informática] van más allá de una simple violación a los derechos patrimoniales de las víctimas"; ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002, p. 69, "no puede partirse ya de la base de configurar el delito informático únicamente sobre el bien o interés jurídico tradicional afectado"; BARRIO ANDRÉS, M., "La ciberdelincuencia en el Derecho español", en *Revista de las Cortes Generales*, núm. 83, 2011, p. 278, "ahora bien, los delincuentes han encontrado en Internet un campo especialmente abonado para la comisión de delitos, lo que exige una respuesta penal específica a estas conductas", para luego señalar como delitos de esta respuesta penal especifica los delitos relacionados con la pornografía infantil, el acceso ilícito y la causación de daños; MAZA MARTÍN, J.M., "La necesaria reforma del Código Penal en materia de Delincuencia Informática", en *Estudios Jurídicos. Ministerio Fiscal*, núm. 2, 2003, p. 299, concluye en su estudio sobre el sabotaje informático en "la conveniencia del tratamiento independiente y separado del sabotaje informático respecto del delito de daños, máxime cuando en éste se protege exclusivamente el patrimonio de un tercero, a diferencia del carácter pluriofensivo de aquel, que se refiere también a otros intereses económicos distintos del meramente patrimonial"; en sentido similar también, ÁLVAREZ VIZCAYA, M., "Consideraciones político-criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Internet y Derecho penal. Consejo General del Poder Judicial*, número 10, 2001 p. 277; ANDRÉS DOMÍNGUEZ A.C., "Los daños informáticos en la Unión Europea", en *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*, núm. 1, 1999, pp. 1726 y ss.; o RODRÍGUEZ MOURULLO, G., LASCURAIN SÁNCHEZ, J.A., y ALONSO GALLO, J., "Derecho penal e Internet", en FERNÁNDEZ ORDÓÑEZ, M.A., CREMADES GARCÍA, J., e ILLESCAS ORTIZ, R. (coords.), *Régimen jurídico de Internet,* La Ley, Madrid, 2001, pp. 280 y ss. En contra: MATELLANES RODRÍGUEZ, N., "Algunas notas sobre las formas de delincuencia informática en el Código Penal", en DIEGO, DÍAZ-SANTOS M.R., y SÁNCHEZ LÓPEZ, V. (coords.), *Hacia un Derecho penal sin fronteras*, Colex, Madrid, 2000, p. 132, se posiciona a favor de la actual regulación a través de las figuras típicas tradicionales al señalar que la protección de los intereses patrimoniales "se pueda[e] seguir ofreciendo desde tipos penales no específicamente informáticos"; MATA Y MARTÍN, R. M., *Delincuencia informática y Derecho penal,* Edisofer, Madrid, 2001, pp. 63 y ss.; o GUTIÉRREZ FRANCÉS, M.L., "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual", en *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja*, *REDUR*, núm. 3, 2005, p. 90, para quien "la utilización pervertida y abusiva de las altas tecnologías en la dinámica comisiva de un hecho ilícito no cambia la naturaleza de éste (el delito seguirá siendo, por ejemplo, una estafa, o un delito de falsedad documental, o de blanqueo de capitales o fraude fiscal…)"; aunque es cierto que la misma autora ha manifestado en GUTIÉRREZ FRANCÉS, M.L., "Reflexiones…", ob. cit., p. 71, que "es hora de replantearse si tiene sentido seguir abordando esta materia como algo excepcional". Con dudas, GALLARDO RUEDA, A., "Delincuencia informática: la nueva criminalidad de fin de siglo", en *Cuadernos de Política Criminal,* núm. 65, 1998, p. 373, "cierto es que la estafa, el robo de información, la copia ilegal, la apología del terrorismo, de la pornografía y de la violencia, la invasión ilícita de la intimidad… son delitos de siempre. Pero también es cierto que la tecnología ha hecho posible diluir la rotundidad de conceptos como el espacio y el tiempo".

nales de transmisión de los datos informáticos entre sistemas informáticos, se encuentren o no en determinado momento realizando su función de canal de comunicación.

Además, cabe señalar que en este bien jurídico que planteamos no existe sólo el riesgo de su vulneración en forma de resultado (delitos de lesión), sino que existen ciertas manifestaciones que, se ha comprobado, sin llegar a producir un daño concreto, pueden poner en riesgo dicho bien con suficiente entidad como para que estas acciones deban ser igualmente incardinadas como delitos contra la seguridad en los sistema de información (delitos de peligro). Es decir, no sólo el daño concreto provoca la vulneración del bien jurídico, sino que acciones encaminadas a la perpetración del daño, pero que nada tienen que ver con él, deben ser igualmente perseguidas al menos en los casos más flagrantes. Nos referimos fundamentalmente a la creación de virus informáticos u otro *software* malicioso, y su difusión por las redes informáticas. La entidad de estas acciones, aunque pudieran no producir daños concretos sobre las clases de objetos materiales referidos, pone manifiestamente en peligro la seguridad en los sistemas de información. Por ello, en nuestra elección de los tipos penales que integran la protección de la seguridad de los sistemas de información se encontrarán tanto delitos de resultado como delitos de peligro.

En este contexto, aunque no vamos ahora a realizar una propuesta más pormenorizada ni una aconsejable propuesta de reformulación de los tipos en torno a la protección de los sistemas de información, podemos señalar sin lugar a dudas que deben incluirse entre ellos los delitos de acceso ilícito y muy estrechamente ligado el intrusismo informático, daño informático, sabotaje informático, abuso de dispositivos y desórdenes públicos en las telecomunicaciones.

A pesar de las diferencias obvias en cada tipo penal, todos ellos reúnen una serie de características comunes más allá del figurado bien jurídico protegido que defendemos.[57] En primer lugar existe una coincidencia sustancial entre los objetos materiales a que se refieren estos delitos —datos informáticos, sistemas informáticos y redes informáticas—, además, la comisión de estas conductas típicas, más allá de suponer un daño en sentido amplio para el sujeto propietario de los datos, el sistema o la red, va a crear una situación de desconfianza hacia la utilización de los medios informáticos en la sociedad.[58] Quebrantar la confianza en la utilización de los sistemas informáticos va suponer un daño —general— de entidad mucho mayor que el daño —concreto— efectivo que se pueda producir sobre los objetos del delito, ya suponga éste un atentado al patrimonio u otros bienes jurídicos tradicionales relevantes. Así, la hipotética situación en la que a través de un ataque informático se accede ilícitamente a los documentos almacenados en un servidor *web* en el que se encuentran los datos relativos a las compras realizadas por sus usuarios; mucho más allá de un posible —pero no automático— delito contra la intimidad, genera una inseguridad creada en los usuarios de sistemas y redes informáticas a continuar ejerciendo su libertad informática, en la que radica la verdadera trascendencia de la acción. No se trata de que la posible vulneración de la intimidad sea de mayor o menor entidad, debido a que posiblemente los sistemas informáticos a los que se ha accedido contengan datos de usuarios de escaso valor en relación con su intimidad, sino que el mero hecho de tal acción crea la desconfianza en esos usuarios, que les plantea la razonable duda sobre lo acertado de utilizar sistemas informáticos en el futuro.[59] Puede resultar igualmente conveniente poner como ejemplo el bloqueo de una página *web,* en la que cientos de miles de usuarios realizan consultas diariamente. Dicha acción puede no implicar un ilícito —civil o penal— meramente patrimonial que afecta al propietario de la *web* atacada, sino que va a trascender

[57] Se puede pensar, de una forma análoga, por ejemplo, en los delitos contra la seguridad vial.

[58] URBANO CASTRILLO, E., "Los delitos…", ob. cit., p. 18, señala que "cuando hablamos de delito informático nos referimos a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta", lo que deja entrever claramente que se posiciona a favor de las dos soluciones a la hora de regular los delitos informáticos en el Código, por un lado aquellos para los que bastará una simple acomodación de tipos clásicos, y por otro aquellos que por sus características especiales, y homogéneas entre ellos, deberán propiciar una regulación autónoma del resto de figuras vigentes.

[59] Sigue esta idea CORCOY BIDASOLO, M., "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", en *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*, núm. 21, 2007, p. 10, al señalar que "se parte de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días, porque de ello depende que no se colapsen las actividades del mundo bancario, bursátil, de seguros, transportes, gestión tributaria, Seguridad Social, sanitario […] Esta segunda posibilidad es la admitida en muchas legislaciones locales estadounidenses que tipifican, de forma autónoma, conductas de acceso ilegal a un sistema informático, su uso sin autorización y la manipulación ilícita y modificación de datos informatizados".

al propietario del objeto para suponer una vulneración de la seguridad y confianza de los usuarios en las redes de información. O siguiendo dentro de lo que hasta ahora en España se consideran delitos patrimoniales, un ataque contra los servidores de la administración pública con el fin de borrar los datos informáticos de los ordenadores en un determinado ámbito (licitaciones públicas, por ejemplo) encuentra una discutida cabida como delito patrimonial.[60] En todo caso, aunque pueda existir el daño patrimonial clásico, parece claro que el bien jurídico que se encuentra principalmente vulnerado no es el patrimonio, sino la seguridad informática de los sistemas y redes informáticas. Todavía más, la mera distribución de virus informáticos no puede considerarse delictiva sino como manifestación de un atentado contra la seguridad en los sistemas de información, pues objetivamente tal acción puede provocar resultados dañinos (en ocasiones, de máxima intensidad) en sistemas informáticos, lo que requiere, por su relevancia, a pesar de tratarse de un mero riesgo abstracto, la intervención del Derecho penal.

Sin embargo, y a pesar de la reciente reforma del Código Penal español de 2015,[61] tanto en el delito de acceso ilícito, en el que, por su ubicación sistemática se entiende como bien jurídico protegido primordial la intimidad, como en los delitos de intrusismo informático, muy relacionado con el anterior, pero vinculado al patrimonio; así como los daños informáticos en los que el bien jurídico primordial se considera el patrimonio, los efectos de este tipo de acciones y el perjuicio en la sociedad que suponen distan mucho de afectar exclusivamente —e incluso principalmente— a los bienes jurídicos tradicionales protegidos en los tipos penales que los acompañan en el Código Penal en la actualidad. Además de éstos, el artículo 560 CPesp que tipifica realmente una suerte de sabotaje informático, suponemos, de especial gravedad atendiendo a la penalidad señalada (de uno a cinco años) por causar daños "que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones" como manifestación de desórdenes públicos, podría ubicarse perfectamente, y con mayor facilidad al tratarse ya de un delito que protege un bien jurídico colectivo, en el catálogo de tipos penales destinados a proteger la seguridad en los sistemas de información. Por último, no debemos olvidar las acciones de abuso de dispositivos, que también deben tenerse en cuenta para una completa cobertura penal de este tipo de delincuencia.

Este listado sería por tanto el de los delitos que integrarían la protección de la seguridad en los sistemas de información y los que, a la postre, deberían formar el núcleo de los delitos contra la seguridad en los sistemas de información, que deberían sufrir una reordenación en el Código Penal español,[62] consecuencia de la cual sería necesario realizar una reevaluación de la interpretación de sus elementos típicos bajo este nuevo prisma.

---

[60] DE LA MATA BARRANCO, N.J., y HERNÁNDEZ DÍAZ, L., "El delito…", ob. cit., p. 330, aunque se refieren al antiguo 264.2 CPesp su conclusión es igualmente válida: "que los daños informáticos lesionen o pongan en peligro la confidencialidad, integridad y disponibilidad de los datos y sistema informáticos no impide que, al mismo tiempo, se vulnere la propiedad u otro tipo de intereses de carácter económico; las conductas que describe el art. 264.2 tendrían, en este sentido, carácter pluriofensivo". También RODRÍGUEZ MOURULLO, G., LASCURAIN SÁNCHEZ, J.A., y ALONSO GALLO, J., *Derecho*…, ob. cit., pp. 261 y ss.; y ROVIRA DEL CANTO, E., *Delincuencia informática*…, ob. cit., pp. 71 y ss.

[61] En contra de una visión de bien colectivo en la llamada "seguridad informática" se muestra 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", en *Revista Penal*, núm. 24, 2009, pp. 95 y ss., que determina que el acceso a un sistema informático ajeno sólo afecta al sistema accedido y a su legítimo usuario y no existe otra afección real de índole colectiva. Violar la seguridad de un sistema informático, en opinión del autor, no es violar la seguridad informática como valor general del ordenamiento, que, es cierto, no descarta su existencia. Construye así el derecho a la inviolabilidad informática, estrechamente relacionado con la intimidad, pero sin ser exactamente igual. Nuestra posición difiere sustancialmente de este punto de vista, pues consideramos, al contrario que el autor, que la seguridad informática como bien colectivo sí se ve vulnerada con la realización de la conducta típica, en tanto que, en el acceso ilícito a un sistema informático, el peligro que tal acción supone para la sociedad tiene una intensidad notablemente mayor por motivos muy diversos. El sujeto que es capaz de acceder vulnerando las medidas de seguridad de un sistema informático puede, a través de dicho acceso, proveerse de múltiples herramientas para acceder a otros sistemas, datos, o producir otra serie de acciones delictivas como daños, estafas, u otros tipos penales, con una capacidad de daño sustancialmente mayor. No es un problema exclusivo del propietario de la máquina a la que se ha accedido ilegítimamente, la capacidad del sujeto de llevar a cabo tal conducta pone en peligro cualquier otro sistema informático que se encuentre conectado al anterior, que hoy en día, con la existencia de Internet, puede ser eventualmente cualquier equipo del mundo. Pero como hemos señalado, la diferente visión parte esencialmente de la consideración diferente de los bienes jurídicos tutelados, siendo la opción elegida por el legislador más cercana a la posición del autor que a nuestra propuesta.

[62] Aunque bajo la jurisdicción francesa es ilustrativo el ejemplo aparecido en prensa hace un tiempo: "Un ataque informático a gran escala ha afectado durante semanas al Ministerio francés de Economía. El asalto […] se centró en documentos preparativos del G20 y de otros asuntos internacionales" (EFE - 07/03/2011).

3. La regulación de los delitos informáticos en el Código Penal federal de México. Un ejemplo que seguir en España

Desde el reconocimiento de que la regulación penal de cada país siempre tiene peculiaridades que un extranjero, aunque hermano, nunca llega a conocer en su totalidad, lo cierto es que no he podido evitar realizar una pequeña, casi sistemática comparación entre la regulación de los delitos informáticos en España y en México. Y lo cierto es que las conclusiones que he extraído de esta comparación son, por una parte, esperanzadoras respecto de cómo pueden hacerse las cosas bien y pronto (el grueso de la regulación mexicana data del año 1999), como fue el caso de México en esta particular temática, y por otro lado, de cierta envidia al comprobar la situación en mi país, España.

Y es que el Código Penal federal de México recoge agrupados de forma más o menos análoga a la proposición expuesta anteriormente para España los tipos penales en los que el bien jurídico relativo a la seguridad en los sistemas de información se manifestaría con mayor intensidad. No sólo eso, sino que tal configuración legal fue establecida allá por el año de 1999, recogiendo en un Código Penal nacional por primera vez, y de forma muy similar, las recomendaciones de las tres normas internacionales de alcance al respecto, que por ejemplo, en Europa, habían tenido un impacto muy limitado en los ordenamientos penales, a saber:

a) En 1989 se aprueba la recomendación R(89)9 del Consejo de Europa.[63] En ella se reconoce la revolución que supuso la implantación de las tecnologías de la información tanto en un sentido positivo como también en un sentido negativo, relativo a los abusos y el crimen derivado de la misma. El texto de la recomendación, tras una introducción a la situación existente en la que repasa los trabajos de la OCDE (la ONU no trataría esta materia hasta el 8º Congreso en 1990), procede a realizar un documento completo desde diversas perspectivas del delito informático. La recomendación divide su contenido en cinco puntos fundamentales, resultando ahora de interés el segundo de ellos, en el que se centra en la elaboración de un listado sobre las conductas que deberían ser consideradas delictivas en los ordenamientos de los Estados; haciendo una doble lista de conductas delictivas: en la primera de estas listas establece aquellas conductas que en todo caso deberían ser consideradas delictivas y, en una segunda lista, enumera una serie de supuestos de regulación recomendada.[64] Podemos extraer de este sistema de doble lista el hecho de reconocer una mayor preocupación por un tipo de conductas que por otras, y el priorizar los esfuerzos legislativos en las materias de la lista de mínimos.
b) En 1992 la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.[65]
c) La ONU, siguiendo una línea de trabajo similar a la de la OCDE, elaboró en 1994 el "Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos" con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad que proteja los sistemas informáticos. Ésta fue una de las herramientas más importantes a nivel internacional en la lucha contra los delitos informáticos, tanto por su nivel de concreción

[61] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[62] Sobre la anterior regulación de los daños informáticos —aunque creemos extensible al resto de los delitos descritos— ya se manifestaba MARCHENA GÓMEZ, M., "El sabotaje informático: entre los delitos de daños y los desórdenes públicos", en *Internet y Derecho Penal. Consejo General del Poder Judicial*, núm. 10, Madrid, 2001, p. 363, al señalar que "el día a día demuestra que esa visión [delitos en los que el interés primordial es el patrimonio de la víctima] ha sido desbordada por una realidad que impide ver en el patrimonio ajeno el único bien jurídico dañado o amenazado por la acción delictiva".

[63] Recommendation nº R(89)9 of the Committee of Ministers to Member States on Computer-related Crime and Final Report of the European Committe on Crime Problems (aprobada por el Comité de Ministros el 13 de septiembre 1989 en la reunión 428 de Delegados), Council of Europe Publishing and Documentation Service, Estrasburgo, 1990.

[64] En la Recommendation nº R(89)9 on computer-related crime…, ob. cit., pp. 36-68, se reconocen dentro de la lista mínima el fraude informático, la falsificación informática, daños a datos o programas informáticos, el sabotaje informático, el acceso ilícito, la interceptación ilícita y delitos contra la propiedad intelectual e industrial. La lista opcional de conductas a regular incluye la alteración de datos o programas informáticos, el espionaje informático, la utilización de un ordenador sin consentimiento de su titular y la utilización de un programa informático sin el consentimiento de su titular.

[65] OCDE: "Guidelines for the Security of Information Systems", 1992:
www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

como por realizarse en el seno de la mayor organización internacional que existía.[66]

Resulta importante señalar que la legislación mexicana de 1999, que introduce los delitos informáticos, toma la correcta —y poco común— decisión de incorporar a su ordenamiento la normativa internacional, con pocos cambios en lo sustancial. Así, mediante Decreto publicado en el *Diario Oficial de la Federación* el 17 de mayo de 1999, se introdujo un nuevo Capítulo II en el Título IX del Libro II referente al "Acceso ilícito a sistemas y equipos de informática", y que comprende los actuales 211 bis 1 y 211 bis 7. Estos siete artículos del Código Penal federal recogen casi en su totalidad las conductas que ponen en riesgo la seguridad en los sistemas de información, y además lo hacen desde una perspectiva no tanto individual, sino de defensa de intereses colectivos. Ello se puede observar a la perfección en el nivel de detalle alcanzado en su redacción, en especial en el párrafo segundo de los artículos 211 bis 2 y 211 bis 3 cuando tipifica el acceso y el daño informático a ordenadores del Estado, que ha sido ampliado a los equipos de seguridad pública en 2009.[67] En la misma línea tipifica el acceso y daño a sistemas informáticos de entidades financieras del país. Tipo penal absolutamente novedoso en aquel momento y previsor de la importancia de la informática en el siglo que estaba por venir.

Lo cierto es que hoy por hoy, mediada la segunda década del siglo XXI, aquella decisión de introducir en el ordenamiento penal mexicano las recomendaciones internacionales con tal nivel de detalle ha permitido a México ser pionero en la regulación de la delincuencia informática en el mundo, y un buen ejemplo para el resto de países de nuestro entorno, como sin duda es España.

Es igualmente cierto, y debemos señalarlo que no parece que esté todo el camino recorrido en la legislación mexicana, pudiendo, como propongo, para la española, deslindar definitivamente a los delitos informáticos de otros tipos penales y crear un nuevo Título que recoja, sustancialmente, lo contenido en los artículos 211 bis 1 a 211 bis 7, pues, como hemos señalado, parece que cuestiones contenidas en esos artículos referidas al orden público —como son los párrafos segundo y tercero de los artículos 211 bis 3 y siguientes— mucho tienen que ver con lo que hemos venido a denominar en este artículo "seguridad en los sistemas de información" como bien jurídico autónomo y digno de protección penal, y algo menos con el bien jurídico intimidad con el que comparten Título en el Código Penal federal.

Por otro lado, el Código federal no contempla lo que se ha venido a llamar abuso de dispositivos que faciliten la comisión de delitos, actividades que empiezan a ser consideradas un elemento básico de la delincuencia informática más bien a partir del Convenio sobre la Ciberdelincuencia de Budapest de 2001. Es cierto también, y así debe ser advertido, que tales hechos típicos se encuentran de forma más o menos extensa contenidos en los códigos penales de las entidades federativas, aunque siempre desde una perspectiva del fraude económico, y no como hechos merecedores de protección desde la perspectiva de la seguridad en los sistemas de información.

En todo caso, y concluyendo este brevísimo excurso, la legislación penal mexicana a nivel federal es un buen espejo donde debería mirarse el ordenamiento español, pues en definitiva de eso se trata, y es labor de los que nos dedicamos a la investigación saber valorar los aciertos ajenos y proponer la introducción de los mismos en los ordenamientos que de forma más cercana nos afectan.

4. Opinión del autor

Reconociendo las bondades de la actual normativa que ha venido a completar el ordenamiento penal español en casi todos los aspectos en los que la regulación no respondía a los designios internacionales al respecto, a la hora de hacer un análisis crítico de la regulación española se plantean algunos problemas no resueltos. El más importante es el relativo a la determinación del bien jurídico protegido por los delitos informáticos. La doctrina más clásica y el legislador español afirman que el único bien jurídico —o los únicos bienes— que se protegen en estos delitos son bienes jurídicos tradicionales, en los que la única novedad es la aparición

[66] ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos", en *Revista Internacional de Política Criminal*, núms. 43 y 44, Naciones Unidas, 1994.

[67] DECRETO de 24 de junio de 2009 por el que se adicionan diversas disposiciones al Código Penal federal: http://www.diputados.gob.mx/LeyesBiblio/ref/cpf/CPF_ref100_24jun09.pdf.

de un sistema informático en algún momento del proceso delictivo. El hecho de realizarse tales ataques por medios informáticos, o contra elementos informáticos, no confiere una naturaleza diferente al bien jurídico protegido.

Por su parte, la doctrina más moderna —que es coincidente con la seguida por el legislador en México para la regulación de este fenómeno—, por el contrario, cree que esta interpretación no es adecuada, pues si bien es cierto que se protegen unos bienes individualizables y concretos, junto a ellos se propone la existencia de un nuevo bien jurídico colectivo merecedor de protección penal.

Es cierto también que en España no se han realizado estudios pormenorizados de la situación y existen escasas propuestas al respeto, pero parece fuera de toda duda que la realidad ha evolucionado de tal manera que cuando se ataca un sistema informático no sólo se está produciendo un daño concreto para un individuo concreto, sino que se está vulnerando "algo más", cuyo objeto no se ha sabido definir detalladamente todavía, pero que gira en torno a la idea de libertad informática y la seguridad en los sistemas informáticos, que deben ser considerados autónomamente como valores protegibles y protegidos de nuestro ordenamiento. Una sociedad interconectada, como la actual, debe tener un ordenamiento que sea consciente de la importancia de la herramienta que interconecta a la propia sociedad y la proteja directa y autónomamente.

Debemos, por tanto, confirmar lo acertado de la tendencia a incardinar la relevancia de la seguridad en los sistemas informáticos tanto en la libertad individual de los ciudadanos como en la protección de valores colectivos de la sociedad; y a este respecto conviene aplaudir la pionera legislación en México. La seguridad informática en un elemento de peso considerable en la configuración de una sociedad libre y segura. Y así debe ser considerada en los ordenamientos más avanzados.

5. Bibliografía

ADÁN DEL RÍO, C., "La persecución y sanción de los delitos informáticos", en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. 20, 2006.

ÁLVAREZ VIZCAYA, M., "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Internet y Derecho Penal. Consejo General del Poder Judicial*, núm. 10, 2001.

ANDRÉS DOMÍNGUEZ A.C., "Los daños informáticos en la Unión Europea", en *La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*, núm. 1, 1999.

AROCENA, G.A., "De los delitos informáticos", en *Revista de la Facultad de Derecho UNC*, vol. 5, núm. 1, 1997.

BACIGALUPO ZAPATER, E., *Derecho penal. Parte General*, 2ª ed., Hammurabi, 1999. BAJO FERNÁNDEZ, M., y BACIGALUPO SAGGESE, S., *Derecho penal económico*, 2ª ed., Editorial Universitaria Ramón Areces, Madrid, 2010.

BARRIO ANDRÉS, M., "La ciberdelincuencia en el Derecho español", en *Revista de las Cortes Generales*, núm. 83, 2011.

COTINO HUESO, L., *Libertad en Internet. La red y las libertades de expresión e información,* Tirant lo Blanch, Valencia, 2007.

DE ESTEBAN ALONSO, J., y GONZÁLEZ-TREVIJANO SÁNCHEZ, P., *Tratado de Derecho constitucional. II,* 2ª ed., Universidad Complutense de Madrid, Madrid, 2004.

DE LA MATA BARRANCO, N.J, y HERNÁNDEZ DÍAZ, L., "El delito de daños informáticos. Una tipificación defectuosa", en *Estudios Penales y Criminológicos*, núm. 29, 2009.

DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", en *REDUR*, núm. 8, diciembre de 2010.

FERNÁNDEZ FERNÁNDEZ, C., "Delitos informáticos", en *Base Informática*, núm. 43, 2009.

FERNÁNDEZ LÁZARO, F., "La Brigada de Investigación Tecnológica: la investigación policial", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial/Cuadernos de Derecho Judicial, Madrid, 2006.

GALÁN MUÑOZ, A., "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática", en *Revista de Derecho y Proceso Penal*, núm. 15, 2006.

GALLARDO RUEDA, A., "Delincuencia informática: la nueva criminalidad de fin de siglo", en *Cuadernos de Política Criminal,* núm. 65, 1998.

GARCÍA-PABLOS DE MOLINA, A., *Introducción al Derecho penal*, 4ª ed., Universitaria Ramón Areces, Madrid, 2006.

GUTIÉRREZ FRANCÉS, M.L., "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual", en *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja*, *REDUR*, núm. 3, 2005.

HEFENDEHL, R., *La teoría del bien jurídico. ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Marcial Pons, Madrid, 2007.

HERRÁN ORTIZ, A.I., *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Dykinson, 2002.

HUERTA TOCILDO, S., y ANDRÉS DOMÍNGUEZ, C., "Intimidad e informática", en *Revista de Derecho Penal*, núm. 6, 2002.

JAKOBS, G., *Derecho penal. Parte General. Fundamentos y teoría de la imputación*, 2ª ed. corregida, Marcial Pons, Madrid, 1997.

LÓPEZ, A., "La investigación policial en Internet: estructuras de cooperación internacional", en *Revista de Internet, Derecho y Política. Revista d'internet, dret i política*, núm. 5, 2007.

MATA Y MARTÍN, R.M., *Delincuencia informática y derecho penal,* Edisofer, Madrid, 2001.

____, "Criminalidad informática: una introducción al cibercrimen", en *Actualidad Penal*, núm. 36, 2003.

MATELLANES RODRÍGUEZ, N., "Algunas notas sobre las formas de delincuencia informática en el Código Penal", en DIEGO, DÍAZ-SANTOS M.R., y SÁNCHEZ LÓPEZ, V. (coords.), *Hacia un Derecho penal sin fronteras*, Colex, Madrid, 2000.

MAZA MARTÍN, J.M., "La necesaria reforma del Código Penal en materia de delincuencia informática", en *Estudios Jurídicos. Ministerio Fiscal*, núm. 2, 2003.

MIR PUIG, S., "Bien jurídico y bien jurídico-penal como límites del *ius puniendi*", en *Estudios Penales y Criminológicos*, núm. 14, 1991.

____, *Delincuencia informática*, PPU, Barcelona, 1992.

MUÑOZ CONDE, F., y GARCÍA ARÁN, M., *Derecho penal. Parte General,* 8ª ed., Tirant lo Blanch, Valencia, 2010.

MORILLAS CUEVA, L., "Nuevas tendencias del Derecho penal: Una reflexión dirigida a la ciber-criminalidad", en *Cuadernos de Política Criminal*, núm. 94, 2008.

NAVA GARCÉS, A.E., *Delitos informáticos*, 2ª ed., Porrúa, México, 2007.

PÉREZ LUÑO, A.E., "La protección de la intimidad frente a la informática en la Constitución española de 1978", en *Revista de Estudios Políticos*, núm. 9, 1979.

____, *Manual de informática y derecho,* Ariel, 1996.

QUINTANO RIPOLLÉS, A., *Tratado de la Parte especial de Derecho penal*, t. III, 2ª ed., Revista Derecho Privado, Madrid, 1978.

QUINTERO OLIVARES, G., *Parte General del Derecho penal,* 4ª ed., Thomson Reuters, Navarra, 2010.

REQUEJO NAVEROS, M.T., *El delito de revelación de secreto médico y la protección penal de la información genética,* Colex, Madrid, 2006.

REYNA ALFARO, L.M., "La criminalidad informática: cuestiones para una reflexión inicial", en *Actualidad Penal,* núm. 21, 2002.

RODRÍGUEZ MOURULLO, G., LASCURAIN SÁNCHEZ, J.A., y ALONSO GALLO, J., "Derecho penal e Internet", en FERNÁNDEZ ORDÓÑEZ, M.A., CREMADES GARCÍA, J., e ILLESCAS ORTIZ, R. (coords.), *Régimen Jurídico de Internet,* La Ley, Madrid, 2001.

RODRÍGUEZ RAMOS, L., "Protección penal de la propiedad industrial", en VV.AA., *Propiedad industrial. Teoría y práctica*, Centro de Estudios Ramón Areces, Madrid, 2001.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002.

ROXIN, C., *Derecho penal. Parte General,* t. I, Thomson Civitas, Navarra, 1997 (reimpresión de 2008).

SALOM CLOTET, J., "Delito informático y su investigación", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial/Cuadernos de Derecho Judicial, Madrid, 2006.

SÁNCHEZ MEDERO, G., "Internet: Un espacio para el cibercrimen y el ciberterrorismo", en *Crisis analógica, futuro digital. Actas del IV Congreso Online del Observatorio para la Cibersociedad, celebrado del 12 al 29 de noviembre de 2009*, Meddia, cultura i comunicació (edición electrónica sin numerar).

URBANO CASTRILLO, E., "Infracciones patrimoniales por medios informáticos y contra la infor-

mación, como bien económico", en VELASCO NÚÑEZ, E. (dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial/Cuadernos de Derecho Judicial, Madrid, 2006.

____, "Los delitos informáticos tras la reforma del CP de 2010", en *Delincuencia informática. Tiempos de cautela y amparo,* Thomson Reuters Aranzadi, Navarra, 2012.

WOHLERS, W., "Las jornadas desde la perspectiva de un escéptico del bien jurídico", en HEFENDEHL, R., *La teoría del bien jurídico. ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmáticos?*, Marcial Pons, Madrid, 2007.