MODELOS DE IMPUTACIÓN EN EL DERECHO PENAL INFORMÁTICO

Julio F. Mazuelos Coello

En las últimas décadas las tecnologías de la información y de la comunicación han tenido repercusión casi en todos los ámbitos sociales, modificando las condiciones de vida y de trabajo de la mayoría de las personas; ello se ha posibilitado debido al procesamiento electrónico de datos, al almacenamiento y procesamiento de grandes cantidades de información, que especialmente son de considerable utilidad para la ciencia, la economía y la administración. Este cambio no sólo se presenta en tales ámbitos, también en el mantenimiento de muchos hogares se han convertido las computadoras en un elemento permanente. Junto a ello la interconexión universal de computadoras a través de internet posibilita que cualquiera desde cualquier lugar, con poco esfuerzo, pueda transmitir y pedir informaciones, además de hacer posible la comunicación universal mediante el empleo del e-mail.

En general, todas estas posibilidades de transmisión de información inciden en diversos ámbitos que, a su vez, promueven y favorecen nuevos ámbitos de desarrollo de las actividades, como sucede en el campo de la economía a través del e-commerce o el e-business y el electronic-banking, o en el ámbito privado a través de la diversidad de ofertas de información o entretenimiento, junto a la posibilidad de realizar transacciones comerciales y bancarias vía internet; mientras que en el ámbito de la educación escolar y universitaria resultan hoy en día inimaginables las posibilidades que se pueden desarrollar no sólo como fuente de información sino, además, como medio para el dictado de clases y seminarios on line.

Estas son sólo algunas de las características de la sociedad de la información, caracterizada como sociedad post-industrial[1], pues mientras en la sociedad industrial la producción de bienes con ayuda de la máquina se encuentra en primer plano, la sociedad post-industrial se caracteriza porque el conocimiento y la información juegan un rol decisivo, al punto de desarrollar una "tecnología intelectual" que tiene como consecuencia una profunda transformación dentro de la estructura social[2].

Ahora bien, el procesamiento de información y la información en sí no están libres de abusos que generan perturbaciones, daños, etc., y que, además, producen grandes afectaciones a los sistemas y enormes pérdidas financieras. El legislador, en la lucha contra este abuso, se encuentra frente al problema de que el Derecho evoluciona, en principio, al contrario de las nuevas tecnologías. En efecto, la velocidad de los grandes cambios vinculados al proceso dinámico de nuestra sociedad hacia una sociedad de la información presenta para la legislación dificultades para poder comprender dicha transformación permanente y las posibilidades de abuso ligadas a ella, sin que exista una situación de inseguridad y falta de claridad jurídicas[3].

El presente trabajo persigue realizar una contribución a la fijación de un derrotero a seguir en el desarrollo de la configuración de una dogmática jurídico-penal de los delitos informáticos, que tome como punto de partida una perspectiva normativa en la construcción de los respectivos tipos penales. Nos ocupamos, en primer lugar, de una breve exploración de la presencia de la criminalidad con contenido informático y de la respuesta legal de que ha sido objeto, lo cual nos permite comprender la volubilidad del fenómeno informático y la lentitud con que es aprehendido por el Derecho penal; seguidamente, revisamos las principales concepciones del delito informático con la finalidad de precisar cuál es la conducta en sí que se pretende imputar; en tercer lugar, procedemos a una revisión crítica de los principales modelos de imputación empleados por el legislador penal para tipificar los delitos informáticos, y, en último lugar, sugerimos una construcción de la estructura de los delitos informáticos a partir de un criterio de imputación en virtud de competencia, como el propuesto por la moderna concepción del funcionalismo normativista de la Escuela de Jakobs.

---

1 Concepto aportado por Bell, The Coming of Post-Industrial Society. A Venture in Social Forecasting, 1973.

2 Sobre ello véase Krutisch, *Strafbarkeit des unberechtigten Zugangs zu Computerdaten uns-systemen*, Frankfurt a. M., 2004, p. 21.

3 Cfr. Krutisch, *Strafbarkeit*, cit., p. 23; en el mismo sentido, Mayer-Schönberger, *Information und Recht-Vom Datenschutz bis zum Urheberrecht*, Wien-New York, 2001, p 7.

I. Breve reseña del desarrollo de la criminalidad informática y de la reacción a través de medidas legislativas

Los peligros generados a través del abuso de las nuevas tecnologías han originado diversas reacciones en diferentes ámbitos por parte del legislador[4]. Así, en los años 60 los peligros originados por las nuevas tecnologías principalmente fueron vistos como posibles peligros a los derechos de la personalidad, situación que condujo en diferentes países a que en los años 70 las leyes se orientaran a la protección de los datos personales. Luego, en la década de los 70 se desplazó el centro de la discusión a los delitos económicos con contenido informático, los cuales hasta la actualidad despliegan una amenaza constante, sin que se conozcan con precisión cifras estadísticas acerca de las afectaciones producidas con esta forma de criminalidad, pues apenas algunos casos han sido conocidos[5].

Esta situación varió considerablemente en la década de los 80 con la evidencia pública de casos espectaculares de espionaje informático, hacking, difusión de virus y piratería de software[6], los cuales hicieron que a partir de ese momento se reconociera ampliamente que existe una amenaza para nuestra sociedad de la información mediante la criminalidad informática. Ya a mediados de los años 80 comenzó en varios países la discusión sobre los problemas procesal-penales presentados en relación con la comisión de delitos y el creciente ingreso de las tecnologías de la información y la comunicación, lo cual originó a su vez reformas procesal-penales[7].

A finales de los años 90 los temas de discusión acerca de la criminalidad informática giraron en torno a la problemática de la difusión de contenidos antijurídicos en internet: racistas, pornográficos, de apología de la violencia, etc., generándose la discusión, todavía pendiente de solución, acerca de si este tipo de delitos también deben ser considerados dentro del concepto de delitos informáticos[8].

En la década del 2000 y en adelante, la temática sobre el abuso de las nuevas tecnologías informáticas se orienta hacia el empleo de medidas de seguridad sobre el campo técnico: sistemas de criptografía, firma digital, seguridad IT, así como hacia la normativización de mandatos y prohibiciones en este ámbito.

---

4 Una revisión práctica de este tema puede encontrarse en KRUTISCH, *Strafbarkeit*, cit., pp. 27 y ss. Sobre el desarrollo de la criminalidad informática véase SIEBER, Computerkriminalität und andere Delikte im Bereich der Informationstechnik, *zstw* 104, 1992, pp. 251 y ss.

5 Cfr. JESSEN, *Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB*, Frankfurt a. M., 1994, p. 18.

6 Véase SIEBER, Computerkriminalität und Informationsstrafrecht, *CR*, 1995, pp. 100 y s., p. 101.

7 Cfr. SIEBER, Computerkriminalität, cit., pp. 109 y s.

8 Se deja de considerar a la computadora como un mero archivador y procesador electrónico de datos para pasar a ser la vía de acceso a la red universal de computadoras, con la consiguiente difusión de contenidos ilegales. Cfr. KRUTISCH, *Strafbarkeit*, cit., p. 35.

II. El concepto de "delito informático"

El concepto de "delito informático" está vinculado a la idea de "*computer crime*" en la literatura norteamericana y a su traducción alemana "*Computerkriminalität*", con la salvedad de no acarrear las críticas que reciben estos conceptos: la computadora en sí no podría ser criminal, más bien es empleada por los usuarios en algunos casos con fines criminales y, por otro lado, esta denominación dejaría sin comprender el procesamiento de datos en sí como objeto de posibles ataques.

La denominación de delito informático es poco usada en las legislaciones penales; no obstante bajo ella se describe, en líneas generales, una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática; esta denominación sirve a su vez como "tópico" para el tratamiento del tema en diversos ámbitos[9]; así, por ejemplo: en los medios de comunicación se emplea para informar sobre los peligros para la sociedad de la información mediante el uso abusivo y socialmente perjudicial de nuevas tecnologías de la información y la comunicación; desde un punto de vista político-jurídico permite englobar las discusiones referidas a una equiparación internacional del Derecho o a la verificación de la suficiencia de las normas actualmente existentes para comprender este problema; en el campo de la criminología dicha denominación sirve para incluir en las estadísticas un ámbito determinado de la criminalidad, como también para verificar la concurrencia de una cifra oscura de la criminalidad, o bien para poder agrupar a un determinado sector de autores; en el ámbito jurídico-penal no se presentan mayores consecuencias jurídicas derivadas directamente de esta denominación, sin embargo en la doctrina permite agrupar determinados tipos penales como fraude informático, alteración de datos o sabotaje informático.

Ahora bien, en la actualidad, dado el desarrollo que ha tenido esta forma delictiva se vienen acogiendo nuevas denominaciones para abarcar esta problemática delictiva: "abuso de computadoras", "delitos bajo la influencia de la computadora"[10], "criminalidad de la información y la comunicación"[11], "criminalidad de internet"[12] o "criminalidad multimedia"[13]. Sin embargo, estas denominaciones son insuficientes por sí mismas para describir y delimitar con claridad el fenómeno de la delincuencia informática, y aunque la denominación "delito informático" no tiene mayor incidencia en el ámbito jurídico-penal a efectos de la tipicidad de las conductas ni de las consecuencias jurídi-

---

9 Sobre ello véase, Krutisch, *Strafbarkeit*, cit., pp. 30 y s.

10 Cfr. Steinke, Die Kriminalität durch Beeinflussung von Rechnerabläufen, *NJW*, 1975, pp. 1867 y ss.

11 Así, a efectos del ámbito policial alemán, cfr. Dammann, Computerkriminalität aus Sicht von Ermittlungsbehörden, [http://www.cert.dfn.de/dfn/berichte/db087/lka52.html].

12 Véase Vetter, *Gesetzeslücken bei der Internetkriminalität*, Hamburg, 2003.

13 Por ejemplo, como un fenómeno posterior a la criminalidad informática, Vassilaki. "Multimediale Kriminalität – Entstehung, Formen und rechtspolitische Fragen der 'Post-Computerkriminalität'", *CR*, 1997, pp. 297 y ss. También Barton, *Multimedia – Strafrecht. Ein Handbuch für die Praxis*, Neuwied, 1999.

cas, sigue siendo una denominación que identifica de manera general la problemática de la delincuencia mediante computadoras y mediante el empleo de redes de comunicación que incide tanto en los sistemas en sí como en la información como un valor autónomo; debido a ello sigue siendo conveniente mantener, a efectos didácticos, en la doctrina y frente a los usuarios la denominación "delito informático" para identificar esta forma de criminalidad vinculada a un área específica de la tecnología.

En líneas generales, desde el valioso aporte de SIEBER[14] en 1977 para la dogmática de los delitos informáticos, se viene distinguiendo entre la alteración de datos, la destrucción de datos, la obtención indebida de datos y la agresión al hardware.

Con posterioridad al aporte de SIEBER, se han propuesto en la doctrina diferentes conceptos de delito informático. Para MÜHLEN[15] este concepto ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho[16]. Por su parte, DANNECKER[17] concibe el delito informático como aquellas formas de criminalidad que se encuentran directa o indirectamente en relación con el procesamiento electrónico de datos y se cometen con la presencia de un equipo de procesamiento electrónico de datos. Ambas posiciones resultarían muy amplias, de tal modo que las conductas pueden quedar subsumidas en los clásicos tipos penales; lo único que los diferenciaría es que la computadora sirve como medio de realización del hecho y, en otros casos, que se encuentran en una relación directa o indirecta con el procesamiento electrónico de datos[18].

Otro sector de la doctrina renuncia a una definición del concepto de delito informático, y a cambio de ello intenta comprender sistemáticamente las correspondientes formas de manifestación del fenómeno, por lo que recomienda diferentes clasificaciones; así, por ejemplo, se sugiere llevar a cabo una clasificación según el bien jurídico afectado y diferenciar en el ámbito de los delitos informáticos entre delitos patrimoniales, lesiones de los derechos de la personalidad y lesiones de bienes jurídicos supra-indi-

---

14 Véase SIEBER, *Computerkriminalität und Strafrecht*, München, 1977, pp. 39 y ss.

15 Cfr. MÜHLEN, *Computer-Kriminalität: Gefahren und Abwehrmaßnahmen*, Neuwied / Berlin, 1973, p. 17.

16 Una visión restrictiva de esta posición sería la formulada por MATA, quien vincula los llamados delitos informáticos únicamente a aquellos supuestos en los que la computadora constituye el medio de ejecución del hecho. Cfr. MATA, *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001, p. 22, siguiendo a MILLITELLO, *Nuove esigenze di tutela penale e trattamento elettronico della informazione, Verso un nuovo Codice penale*, Giuffrè, Milano, 1993, p. 476.

17 Cfr. DANNECKER, Neuere Entwicklungen im Bereich der Computerkriminalität – Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, *BB*, 1996, pp. 1285 y ss. Esta parece ser también la opinión de GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, p. 50.

18 Críticamente KRUTISCH, *Strafbarkeit*, cit., p. 33.

viduales[19]; otro sector de la doctrina aboga por una clasificación según las formas de agresión fenomenológicamente observadas, esto es, una clasificación en manipulación informática, espionaje informático y sabotaje informático[20].

Nótese que todas estas construcciones, en mayor o menor medida, se erigen sobre la base de una perspectiva naturalística, en la que la pertenencia del hecho a una computadora o su alejamiento sigue siendo el punto decisivo en la cuestión.

Más allá de estas concepciones del delito informático vinculadas a la computadora en sí, una perspectiva que toma en cuenta la propia red es la propuesta por JOFER[21]; en su opinión es posible identificar tres categorías: a) Delitos de difusión específica en la red (*netzspezifische Verbreitungsdelikte*), en los cuales internet funge como instrumento del hecho; b) Delitos en los que internet constituye el medio para comunicar el hecho (*Delikt als Mittel zur Tatkommunikation*), es decir, ésta no representa el lugar en el que se realiza el hecho punible ni el instrumento para su realización, únicamente sirve de medio de comunicación, como el correo postal o el teléfono, y c) Delitos en los que internet constituye el virtual instrumento del hecho con cuya ayuda pueden realizarse hechos punibles en la realidad.

Esta clasificación presenta la ventaja de hacer una referencia directa al procesamiento de datos como característica principal de la categoría de delito informático en sentido estricto, ya sea en la forma en que es aprovechada la red para la realización del hecho punible, quedando ésta comprendida parcialmente en algunos casos dentro del objeto de la acción, o bien dejándola absolutamente fuera de la realización del hecho. Lo que no hace sino poner en evidencia que internet es aquí abarcada sólo parcialmente en cuanto instrumento del hecho, sin tomarse en cuenta sus particularidades específicas.

De ahí que ante las amplísimas concepciones del delito informático se ha de encontrar un referente funcional que permita identificar y luego delimitar qué comportamientos ingresan en la categoría del delito informático y cuáles, a pesar de su vinculación fenomenológica con una computadora, un procesador de datos o la red de información, no es posible considerarlos en dicho rubro. En ello, debido a que en la actualidad la computadora está presente en todos los ámbitos de la vida diaria, se ha de tener en cuenta que muchos de los clásicos delitos pueden ser realizados con ayuda de una computadora, pero no por eso van a comprenderse como delitos informáticos.

---

19 Así, por ejemplo, la propuesta de JESSEN, *Zugangsberechtigung*, cit., pp. 15 y ss.

20 Así HILGENDORF, Grundfälle zum Computerstrafrecht, *JuS*, 1996, pp. 509 y ss., p. 510; MÖHRENSCHLAGER, Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, *Wistra*, 1991, pp. 321 y ss., p. 322; TIEDEMANN, Computerkriminalität und Missbrauch von Bankomaten, *WM*, 1983, pp. 1326 y ss., pp. 1327 y ss.

21 Cfr. JOFER, *Strafverfolgung im Internet. Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen*, Peter Lang, Frankfurt a. M., 1999, pp. 35 y ss.

En este orden de ideas, se requiere que el comportamiento delictivo, comparativamente, no sea realizable sin la intervención de la informática, luego existirá un delito informático en sentido estricto si el autor aprovecha precisamente las posibilidades técnicas del procesamiento electrónico de datos para sus fines[22]; esto es, el aspecto informático tiñe la realización misma de la conducta (se requiere del conocimiento de la tecnología informática para su perpetración, investigación y prosecución, de tal forma que el medio informático caracterice a la conducta)[23]. Luego, se ha de separar los comportamientos criminales que se encuentran sólo en una relación externa con el empleo de la tecnología informática y no están impresos de las peculiaridades del procesamiento electrónico de datos[24].

Así, es posible identificar tres categorías de delitos informáticos[25]: manipulación informática, sabotaje informático y acceso no autorizado a datos o sistemas computarizados.

La manipulación informática se caracteriza porque el autor que generalmente es empleado de las empresas afectadas tiene influencia sobre el procesamiento de datos para modificar sus resultados y obtener una ventaja personal; el sabotaje informático se presenta en aquellos casos en que un sistema informático es dañado mediante agresiones sobre el hardware o sobre el software; a este ámbito pertenecen los programas de virus que son extendidos a través de una copia ilegal de un software o de una red de computadoras como un *attachment* de un e-mail. Por su parte, el acceso no autorizado a un sistema de datos o sistema informático representa aquellos casos en los que el autor, sin estar autorizado, consigue el acceso a un sistema de datos o un sistema informático. Esta última categoría no presentaría una estricta diferenciación con los supuestos de manipulación informática o de sabotaje informático[26], toda vez que el acceso no autorizado a los sistemas informáticos constituye el nivel previo para una conducta posterior de manipulación o sabotaje informático.

Más allá del abuso de los equipos automatizados de procesamiento de datos puede identificarse, sin lugar a dudas, el aprovechamiento delictivo de las redes de información, lo cual puede reconducirse al concepto de criminalidad de internet, que se erige como una categoría autónoma para agrupar a aquellas conductas antijurídicas en relación con el abuso de las nuevas técnicas de comunicación y medios que se cometen en

---

22 En este sentido, KRUTISCH, *Strafbarkeit*, cit., p. 35.

23 Así, MAZUELOS, Delitos informáticos: una aproximación a la regulación del Código Penal peruano, *RPDJP*, n.º 2, 2001, pp. 253 y ss., p. 271.

24 Cfr. FREY, *Computerkriminalität in eigentums- und vermögensstrafrechtlicher Sicht*, München/Florenz, 1987, p. 8.

25 Así, KRUTISCH, *Strafbarkeit*, cit., pp. 51 y ss.

26 Cfr. KRUTISCH, *Strafbarkeit*, cit., p. 54.

gran parte por un autor socialmente desapercibido y cuyo comportamiento transcurre completamente en el anonimato[27].

De tal forma que junto a la descripción tradicional de los delitos informáticos surge una nueva concepción a tomar en cuenta: los delitos de información en internet[28], que posibilitan abarcar nuevas conductas delictivas bajo una diferente agrupación: a) ataques a los bienes jurídicos de vendedores y usuarios de los servicios de internet: ataques a los datos durante su transporte en internet, ataques a los datos archivados en internet, difusión de programas dañinos en internet; b) lesión de los derechos de terceros: delitos de expresión (p.ej., difusión de pornografía), lesión de la propiedad intelectual.

En definitiva, la categoría de delito informático ha de ser reconducida a aquellos comportamientos cuya realización sólo sea posible a través del empleo de los elementos de la informática: el procesamiento y almacenamiento de datos. Por su parte, se ha de admitir la presencia de nuevas conductas provenientes de las actividades desplegadas en internet cuyo centro gravitacional gira en torno a la información como valor en sí misma, luego es posible concebir los denominados delitos de información en internet. Se trata de variar la noción naturalista de la construcción de los delitos informáticos por una noción normativa, que ponga el centro de la cuestión no en el ámbito corporal del bien en sí (computadora), sino exclusivamente en su funcionalidad.

Ambos grupos deberían ser recogidos como punto de partida para un modelo de imputación de este tipo de delitos.

III. DESCRIPCIÓN DE LOS MODELOS ACTUALES DE IMPUTACIÓN EN EL ÁMBITO PENAL INFORMÁTICO

A. El recurso a los delitos de peligro: delitos de peligro abstracto (delitos de mera peligrosidad)

La principal característica del delito de peligro abstracto es que no se haya puesto efectivamente en peligro o lesionado un bien valorado positivamente. La idea de peligro ha de ser concebida normativamente, esto es, sobre la base de un juicio normativo respecto de las posibilidades de existencia de un bien. Se trata de verificar las condiciones para la disposición de un bien libre de perturbaciones, luego el delito de peligro abstracto representa precisamente la afectación de estas condiciones de disposición[29].

---

27 Cfr. VASSILAKI, Multimediale Kriminalität, cit., p. 300.

28 Véase, PREUSSE, *Informationsdelikte im Internet*, Hamburg, 2001, passim.

29 Cfr. KINDHÄUSER, Rationaler Rechtsgüterschutz durch Verletzungs-und Gefährdungsverbote, en LÜDERSSEN (ed.), *Aufgeklärte Kriminalpolitik oder Kampf gegen das Böse?*, I, Baden-Baden, 1998, pp. 269 y ss., p. 276.

En la doctrina se ha desarrollado en el ámbito de la criminalidad informática bajo la noción de los delitos de peligro abstracto, marcadamente los delitos de difusión de documentos pornográficos (§ 184 III StGB), como también el delito de agitación xenófoba (§130 StGB)[30].

Sin embargo, es posible desarrollar con mayor amplitud distintos tipos penales en materia informática que respondan a la estructura de los delitos de peligro abstracto, a partir de la perturbación de las condiciones de disposición de los sistemas o programas informáticos, como el caso del acceso indebido al correo electrónico de otro.

En los delitos de peligro abstracto para fundamentar la imputación objetiva es suficiente la imputación del comportamiento.

B. Los delitos de acumulación

El desarrollo de los delitos de acumulación en materia penal informática, si bien no ha sido aún mayormente aceptado por las diversas legislaciones, constituye una de las formas de imputación con elevada fuerza preventiva.

La característica central de estos delitos radica en el hecho de que no es posible determinar en algunas conductas si se trata de delitos de peligro o de delitos de resultado, el perjuicio ocasionado sólo es posible que sea apreciado de forma cumulativa[31]. En estos delitos basta la imputación objetiva del comportamiento.

En el ámbito penal informático se evidencia la introducción de esta estructura típica en la tendencia de castigar como delito autónomo el mero ingreso indebido a una base de datos, sistema o red de computadoras, sin que se acredite la producción de un peligro o una lesión. Así, el artículo 207-A del Código Penal peruano que sanciona dicha conducta en su parte objetiva, exigiendo sólo que el autor persiga fines de copiar o alterar la información, sin que esto llegue efectivamente a ocurrir.

C. Los delitos de emprendimiento

Los delitos de emprendimiento se caracterizan por ser tipos penales en los que se equipara la tentativa con la consumación[32], en tal sentido es suficiente para la imputación objetiva la imputación del comportamiento.

---

30 En este sentido, Lehle, *Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet*, Konstanz, 1999, p. 26.

31 Propuesta inicialmente para los delitos medioambientales: véase Kuhlen, Der Handlungserfolg der strafbaren Gewässerverunreinigung (§ 324 StGB), *GA*, 1986, pp. 389 y ss.

32 Cfr. Berz, Formelle Tatbestandsverwirklichung und materialer Rechtsgüterschutz, Berlin, 1986, pp. 125 y ss.

En materia informática ésta ha sido la estructura seguida mayormente por el legislador peruano para la configuración de los tipos penales informáticos: así, el artículo 207-B del Código Penal sanciona con pena de hasta dos años de privación de libertad a quien ingresa indebidamente a una base de datos con la finalidad de alterarlos, siendo suficiente el ingreso ilícito para agotar el tipo penal en su aspecto objetivo. Esto es, se agota el delito de sabotaje informático con la conducta de ingresar indebidamente, sin que se exija la producción del daño (material).

D. Los delitos de mera actividad

Frente a la categoría de los delitos de resultado se ubican los delitos de mera actividad, en los que el tipo de injusto se realiza mediante la intervención descrita en el tipo penal como tal. En la problemática de los delitos informáticos la conducta de acceso no autorizado a una base de datos ajena constituye una conducta de mera actividad, ya que es suficiente el solo acceso indebido, sin que se requiera una consecuencia adicional.

E. La solución de los delitos de resultado

Dentro de la dogmática penal actual es en determinados ámbitos de delitos en los que el concepto de resultado tiene algún papel trascendente[33]; en especial sirve como criterio para la determinación del momento de la culminación del hecho punible y del inicio del cómputo de la prescripción, además de jugar un rol importante en relación con la causalidad y el desistimiento de la tentativa.

La doctrina tradicional defiende un concepto de resultado basado en un sustento eminentemente naturalístico, anclado en la afectación de un bien o en la transformación del mundo exterior.

Importante para el análisis de la solución a través de la concepción de los delitos de resultado es la diferencia entre resultado en sentido estricto y resultado en sentido amplio[34]. Este último se refiere, en principio, a todo delito consumado, por lo que el resultado está en la realización del tipo, esto es, se equipara con la propia conducta del autor. El resultado en sentido estricto, por el contrario, va más allá de la mera conducta; aquí es necesario un efecto separable de la conducta[35].

Nos ocuparemos acá de la incidencia de los delitos de resultado en sentido estricto en el ámbito de la imputación objetiva de los delitos informáticos, es decir, en aquellos

---

33 Cfr. Lehle, *Der Erfolgsbegriff*, cit., p. 56.

34 Sobre ello, con mayores referencias, Lehle, *Der Erfolgsbegriff*, cit., p. 56.

35 Importante para la imputación penal en los delitos informáticos es tomar partido por una u otra concepción del resultado; según el camino que se siga se requerirá o no en estos delitos la necesidad de contar con un efecto separable de la acción para poder afirmar la consumación del delito.

casos en que, además de la conducta, se requiere un perjuicio efectivo en el objeto de ataque de la acción (delitos de lesión).

Respecto de los delitos de resultado en sentido estricto, la doctrina es marcadamente unánime en considerar en esta categoría tanto a los delitos de lesión como a los delitos de peligro concreto; en ellos se muestra la producción de la lesión del bien jurídico y la producción del peligro concreto, respectivamente. Por su parte, los delitos de peligro abstracto y los delitos de peligro potencial, a este respecto equiparables, no son en ningún caso un delito de resultado[36], luego, debido a que en los delitos de peligro abstracto no es exigible una lesión al bien jurídico ni la producción de un peligro concreto, en consecuencia es posible concluir que estos delitos no pueden tener ningún resultado.

De esta forma algunos delitos informáticos, como el sabotaje o daños, se estructuran en la construcción de los delitos de resultados, exigiéndose un menoscabo material ya sea en el sistema o programa informático, o también a través de la creación de un peligro concreto, como en el caso del espionaje informático; mientras otros delitos, como el intrusismo, exigen únicamente la realización de la conducta descrita en la norma penal.

La diferenciación entre delitos de resultado (lesión o puesta en peligro concreto) y delitos de mera actividad resultaría frágil, pues de una parte los delitos de mera actividad tendrían también un resultado en sentido amplio: la realización de la conducta, y, de otra parte, como ha destacado Roxin[37], no todo delito puede ordenarse fácilmente como delito de resultado o de mera actividad, en todo caso es posible constatar que dicha diferenciación carece de sentido cuando se trata del concepto de resultado en sentido estricto.

En la problemática de los delitos informáticos la conducta de acceso no autorizado a una base de datos ajena es por lo general previa a la manipulación o al sabotaje informático, de ahí que la barrera entre mera actividad o resultado resulta ser mínima.

Con la finalidad de lograr una marcada distinción, más allá de la conducta realizada por el autor, entre los delitos de resultado y los delitos de mera actividad a partir de un concepto de resultado en sentido estricto, la doctrina considera que la distinción ha de apoyarse sobre algo distinto a la conducta en sí. Se trata del "objeto de la acción", esto es, el objeto frente al cual se emprende la conducta típica[38].

---

36 Cfr. Tröndle/Fischer, *Strafgesetzbuch und Nebengesetze*, 52.ª ed., München, 2004, vor §13, n.m. 13a.

37 Cfr. Roxin, *Strafrecht, Allgemeiner Teil, Grundlagen der Aufbau der Verbrechenslehre*, Band I, 3.ª ed., München, 1997, § 10, n.m. 104.

38 Cfr. Martin, *Strafbarkeit grenzüberschreitender Umweltbeeinträchtigung. Zugleich ein Beitrag zur Gefährdungsdogmatik und zum Umweltvölkerrecht*, Freiburg, 1989, p. 23.

Sobre esto pueden observarse hasta tres posiciones en el desarrollo de la doctrina: SCHÜTZE[39] diferencia entre el patrimonio como instituto y la cosa aislada que pertenece a una persona como patrimonio, luego el objeto de la acción es caracterizado por dicha cosa en concreto. Para VON. LISZT[40] el resultado del delito radica en la transformación causada mediante la acción en el mundo exterior, esto es, algo tangible, a saber, un objeto, una persona o una cosa sobre la que se produce la transformación y, con ello, el resultado. Esto es caracterizado por VON. LISZT como el objeto de la acción delictiva. La tercera posición[41] es defendida por BELING, MAYER y MEZGER; en su opinión, el concepto de objeto del hecho representa el objeto sobre el cual se ejecuta la acción típica[42]; en este sentido, el bien jurídico es comprendido como el objeto determinado mediante la interpretación sobre los efectos de protección de una norma penal, que en algunos casos podrá identificarse con el objeto de la acción.

Esta tercera posición es actualmente la más extendida en la doctrina, y según ella el objeto del hecho es aquel objeto frente al cual se emprende la conducta típica[43]. A partir de esta posición aparecen las más diferenciables variantes y las más diferentes caracterizaciones.

Entre ellas destaca, aunque aún con pocos seguidores, la propuesta de JAKOBS[44], para quien sólo es idóneo como objeto del hecho los objetos corporales, esto es, el resultado se comprende como todo efecto que obra en un objeto corporal recogido en el tipo penal. Sin embargo, para la doctrina este planteamiento trae consigo dos consecuencias importantes: presenta una considerable restricción del número de los delitos de resultado[45] y, de otra parte, origina una mezcla de los conceptos de acción y de resultado; luego, en la medida en que resulta apropiada para la afirmación del concepto de resultado la relación del autor con cualquier objeto mencionado en el tipo penal, se vería amenazada además la delimitación de los contornos del correspondiente bien jurídico[46].

Definitivamente, en materia informática el objeto jurídico de protección penal ha de estar desvinculado de una noción material, física o natural, pues lo trascendente es la

---

39 Cfr. SCHÜTZE, *Die notwendige Teilnahme am Verbreche*, Leipzig, 1869, p. 64.

40 Cfr. VON LISZT, Der Begriff des Rechtsgutes im Strafrecht und in der Enzyklopädie der Rechtswissenschaft, *ZStW* 8, 1888, pp. 131 y ss., p. 150.

41 Véase, BELING, *Die Lehre vom Verbrechen*, Tübingen, 1906, pp. 203 y s.; MAYER, *Der Allgemeiner Teil des Deutsches Strafrechts-Lehrbuch*, Heidelberg, 1923, pp. 97 y s.; MEZGER, *Strafrecht Ein Lehrbuch*, 3.ª ed., Berlin, 1949, p. 188.

42 En este sentido, MEZGER, *Strafrecht*, cit., p. 188.

43 Véase con mayores referencias bibliográficas, MARTIN, *Strafbarkeit*, cit., p. 24.

44 Cfr. JAKOBS, *Strafrecht, Allgemeiner Teil, Die Grundlagen und die Zurechnungslehre,* 2.ª ed., Berlin – New York, 1991, § 29, n.m. 2.

45 En este sentido, MARTIN, *Strafbarkeit*, cit., p. 25.

46 Crítico frente a esta postura, LEHLE, *Der Erfolgsbegriff*, cit., p. 60.

funcionalidad del sistema informático en sí mismo como un valor independiente del soporte físico en el que se encuentre. Luego, la idea de resultado ha de comprender tanto un perjuicio efectivo en el objeto de ataque de la acción como también la producción de una situación de peligro para determinado objeto de ataque existente en la realidad; para el primer caso será necesaria la imputación del resultado al comportamiento realizado, en el segundo caso deberá establecerse una relación de imputación entre la peligrosidad de la conducta y el resultado de peligro concreto[47].

Desde esta perspectiva, el delito de sabotaje informático exigirá la producción de un resultado de lesión: destrucción del programa informático; el delito de espionaje exigirá la producción de un peligro concreto sobre la información reservada.

F. Los elementos subjetivos de intención trascendente: subjetivización de la imputación jurídico-penal

Hasta el momento todos los modelos de imputación mencionados se erigen sobre la base de una construcción objetiva, esto es, giran en torno a la imputación objetiva del comportamiento o del resultado. Sin embargo, algunas construcciones legislativas han puesto el acento en el aspecto subjetivo del comportamiento, en concreto, en la finalidad perseguida por el autor del hecho, variando la sanción según el objetivo perseguido en la realización de una conducta objetiva común.

Este es el caso de la estructura de los delitos informáticos en el Código Penal peruano, en la que a partir de la realización común del ingreso o utilización indebida de una base de datos, red de computadoras o programas, el autor persigue finalidades distintas: alterar, copiar, interferir, destruir, obtener un provecho económico, etc., luego se observan distintas modalidades de delitos informáticos de acuerdo con el fin perseguido. Se trata del recurso a los elementos subjetivos de intención trascendente, en los que la subjetividad va más allá de la realización objetiva exigida[48]. Debido a ello no alcanza el nivel del dolo, ya que éste representaría voluntad realizada.

Dentro de la problemática de los elementos subjetivos de intención trascendente es posible distinguir dos grupos:

– *Delitos de resultado cortado*, en los que el legislador prescinde del resultado: basta que se lleve a cabo la conducta, sin que sea necesario que se produzca un resultado externo, separable materialmente de la acción; así el caso del delito de fraude informático del artículo 207-A, segundo párrafo, del C.P. peruano que sanciona el ingreso indebido a una base de datos con el fin de obtener un provecho económico, o el sabotaje informático en el que se prevé el fin de dañarlo en el artículo 207-B del C.P. peruano.

---

47 Así, García Cavero, *Derecho penal económico. Parte general*, Lima, 2003, p. 469.

48 Cfr. Bustos Ramírez, *Manual de Derecho penal. Parte general*, 3.ª ed., Barcelona, 1989, p. 186.

En todos estos casos respecto del resultado sólo se requiere un elemento subjetivo del tipo, pero no que se realice efectivamente.

– *Delitos mutilados de dos actos*: en estos casos el legislador recoge dos comportamientos en el tipo penal, pero sólo exige que se realice uno de ellos y prescinde del otro acto, del que sólo exige su aspecto subjetivo. Así, el delito de copia ilegal de archivo informático (art. 207-A C.P. peruano) en el que se recoge, como primer comportamiento, el ingreso indebido a un sistema informático y, como segundo comportamiento, que sea "para" copiar información contenida en el sistema, luego no es necesario que se dé el lado objetivo de esta segunda conducta, basta únicamente su aspecto subjetivo (para copiar información).

Esta perspectiva adoptada en el ámbito penal informático toma muy en cuenta que el acceso no autorizado a datos y sistemas computarizados es un aspecto parcial de la criminalidad informática de elevada relevancia, ya que por lo general constituye el estadio previo de posteriores conductas criminales[49]. Pero ello no debe conducir a sobredimensionar el aspecto subjetivo de las conductas típicas, menos aún a poner el acento en la voluntad perseguida por el autor al momento de la realización del hecho, lo cual es prácticamente de imposible determinación.

Esta estructura de imputación no resiste la pregunta de cómo distinguir entre un acceso indebido a una base de datos con la finalidad de copiar un archivo y un acceso indebido a una base de datos con la finalidad de destruir un archivo: todo queda en manos o, mejor dicho, en la cabeza del autor, generándose un elevado clima de inseguridad jurídica.

Para solventar esta critica podría afirmarse que esta conducta con ambas finalidades se encuentra sancionada con la misma pena, por lo que una elevada precisión acerca de lo que realmente persigue el autor no sería necesaria. Sin embargo, la igualdad de punibilidad de ambas conductas no es razón suficiente para obviar la determinación del aspecto subjetivo del hecho en una perspectiva normativa y no eminentemente psicológica, ni para tener que adivinar cuál era la real voluntad del autor del hecho.

IV. LA IMPUTACIÓN PENAL EN VIRTUD DE COMPETENCIAS

El punto de partida en este apartado es la comprensión de que los contactos sociales deben contar fundamentalmente con expectativas normativas, pues ellas configuran las pautas de comportamiento de las personas en determinadas situaciones y las que los demás deben esperar de las personas. En tal sentido, el Derecho penal tiene por misión determinar las pautas normativas de orientación de las conductas de los miembros de la sociedad, a efectos de eliminar las interpretaciones individuales que pueden

49 En este sentido, KRUTISCH, *Strafbarkeit*, cit., p. 24.

ser de lo más variado y verse enmarcadas dentro de una desorientación cognitiva en la sociedad[50].

En este orden de ideas, es posible distinguir entre delitos de dominio o de organización que contienen un deber común dirigido a la generalidad (ciudadanos) de obrar conforme a Derecho, que conllevan el desarrollo de una prestación negativa: evitar lesionar a los demás; y delitos de infracción de un deber que están referidos al ejercicio de un rol especial y conllevan el desarrollo de una prestación positiva: administración de justicia.

A. El delito informático como delito de dominio o de organización: la esfera de organización del usuario de la red (deberes comunes en la red)

Uno de los espacios de administración descentralizada de la organización personal se presenta en el ámbito del uso de internet: el ciberespacio es una estructura descentralizada[51], de tal forma que internet no conoce ningún tipo de jerarquía, aquí son todos los usuarios fundamentalmente iguales, no se conocen privilegios. En efecto, la autopista global de la información no posee un administrador o usufructuario que pueda responsabilizar a otro por contenidos jurídico penalmente relevantes en la red. No obstante, ante la ausencia de una regulación oficial de los usuarios de la red se generó un código de ética que tiene por finalidad dotar de una guía del buen uso y comportamiento en la red, así el caso de la "*netiqueta*".

Aquí se observa la configuración de un ámbito de organización determinado en el cual el interviniente en la red ha de obrar de manera que no interfiera en el ámbito de organización de los demás intervinientes, debiendo responder por una mala configuración de su ámbito de organización[52].

a) Los participantes y sus funciones en internet

Cada vez son más las personas o instituciones que deben intervenir para que se lleve a cabo una eficaz comunicación en internet; a cada uno de los participantes corresponde una función o tarea distinta a la de los demás intervinientes, es decir, ejercen un rol autónomo cuyo contenido viene determinado por los deberes que son inherentes al ejercicio del rol. De tal forma que es posible esperar el cumplimiento de determinadas expectativas de actuación en un contexto social concreto: la actuación en la red.

---

50 Al respecto, véase Jakobs, La ciencia del Derecho penal ante las exigencias del presente, *Estudios de Derecho Judicial*, n.º 20, Galicia, 2000, pp. 121 y ss., especialmente pp. 123 y s.

51 Cfr. Lehle, *Der Erfolgsbegriff*, cit., p. 11.

52 Sobre ello con mayores detalles, véase Mazuelos, Delitos informáticos, cit., pp. 262 y ss.

Encontramos en la red y su funcionamiento un sistema organizado por competencias de los sujetos intervinientes que posibilita su propia existencia, de tal manera que cada uno de los miembros espera que el otro actúe de acuerdo a lo esperado en el caso concreto.

En este sentido, la ordenación de las funciones individuales de los participantes presenta un punto de partida para la valoración jurídico penal[53]:

– *El rol de proveedor de contenido* en una red de datos es el de colocar la información y contenidos en la red. El proveedor de contenido es el autor de los correspondientes contenidos o desea que le sean atribuidos como propios. En términos generales, no existe una configuración de deberes que deben ser tomados en cuenta al momento de la configuración de los contenidos, sin embargo sí se ha de advertir que en el caso de que ellos estén orientados a menores, deberá de evitarse contener información que sea perjudicial para los mismos por ejemplo, pornografía (posición de garante).

– *El rol de proveedor del servicio de internet* puede ser dividido en varios sub servicios desde un punto de vista funcional, por lo que es posible identificar diversos ámbitos de actividad: el acceso a internet, ofrecer su propio contenido (proveedor de contenido), moderar los datos ajenos (listas de correos); además pueden corresponderle adicionales tareas en virtud de las estructuras técnicas en internet (hosting).

– *El rol de proveedor de acceso* se caracteriza ofrecer a sus usuarios una entrada a internet, sin presentar ningún contenido de información propio, pues sólo pone a disposición una infraestructura técnica.

– *El rol de proveedor de Links*, si bien no tiene mayores limitaciones en cuanto a las conexiones de que se puedan vincular en una página web, si se verá limitado en cuanto deberá cuidar de que si se trata de una página virtual para menores no sea posible ingresar a través de ella a páginas de otros que puedan contener información perjudicial para los menores (posición de garante)[54].

– *El rol de usuario de la red de datos* ostenta la posición del consumidor de la información, es el usuario del servicio de internet. Su posición no se encuentra limitada, pues éste a su vez puede convertirse en un proveedor de contenidos en la red. El usuario de la red ha de organizar, por ejemplo, su acceso a internet de manera que no acceda a información que no se encuentra a su disposición, como el caso de secretos militares o industriales, a través de la violación de los códigos de seguridad; en tal sentido el delito espionaje informático constituye un delito de organización.

---

53 Véase Preusse, *Informationsdelikte*, cit., pp. 27 y ss.

54 Cfr. Boese, *Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet*, Frankfurt a. M., 2000, p. 154.

También constituye un delito de organización el delito de sabotaje informático, en cuanto la destrucción de los archivos informáticos de otro representa una mala configuración de la esfera personal de organización, debido al ataque producido sobre la esfera personal de organización de otro.

B. Delitos de infracción de deber: deberes especiales en la red

La instauración de prestaciones positivas en el ámbito de las relaciones sociales alrededor de internet o de los sistemas o programas informáticos no ha sido mayormente extendida. La libertad de actuación en las redes ha caracterizado este fenómeno tecnológico en los últimos años, lo que ha evitado que se promueva la consolidación de bases institucionales propias que se vinculen a la identidad normativa de la sociedad; otro argumento explicativo de este déficit sería la "juventud" de este fenómeno y su permanente ebullición en comparación con otras instituciones sociales como la patria potestad, la administración de justicia, etc., que están fuertemente arraigadas en la sociedad.

Sin perjuicio de ello, se van presentando determinadas categorías que se encuentran en vías de consolidación como instituciones propias de la identidad normativa de la sociedad, así el caso del rol de administrador de un sistema.

a) Excurso: la problemática de la responsabilidad penal del administrador de un sistema

El administrador de un sistema es responsable sobre todo de la distribución de las informaciones electrónicas y del cuidado del servicio de e-mail[55]. En caso de una molestia técnica debe el administrador tomar cuidado de que el correo electrónico pueda ser transmitido debidamente a su correspondiente destinatario.

Ahora bien, para el cumplimiento adecuado de esa tarea el administrador del sistema tiene conocimiento periódicamente de los datos de ingreso a la red y se encuentra, por lo tanto, en la posición de acceder al buzón de correo del usuario. De tal forma que para el administrador del sistema es posible retirar e-mail ajenos del buzón de correos y leer su contenido.

Luego, surge inmediatamente la pregunta acerca de si es posible sancionar al administrador del sistema por estas conductas bajo el tipo penal de espionaje informático; indiscutiblemente, si el administrador no cuenta con autorización para acceder a los buzones de correo, incurriría en este delito. No obstante, el tema ha de ser definido a través de la observación de las facultades conferidas por los usuarios al administrador. Un sector de la doctrina entiende que el acceso en sí al buzón de correos estaría

---

55 Cfr. Vetter, *Gesetzeslücken*, cit., p. 149.

dentro de los alcances mismos de las funciones encomendadas al administrador del sistema[56], máxime si tiene la tarea de velar por que los correos electrónicos lleguen a sus correctos destinatarios; de ahí que deba verificar congestiones en la red o en los buzones mismos.

Sin embargo, respecto de un consentimiento general para leer los e-mail ajenos, se tiene que no se ha observado en el ámbito de la tecnología que el administrador de un sistema para el cumplimiento de sus tareas tenga la posibilidad general de acceder a los datos. Deducir aquí un permiso tácito de lectura a favor del administrador del sistema contradice la voluntad real del remitente que dispone de la autorización, pues se trata de la difusión indebida a un tercero.

Diferente es el caso si el contrato del proveedor del sistema autoriza al administrador a que, en determinados casos, como por ejemplo para la evitación de perturbaciones al sistema o de contenidos criminales, tome conocimiento de los correos electrónicos[57].

CONCLUSIONES

A manera de conclusión de la presente contribución cabe anotar las siguientes ideas:

– La estructura típica de los delitos informáticos ha de construirse a partir de la funcionalidad de los sistemas, programas y archivos informáticos, más allá de su naturaleza física. Ello permite identificar el elemento común a todos los comportamientos.

– Se desean eliminar las construcciones fundadas en un sobredimensionamiento del aspecto subjetivo del hecho, debido a su imposibilidad práctica.

– Es posible interpretar los delitos informáticos desde un esquema de imputación en virtud de competencias, sobre todo en el ámbito de los delitos de dominio o de organización.

– Es aún incipiente la consolidación de instituciones sociales al interior de internet que puedan ser vinculadas con el núcleo de la identidad normativa de la sociedad. Debido a ello, en la actualidad son de difícil configuración los denominados delitos de infracción de deber al interior del ciberespacio.

---

56 Así, VETTER, *Gesetzeslücken*, cit., p. 150.

57 En este sentido, VETTER, *Gesetzeslücken*, cit., p. 151.