El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual

The cybercrime and its efects in the theory of typicity: from a physical reality to a virtual reality

Ricardo Posada Maya*

Resumen

Los cibercrímenes son delitos con características particulares por lo que corresponde a la acción, el sujeto, el resultado y su imputación. Características que muestran que la teoría del delito debe ser complementada sino replanteada en algunos de sus aspectos para poder explicar y aplicar estas fenomenologías digitales que ocurren usualmente en realidades virtuales y deslocalizadas, en las cuales se advierte cada vez más una intervención menos directa del ser humano. El presente texto busca plantear algunas inquietudes relacionadas con la teoría de la tipicidad tradicional frente a estos nuevos paradigmas de criminalidad.

Abstract

Cybercrimes are crimes with particular characteristics in regards to the action, the subject, the result and the imputation. Characteristics that show that the theory of crime must be complemented and revised again in some of its aspects, and in that way be able to explain and apply these digital phenomenologies that usually happen in virtual and delocalized realities, in which we can see a less direct intervention of human beings. This text wants to add some concerns about the theory of traditional typicity in face of these new paradigms of criminality.

* Profesor de Derecho Penal y Constitución y Democracia y Director del Grupo de Investigación en Derecho penal y Justicia Transicional "Cesare Beccaria" de la Universidad de Los Andes, Bogotá - Colombia. Doctor en derecho y D. E. A. por la Universidad de Salamanca, España. El presente artículo se inscribe en la línea de aspectos fundamentales del derecho penal sustantivo y procesal penal del Grupo de Investigaciones en Derecho Penal y Justicia Transicional "Cesare Beccaria" de la Universidad de Los Andes.

Palabras clave

Cibercrimenes, nexo virtual, tipicidad, delitos informáticos en sentido amplio.

Keywords

Cybercrime, virtual nexus, typicity, Computer crime in the broad sense.

Sumario

1. Consideraciones iniciales

En los últimos 130 años la teoría científica del delito ha tenido como fundamento la imputación causal-objetiva y subjetiva al autor de conductas que ocurren en la realidad (en el mundo exterior), como la muerte del transeúnte, el hurto del dinero, el incendio forestal, etcétera. Delitos fundamentalmente analógicos que han sufrido importantes transformaciones materiales durante el siglo XX por cuenta del desarrollo de categorías como la imputación objetiva[1], que precisan mejor la imputación legal y limitan o aclaran el alcance particular del nexo de causalidad en los delitos comisivos dolos e imprudentes; pero también por cuenta del uso indiscriminado de tipos penales de amenaza o peligro en las partes especiales de los diferentes códigos penales, incluso para proteger de manera anticipada bienes jurídicos personalísimos. A esto se añade la tendencia, cada vez más amplia, de proteger objetos ideales o inmateriales, como sucede en los delitos que protegen la propiedad intelectual[2] (CP, artículos. 270 y ss.) o industrial.

Es más, a partir de finales de los años setenta de siglo XX, el nacimiento de

1 Frisch, Wolfgang, *La imputación objetiva del resultado,* Barcelona, Atelier, 2015, pp. 41 y ss., y 56 y ss.; Jescheck, Hans Heinrich / Weigend, Thomas, *Tratado de Derecho Penal*, Granada, Comares, 2002, pp. 307 y ss.; Roxin, Claus, *Derecho Penal, Parte General*, Tomo 1, Madrid, Editorial Civitas, 1997, pp. 362 y ss.; Welzel, Hans, *Derecho Penal alemán: Parte General,* Santiago, Jurídica de Chile 1997, pp. 66 y ss. (tipo y adecuación social).

2 Gracia Martín, Luis, *Prolegómenos*, Madrid, Civitas, 2001, p. 88, señala con claridad la insuficiencia dogmática de los nuevos delitos en la era del riesgo.

los delitos informáticos y los cibercrímenes (daños informáticos, trasferencias no consentidas de activos, obstaculización de datos e infraestructuras informáticas, etcétera), ha demostrado la existencia de una serie de factores dogmáticos y político-criminales que obligan a repensar e incluso replantear muchas de las nociones y categorías dogmáticas tradicionales. Esta reformulación permitiría enfrentar lo que sin duda constituye un nuevo paradigma delictivo[3] caracterizado por su virtualidad y por el empleo de medios tecnológicos avanzados en una sociedad modificada digitalmente. Son delitos que lesionan o ponen en peligro efectivo la confiabilidad (confidencialidad), la integridad y la disponibilidad de los datos, los sistemas y las infraestructuras informáticas necesarias para el adecuado funcionamiento social.

Lo importante es que se trata de conductas punibles (CP, artículo 9) que tienen ocurrencia en un "lugar" o ámbito deslocalizado como el *ciberespacio* o la Web[4], que a no dudarlo existe como una realidad simulada e implementada dentro de los computadores y las redes digitales de todo el mundo[5], y que si bien favorece la gestión social globalizada en aspectos políticos, sociales y económicos, también fortalece nuevos riesgos delictivos que se reproducen en una sociedad hiperconectada, mediática y altamente vulnerable por su analfabetismo digital. Riesgos que se caracterizan por

3 Morón Lerma, Esther, "Nuevas tecnologías e instrumentos internacionales: Consecuencias penales", en: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 39, advierte que "se trata de una realidad fluctuante, de un fenómeno dinámico, más parecido a una enfermedad que se contagia y muta que a un ser estático, como podrían ser considerados algunos delitos convencionales"; Castells, Manuel, *La era de la información,* Madrid, Alianza Editorial, 2001, pp. 59 y 60, precisa que "al final del siglo XX, hemos vivido uno de esos raros intervalos de la historia. Un intervalo caracterizado por la transformación de nuestra `cultura material´, por obra de un nuevo paradigma tecnológico organizado en torno a las tecnologías de la información", Y agrega a p. 452, que "el nuevo sistema de comunicación transforma radicalmente el espacio y el tiempo, las dimensiones fundamentales de la vida humana. *Las localidades se desprenden de su significado cultural, histórico y geográfico, y se reintegran en redes funcionales o en collages de imágenes, provocando un espacio de flujos que sustituye el espacio de lugares. El tiempo se borra en el nuevo sistema de comunicación, cuando pasado, presente y futuro pueden reprogramarse para interactuar mutuamente en el mismo mensaje.* El espacio de los flujos y el tiempo atemporal son los cimientos materiales de una nueva cultura"; También lo advierte Velásquez Velásquez, Fernando, "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos", en: *Derecho penal y nuevas tecnología,* p. 354, al concluir que "[…] Hace ya más de treinta años se inauguró un nuevo período en la historia de la humanidad caracterizado por la 'marcha triunfal' de la informática, que ha sacudido la evolución de la especie humana sobre el planeta hasta sus cimientos más profundos".

4 Respecto a la transformación de la actividad criminal en el ciberespacio v.: Miró Llinares, Fernando, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid, Marcial Pons, 2012, p. 231; Wall, David, *Cybercrime: The Transformation of Crime in the Information Age,* Cambridge: Polity Press, 2007., pp. 31 y ss.

5 Habla de mundo virtual, de "una suerte de 'réplica' del mundo real en el entorno digital": Morón Lerma, Esther, "Nuevas tecnologías e instrumentos internacionales, consecuencias penales", En: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 34.

ser automáticos, descentralizados, masivos y técnicos, que no resultan comunes a los delitos físicos tradicionales, y cuyo estudio y aplicación —difícilmente— se satisface con la teoría del "delito analógico". Como lo precisa Miró Llinares:

> El ciberespacio es para las relaciones sociales, en ese sentido, tan real como el meatspace (que es un término utilizado para referirse al espacio físico frente al ciberespacio (Fielding, s.f.)) Y todos los comportamientos socialmente identificables que no requieren de un contacto físico directo pueden realizarse en él del mismo modo que en el espacio físico; esto es solo lo cualitativo, pues, en lo cuantitativo, el ciberespacio también potencia la capacidad de las personas para el contacto social al derribar las barreras del espacio físico[6].

En todo caso, el punto de partida del análisis es claro: el *cibercrimen*, como modalidad criminal (pero en cierta medida también los delitos informáticos en sentido amplio) sitúan a la doctrina contemporánea frente a varias trasformaciones sustantivas del delito y de la pena que hay que atender con relativa urgencia[7]. *En primer lugar*, se advierte la existencia de una definición de delito más compleja y especializada que la noción de los delitos realizados en el mundo físico, y ello no solo porque ésta abarca nuevas realidades como el *ciberespacio*, o exige el empleo de técnicas especializadas (como medio) y de objetos de protección prevalentemente inmateriales, sino también, porque los comportamientos involucran una compleja transformación (o si se quiere, una evolución o un complemento) de sus elementos típicos objetivos y subjetivos, sobre todo de la acción y sus 'resultados' de acuerdo con este nuevo fenómeno social[8]; lo que genera una enorme incertidumbre dogmática.

En segundo lugar, porque la sociedad moderna, deconstruida y reconstruida como una sociedad digitalmente modificada, tiene como base de funcionamiento la gestión de la información, los datos y las infraestructuras informáticas necesarias para la subsistencia e interacción de sus miembros. Como se sabe, el mundo ha pasado por diversos avances científicos que se han convertido en instrumentos tecnológicos, y cuya transferencia a todos los sectores sociales ha producido significativos

6 Miró Llinares, Fernando, "La cibercriminalidad 2.0: falacias y realidades", pp. 58-59.

7 Precisamente, Durham, Cole, "The emerging structures of criminal information law: Tracing the contours of a new paradigm" en: *Information, Technology, Crime.* National legislation and international initiatives, Ius informationis, Vol. 6, Köln-Berlín-Bonn-München, Heymann, 1994, pp. 546, señala que "The challenge of post-modern society is to make certain that the Enlightenment values of classical criminal law are not eroded by the demands of increasing complexity or alternatively, that such values are transformed and adapted that will provide protections appropriate to the new historical context in which they are being applied".

8 Enrique Pérez Luño, Antonio, *Manual de informática y derecho,* Barcelona, Ariel, 1996, p. 75, habla de nuevas versiones de los delitos tradicionales.

cambios sociales, económicos y políticos, etcétera. Piénsese, por ejemplo, en las transformaciones que han propiciado la rueda (4000 a.C.), la vela cuadrada (1300 a.C.), la imprenta (1450 d.C.), los computadores (1941 d.C.) y el internet (1969 d.C), que han supuesto logros muy significativos en los distintos procesos de desarrollo y, últimamente, avances en los procesos de globalización y de regionalización.

Es un hecho insoslayable que hoy los datos informáticos (y las bases de datos) son activos sociales de primer orden, pues han influido en la forma en que los seres humanos se relacionan con su entorno. Sobre esta base hay que concluir, que en las últimas décadas hemos pasado de un mundo donde prevalecen los medios analógicos a un despertar digital caracterizado por el incremento de un contexto social de hiperconexión digital, y por el surgimiento de sociedades y colonias virtuales que permiten una mejor organización de la democracia deliberativa y participativa, y del ejercicio del control no institucional a las instancias públicas (Facebook, Twitter, etcétera)[9]. De estas consideraciones se intuye ya la necesidad y la importancia de proteger la seguridad de la información como un bien jurídico de naturaleza intermedia, que a su turno permita tutelar otros derechos constitucionales y bienes jurídicos como el patrimonio económico, la intimidad personal y la autodeterminación informática[10].

Y, *en tercer lugar*, porque tales avances tecnológicos hacen cada vez más compleja la delimitación de las categorías dogmáticas de la conducta punible, como estructuras jurídicas que permitirían explicar mejor estas nuevas formas de criminalidad[11]. Por

9 Posada Maya, Ricardo, "Libertad de información e independencia judicial", en *Discriminación, principio de jurisdicción universal y temas de derecho penal,* Bogotá, Uniandes, 2013, pp. 682-683, advierte que: "La fácil acogida de los mensajes mediáticos por parte de la opinión pública obedece, en gran medida, a la influencia de las nuevas generaciones en la construcción de una sociedad altamente mediática y tecnológica, que debe ser apreciada en el contexto de la globalización comunicacional. Un contexto en donde la opinión, a través de las redes sociales como Facebook, Twitter y Messenger, etcétera, resulta el mecanismo más fácil para participar en los asuntos de interés general, en particular para aquellos grupos que tradicionalmente no han tenido un acceso material a las discusiones que deciden el frágil equilibrio de las expectativas sociales; pero también porque dichos escenarios cumplen, como ninguno, o bien la reivindicación cierta del derecho a la administración de justicia, o el clásico recurso al "pan y circo", al "desquite" o a la "venganza social", como fórmulas de reafirmación y optimización subjetiva (no necesariamente objetiva o legítima) de las libertades constitucional de quien participa en este tipo de escenarios" (cursivas por fuera del texto original).

10 Satzger, Helmut, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia", en: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 19, dice que: "En esencia –tanto el ordenamiento jurídico colombiano, como en el sistema jurídico alemán– existen sobradas razones para reconocer en el derecho penal de la información el novedoso bien jurídico, pues, a diferencia de la sociedad industrial que se basa en gran medida, en los objetos de derecho físicos, tangibles, la sociedad de la información se afinca, casi exclusivamente, en datos e información prácticamente intangibles".

11 Posada Maya, Ricardo, "Una Aproximación a la Criminalidad informática en Colombia", en *Revista de*

ejemplo, el contexto de comisión tecnológica, la conexión cibernética, el automatismo, la virtualidad, la deslocalización y desregulación del ciberespacio, la triada informática y los datos inmateriales, no son conceptos que se encuadran perfectamente con una teoría del delito pensada para acciones causales lineales que producen resultados ontológicos (o jurídicos) en el mundo real, porque, como lo señala Miró Llinares, no se estaba pensando en la ciberdelincuencia "[…] cuando se desarrollan prácticamente todas las teorías criminológicas, y tampoco cuando lo hacen las teorías del crimen, pues los presupuestos negados y los datos aportados para hacerlo se refieren siempre a la delincuencia 'física' […]"[12].

En este orden de ideas, no resulta convincente construir la categoría del *cibercrimen* a partir de una noción ontológico-normativa pura que, si bien tiene un cierto rendimiento en el análisis valorativo y normativo de la imputación de delitos clásicos, en realidad no permite explicar todo lo que existe o sucede en una realidad simulada, pues, no solo no incluye todas las posibles formas de objetos y métodos lógicos, sino también, porque no permite resolver de forma hábil y práctica todos los problemas que se producen a partir de la informática en la realidad criminal[13].

Dicho lo anterior, el presente texto busca plantear algunas inquietudes que surgen cuando se observa cómo la teoría de la tipicidad "analógica" trata de explicar y ajustarse a estos nuevos paradigmas de criminalidad, bien o mal, propios del *nuevo derecho penal*[14]; en el sentido de un derecho que nace como producto de complejas

---

Derecho Comunicaciones y Nuevas Tecnologías, 2006, p. 15, indica lo siguiente: "Así las cosas, la fenomenología criminal ha variado como secuela del cambio informático global; pues la primera se ha adaptado al segundo, con el efecto previsible de que los mecanismos institucionalizados de regulación de la vida social han transformado –no siempre de manera adecuad – sus propias perspectivas y criterios de imputación. Especialmente el Derecho penal, con el fin de mejorar sus herramientas de prevención, control y sanción. Y ello es así, pues se afirma que las técnicas jurídicas de control tradicionales resultan cada vez menos eficaces –aunque ello sea discutible– para prevenir o someter formas de criminalidad masificadas, especializadas, continuas, lesivas, muy difíciles de descubrir, rastrear y criminalizar; por oposición a la progresiva vulnerabilidad de las víctimas y de las funciones protegidas".

12 Miró Llinares, Fernando, "La cibercriminalidad 2.0: Falacias y realidades", cit, p. 72.

13 Bien señala Zagrebelsky, Gustavo, *El derecho dúctil: Ley, derechos, justicia,* 5ª edición, Editorial Trotta, Madrid, 2003, p. 122, cuando se refiere al carácter práctico de la ciencia del derecho, que "[…] Naturaleza práctica del derecho significa también que el derecho, respetuoso con su función, se preocupa de su idoneidad para disciplinar efectivamente la realidad conforme al valor que los principios confieren a la misma. Así, pues, las consecuencias prácticas del derecho no son en modo alguno un aspecto posterior, independiente y carente de influencia sobre el propio derecho, sino que son un elemento cualificativo del mismo. No se trata en absoluto de asignar a lo "fáctico" una prioridad sobre lo "normativo", sino de mantener una concepción del derecho que permita que estos dos momentos no sean irrelevantes el uno para el otro […]".

14 En el ámbito continental, Hassemer, Winfried, *Viejo y nuevo derecho penal,* Editorial Temis, Trad. Muñoz Conde/Diaz, Santa Fe de Bogotá, Colombia, pp. 16 y 17, señala que "Lo que hoy podemos denominar

trasferencias tecnológicas que marcan nuevas relaciones individuales y sociales en el marco de un mundo simulado y virtual, que tiende a la globalización. De esta manera, en la segunda parte se precisan algunos elementos centrales del cibercrimen respecto a la teoría de la tipicidad, comenzando por su concepto y las particularidades que lo distinguen de los delitos tradicionales y los delitos informáticos en sentido amplio; para señalar luego algunos criterios a tener en cuenta al momento de su estudio dogmático. En el tercer aparte se efectúan algunas consideraciones a título de conclusión y, finalmente, en el cuarto se enlista la bibliografía utilizada.

2. Cibercrimen y teoría de la tipicidad

La Ley 1273 de 2009[15] adicionó al Código Penal de 2000, el capítulo VII Bis[16], con el fin de proteger un nuevo bien jurídico intermedio[17] denominado de "*De la protección de la información y de los datos*" informáticos, en el que se introducen nuevas figuras delictivas en los artículos 269A y ss., con el propósito de castigar aquellos atentados contra las funciones informáticas en sentido estricto (confidencialidad/confiabilidad, disponibilidad, integridad, no repudio y recuperación de datos)[18]. La ley también incluye los atentados que vulneran la "seguridad de la información informatizada" y los sistemas e infraestructuras informáticas, en particular de naturaleza patrimonial. Dicho título

"moderno" derecho penal se caracteriza no solo por los específicos ámbitos en los que se realiza, las específicas funciones que desempeña y los especiales instrumentos que utiliza, sino también por los especiales problemas y costos que plantea". Estos mismos argumentos sirven hoy para señalar que la cibercriminalidad se distancia y distingue del clásico modo de ejecución de los delitos tradicionales, lo que exige importantes modificaciones en la teoría de la tipicidad.

15 Ley publicada en el Diario Oficial 47.223 del 5 de enero del 2009.

16 Dicho título se compone de dos capítulos: el primero está referido a "Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" (a las cuales se deben agregar el no repudio y la recuperación de información), artículos 269A a 269H; y el segundo, atiende a "Los atentados informáticos y otras infracciones", artículos 269I, 269J y el artículo 105 de la Ley 1453 de 2011 (que resulta innominado o incluido en el artículo 269J de manera absolutamente antitécnica).

17 Mata y Martín, Ricardo, *Bienes jurídicos intermedios y delitos de peligro,* Granada, Comares, 1997, pp. 23 y ss.

18 Sobre las funciones informáticas en sentido estricto, véase Cano Martínez, Jeimy, *Manual de un Chief Information Security Officer,* Bogotá, Ediciones de la U, 2016, pp. 96 y 97; Pomante, Gianluca, *Internet e criminalità,* Torino, Giappichelli Editore, 1999 pp. 109 y 113; Posada Maya, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., p. 22; Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* Bogotá, 2012, pp. 215-216; Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* en *Estudios de Derecho penal* No. 33, Comares, Granada, 2002. pp. 67 y 69 y ss.; id., *Delincuencia informática y fraudes informáticos,* p. 72.

tomó como referencia técnica internacional la Convención contra la Cibercriminalidad de 2001 (Budapest)[19].

En realidad, se trata de nuevas conductas punibles de comisión dolosa[20] (o la reestructuración de delitos tradicionales como ciertas modalidades de *estafa y daño en bien ajeno, lavado de activos, terrorismo, narcotráfico y pornografía*, entre otros comportamientos criminales), que introducen la metodología técnica del cibercrimen a categorías dogmáticas como la conducta, el *nexo de causalidad* como base para la *imputación objetiva* y la determinación del riesgo jurídicamente desaprobado, al *dominio del hecho* en la autoría y a ciertas exigencias para los sujetos del delito; instituciones dogmáticas que resultan imprescindibles para interpretar y aplicar las modernas elaboraciones teóricas[21] del derecho penal. Veamos a continuación las principales diferencias entre los elementos propios de la teoría de la tipicidad para delitos clásicos y para los cibercrímenes.

2.1 La definición de cibercrimen

Uno de los aspectos sintomáticos de la resistencia a esta nueva realidad es, justamente, el hecho de considerar el *ciberespacio* o los sistemas informáticos y telemáticos como simples y casuales instrumentos en la ejecución de los cibercrímenes[22], incluso equiparando estos últimos a los *delitos computacionales o*

19 http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS _ 185 _ spanish.PDF
Lezertua, Manuel, "El proyecto del convenio sobre el Cybercrimen del Consejo de Europa", en: *Internet y derecho penal, Cuadernos de Derecho judicial X,* Madrid, Consejo General del Poder Judicial, 2001 pp. 15-62; Morales García, Oscar, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-Crimen", En: *Delincuencia informática, Cuadernos de derecho judicial IX,* Madrid, Consejo General del Poder Judicial, 2002, pp. 11-34.

20 Posada Maya, Ricardo, *Interceptación informática y violación de datos personales,* pp. 223 y 224, 237. Recuerda que no existen cibercrímenes de omisión pura en Colombia, que respeten el sistema de numerus clausus que cobija este tipo de modalidades. De igual manera, aunque reconoce que podría aplicarse una modalidad omisiva a los delitos de resultado material en los que preceda un deber de garante formal, tal aplicación es imposible en Colombia a partir de un deber de garante basado en fuentes materiales, pues el parágrafo del artículo 25 del CP. limita estas fuentes (los numerales enunciados a título de ejemplo del 1 al 4) a los tipos que castiguen por comisión las conductas punibles contra "la vida e integridad personal, la libertad individual y la libertad y formación sexuales". Así lo señala Velásquez, Fernando, *Fundamentos Derecho Penal, Parte General,* Colimbros, Bogotá, 2009, pp. 422 y ss. (esp. p. 423).

21 Durham, Cole, "The emerging structures of criminal information law: Tracing the contours of a new paradigm", en: *Information, Technology, Crime: National legislation and international initiatives,* Ius informationis, Vol. 6, Köln-Berlín-Bonn-München, Heymann, 1994, pp. 533-542.

22 Matellanes, Nuria, "Algunas notas sobre las formas de delincuencia informática en el Código penal", en: *Hacia un Derecho penal sin fronteras,* XII Congreso Universitario de Alumnos de Derecho penal, Madrid,

de conexidad medial a la red para el tratamiento de datos, información y sistemas informáticos (utilización de elementos incorporales)[23]. Recuérdese que los delitos vinculados al internet, a diferencia de los cibercrímenes, protegen en primera medida otros bienes jurídicos como la intimidad o el patrimonio económico antes que la seguridad de la información, los datos y los sistemas informáticos, que se protegen de manera indirecta[24]. Precisamente, atendiendo a estas diferencias, la Ley 1273 de 2009, artículo 2, adicionó un numeral 17 al artículo 58 del CP, por medio del cual se agrava la pena de los delitos no informáticos: "*Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos*" (cursivas por fuera del texto original). Una circunstancia de mayor punibilidad que recoge un *desvalor de acción en la ejecución de los delitos clásicos*, y que debe ser considerada al momento de la individualización judicial de la pena (CP, artículo 61; CPP, artículo 447).

Desde luego, está indistinción criminológica, por lo demás anacrónica, que ha sido superada por algunos autores recientes y por ciertas convenciones o directivas internacionales[25], en realidad ha impedido apreciar en su verdadero contexto la influencia

---

Colex, 2000, p. 130; Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, pp. 65, 130 y 131; id, "Hacia una expansión doctrinal y fáctico del fraude informático" en *Revista Aranzadi de derecho y nuevas tecnologías,* Nº3, 2003, p. 118; UIT, *Understanding Cybercrime: phenomena, challenges and legal response,* Ginebra, UIT, 2012, p. 11; Wall, David, *Cybercrime: The Transformation of Crime in the Information Age,* Cambridge: Polity Press, 2007, p. 221.

23 Conpes 3701 (2011-2014) define el ciberdelito como una "Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)", definición que infortunadamente no distingue entre el delito informático en sentido amplio y en sentido estricto; De La Cuesta Arzamendi, José Luis / De La Mata Barranco, Norberto, *Derecho penal informático,* Madrid, Civitas-Thomson Reuters, 2010, pp. 31 y 159; Fernández García, Emilio Manuel, "Fraudes y otros delitos patrimoniales relacionados con la informática e internet", en: *Estudios Jurídicos*, IV, Madrid, Consejo General del Poder Judicial, 1999, p. 391; Galán Muñoz, Alfonso, *El fraude y la estafa mediante sistemas informáticos: Análisis del artículo 248.2 C.P.,* Valencia, Tirant lo Blanch, 2005, pp. 29 y ss.; Miró Llinares, Fernando, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* cit, pp. 33 y ss.; Satzger, Helmut, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia", en: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 12; Sieber, Ulrich, *Computerkriminalität und Strafrecht: Neue Entwicklungen in Technik und Recht,* 2da ed., Köln-Berlin-Bonn-München, Heymanns, 1980 p. 39; id, "Criminalidad informática. Peligro y prevención", pp. 29 y ss.; id. "Documentación para una aproximación al delito informático" en *Delincuencia informática,* 1992, pp. 65-90; Tiedemann, Klaus, "Criminalidad mediante computadoras", en: *Nuevo Foro Penal* No. 30, octubre–diciembre de 1985, Bogotá, Temis, pp. 481 a 492; id., *Poder económico y delito,* Ariel, Barcelona, 1985, p. 122.

24 UIT, *El ciberdelito,* p. 25.

25 Convención de Budapest contra el Cibercrimen de 2001 (23 de noviembre), adicionada en el 2003. Y Directiva 2013/40/UE del Consejo de Europa y el Parlamento Europeo del 12 de agosto de 2013. Como bien lo señala la Unión Internacional de Telecomunicaciones: UIT, *El ciberdelito*, p. 14, "El hecho de que

de los avances tecnológicos en este tipo de conductas punibles y, en consecuencia (siguiendo una postura inductiva), ha imposibilitado adaptar y complementar la teoría del delito a nuestra realidad, contra las leyes más elementales de la lógica.

Por el contrario, reconociendo que los sistemas y las funciones informáticas no se pueden reducir a un simple medio de ejecución de los verbos típicos en los delitos comunes, la doctrina especializada sostiene que los *cibercrímenes* (o delitos informáticos en sentido *estricto* o *propio*)[26], castigan los comportamientos que lesionan o ponen en peligro de manera ilícita la seguridad de las funciones informáticas; sin perjuicio de que ello implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados. Desde esta perspectiva, no se trata de delitos tradicionales o comunes, sino de tipologías especiales realizadas a través de procedimientos informáticos, cuya riqueza técnica, su contexto virtual, la afectación de objetos inmateriales[27] y

existan disposiciones en el código penal que son aplicables a actos similares cometidos fuera de la red no significa que puedan aplicarse también a los actos cometidos a través de la internet". No en vano el Reporte Explicativo de la Convención sobre el Cibercrimen distingue con base en el bien jurídico, los medios y el objeto entre los delitos comunes realizados por medios informáticos (como sucede con la *extorsión*, la *estafa* o la *injuria* realizada mediante un correo electrónico, la *falsedad informática,* los delitos vinculados con la *pornografía infantil* y las infracciones de *copyright* y derechos asociados), y los cibercrímenes (como los delitos de *acceso abusivo a sistema informático, la obstaculización ilegítima de sistema informático o red de comunicación, interceptación de datos informáticos, violación de datos personales, daño informático, uso de software malicioso, suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.* Véase. CP, artículos 269A y ss.). A ello se añade el hecho de que los segundos usualmente recaen sobre máquinas, sistemas e infraestructuras e indirectamente sobre personas físicas.

26 Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, p. 187. Nuria Matellanes Rodríguez, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", cit, p. 130; Posada Maya, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., pp. 19-22; id, Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", cit., p. 216; Romeo Casabona, Carlos María, "De los delitos informáticos al cibercrimen", en AA.VV. *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales, Estudios de derecho penal y criminología*, núm. 78, Granada, Comares, 2006, pp. 10 y 11; Velásquez Velásquez, Fernando, "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos", cit, p. 355.

27 Posada Maya, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., pp. 19 y 20; id., Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", cit., p. 214, señala que "la *cibercriminalidad* cubre aquellas conductas punibles realizadas con fines ilícitos, no consentidas (facultadas) por el titular de la información o los datos, o abusivas de este consentimiento (facultad), que se orientan a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática […] de programas de datos o información informatizada reservada o secreta de naturaleza personal (privada o semiprivada), empresarial, comercial o pública, que pongan en peligro o lesionen (C.P., artículo 11) la seguridad de las funciones informáticas en sentido estricto, esto es, la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos *(software)* […]. *Por consiguiente, no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan*

su deslocalización en el *ciberespacio*, rompen los esquemas teóricos y las dinámicas probatorias propias de los delitos comunes.

2.2 Aspectos diferenciales entre los cibercrímenes y los delitos comunes (incluso computacionales) en el ámbito de la teoría tradicional de la tipicidad

1. El bien jurídico. Con independencia de la discusión doctrinal, los cibercrímenes en la legislación colombiana han sido previstos en el Título VII bis[28], con el fin particular de proteger *la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos*, expresada por las funciones informáticas, esto es, como ya se indicó: la integridad, confidencialidad/confiabilidad, disponibilidad, no repudio y recuperación del acceso, procesamiento, almacenamiento y la transmisión eficaz la información, los datos y los sistemas informáticos. La doctrina considera que se trata de un bien jurídico intermedio y autónomo[29], que protege de modo secundario otra clase de bienes jurídicos (personalísimos, personales y colectivos) como la intimidad personal, el patrimonio económico (así sucede en el CP, artículo 269J), la propiedad intelectual, la fe pública, etcétera[30]. También se protegen de manera particular derechos

---

los tipos penales ordinarios como referentes dogmáticos y criminológicos" (cursivas por fuera del texto original). Por otro lado Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, pp. 130. Meek Neira, Michael, *Delito informático y cadena de custodia,* Universidad Sergio Arboleda, Bogotá, 2013, pp. 59.

28 *GC,* año XVI, No. 528 del 18 de octubre de 2007, p. 4.

29 Corcoy Bidasolo, Mirentxu, *Delitos de peligro y protección de bienes jurídico-penales supraindividuales: Nuevas formas de delincuencia [sic] y reinterpretación de tipos penales clásicos,* Valencia, Tirant lo Blanch, D.L. 1999, pp. 183 y ss.; Mata y Martín, Ricardo, *Bienes jurídicos intermedios y delitos de peligro,* Granada, Comares, 1997, p. 71.

30 Posada Maya, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., p. 22. En el mismo sentido véase: María Luz Gutiérrez Francés, *Fraude informático y estafa: Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos,* Madrid, Ministerio de Justicia, 1991, pp. 262 y ss.; Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., pp. 72; Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, p. 72, señala que: "En tales términos, sostengo como principal bien jurídico protegible la información, y secundariamente los datos informáticos en sí mismos o los sistemas y redes informáticos y de telecomunicaciones, pues los primeros no constituyen más que la representación electrónica, incluso digital de la primera, con un valor variable, y los segundos los mecanismos materiales de funciones automáticas de almacenamiento, tratamiento, transferencia y transmisión de aquella, cuya afectación o no, de cualquiera de ellos, datos o elementos, pueden servir normalmente para la configuración de algunas modalidades o tipo de delitos informáticos"; Romeo Casabona, Carlos María, "Los datos de carácter personal como bienes jurídicos penalmente protegidos" en: AA.VV., *Estudios de derecho penal y criminología,* núm. 78, Granada, Comares, 2006, pp. 181 y ss.; Suárez Sánchez, Alberto, *Manual de delito informático en Colombia,* Bogotá, Universidad Externado de Colombia, 2016, p. 124.

fundamentales como el *habeas data* y la *autodeterminación informática* previstos en la Constitución Política, artículo 15; y *la seguridad, la defensa nacional* (*ciberdefensa*[31]) y *la soberanía* digital de los Estados modernos, aspectos que han sido afectados de manera continua en los últimos tiempos.

Tales funciones informáticas son las siguientes: a) La *confiabilidad/confidencialidad*, esto es, el derecho a que los datos o la información no sean divulgados y los sistemas espiados[32]. b) La *integridad, exactitud y ausencia de alteraciones ilegales* de los datos, la información, los sistemas informáticos y los procesos de tratamiento de información, busca garantizar la calidad, pureza, idoneidad y corrección de estos elementos. c) La *disponibilidad* de los datos e infraestructuras permite garantizar su funcionamiento, administración y acceso adecuado. En otras palabras, el derecho que tienen los usuarios para que el uso y acceso a datos y sistemas informáticos se dé sin perturbaciones o inhibiciones violentas o abusivas por parte de terceros o incluso de injerencias por los mismos proveedores de servicios. A estas funciones informáticas tradicionales se suman: d) el *repudio o irrenunciabilidad con prueba de envío o destino* de comunicaciones por parte de sus partícipes auténticos; y e) la recuperación de información a gran escala por parte de los usuarios en los equipos y en los distintos canales en la Web, habida cuenta la densidad digital que existe hoy en el mundo.

Para terminar este punto, vale la pena señalar que la seguridad de la información se trata de uno de los pocos bienes jurídicos de naturaleza colectivo-individual que admite la aplicación del consentimiento del titular de los datos o del sistema informático en Colombia, como causa de exclusión de la responsabilidad penal (CP, artículo 32, numeral 2). Ello se advierte cuando el legislador utiliza en los tipos penales expresiones como: "*sin autorización o por fuera de lo acordado*" o "s*in estar facultado para ello*", la última de las cuales es un elemento ampliamente incluido en los artículos 269 B y ss. En fin, como se ha señalado, el tema del bien jurídico:

> […] exige, entonces, encontrar un punto de equilibrio adecuado entre una intervención punitiva limitada en la materia y las garantías fundamentales de los ciudadanos. Más aún, cuando todo indica que los parámetros tradicionales para justificar la protección de los bienes jurídicos, no resultan plenamente satisfactorios para justificar –del mismo modo– los intereses informáticos;

31 El Conpes 3858/2016, *Política nacional de seguridad digital,* p. 88, define la *Ciberdefensa* como "el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales".

32 Gutiérrez Francés, María Luz, "La privacidad en el espacio virtual (riesgos y cauces de protección)", en *Cuadernos de la Cátedra de Seguridad Salmantina*, Nº. 3, 2011, pp. 131 y ss.

precisamente, atendidas sus características particulares como el uso masivo, la descentralización, la continuidad, el automatismo y la necesaria remisión a complejas cuestiones técnicas (que por lo pronto escapan a las consideraciones jurídicas que se presentan en estas páginas), caracterizadas por su inestabilidad y permanente transformación (de lo cual se deduce que la 'la seguridad de la información' es todavía un interés jurídico en formación y, por ende, difuso)[33].

2. La acción o el nacimiento de la "ciberacción". Es evidente que la teoría del delito moderna se ha construido con base en la realización de conductas exteriorizadas (acciones u omisiones; CP, artículos 9, 10 y 25, inciso 1) que vulneran las prohibiciones y los mandatos en los términos de la ley penal[34]. En su comienzo se trató de nociones causales o finales[35], naturales u ontológicas que, poco a poco, fueron normativizadas; pero que se caracterizan por ser realizadas en un plano físico-real, en donde el movimiento y el sentido mecánico permiten construir un concepto de comportamiento perceptible por los sentidos, enriquecido por importantes elementos de naturaleza normativa y subjetiva.

La conducta humana, al menos para un importante sector de la doctrina mayoritaria, constituye un objeto de valoración jurídica (en categorías ideales sucesivas como la tipicidad, la antijuridicidad y la culpabilidad) a partir de una realidad que tiene una duración temporal, y elementos mensurables como *distancia, intensidad, velocidad,*

33 Posada Maya, Ricardo, "Una Aproximación a la Criminalidad informática en Colombia", cit., p. 17.

34 Berruezo, Rafael, *Delitos de dominio y de infracción del deber,* 2ª edición, Montevideo-Buenos Aires, BdeF, 2016, pp. 17-18; Fernández Carrasquilla, Juan, *Derecho Penal, Principios y categorías dogmáticas*, Ibañez, Bogotá, 2011, p. 184; id., *Derecho Penal, Teoría del delito y de la pena*, Vol. 1, El delito, Bogotá, Ibáñez, 2012, p. 123; Jaén Vallejo, Manuel, *El concepto de acción en la dogmática penal,* Madrid, Colex, 1994, pp. 15 y 94; Luzón Peña, Diego Manuel, *Derecho penal Parte general,* 3ª ed., Montevideo-Buenos Aires, BdeF, 2016, pp. 247 y ss.; Maurach, Reinhart,/ Gössel, Karl Heinz / Zipf, Heinz, *Derecho Penal: Parte General,* 2 vol., 7ª ed. alemana, Buenos Aires, Astrea, 1994 - 1995 pp. 236, 241 y ss., quien la define como "una conducta humana relacionada con el medio ambiente, dominada por una voluntad dirigente y encaminada hacia un resultado"; Muñoz Conde, Francisco / García Arán, Mercedes, *Derecho Penal: Parte General,* 9ª ed., Valencia, Tirant lo Blanch, 2015, p. 228, precisan que "La conducta humana, base de toda reacción jurídico-penal, se manifiesta en el mundo externo tanto en actos positivos como omisiones"; Ricardo Posada Maya, *Delito continuado y concurso de delitos,* Bogotá, Ed. Uniandes-Ed. Ibáñez, 2012, pp. 51 y ss.; Welzel, Hans, *Derecho Penal alemán: Parte General,* cit, pp. 39 y ss.

35 Sobre la importancia de la acción y su evolución conceptual, véase: Berruezo, Rafael, *Delitos de dominio y de infracción del deber,* cit, pp. 19-43; Cuello Contreras, Joaquín, *El Derecho Penal español: Parte General,* 3ª ed., Madrid, Dykinson, 2002 pp. 374 y ss., 393 y ss.; Delitala, Giacomo, *El "Hecho" en la teoría general del delito,* Maestros del Derecho Penal No. 29, Montevideo-Buenos Aires, BdeF, 2009 p. 137; Von Liszt, Franz, *Tratado de derecho penal*, 2 ed., Madrid, Reus, 1927, p. 288; Mir Puig, Santiago, *Derecho Penal: Parte General,* Editorial Autor-Editor, 2015, pp. 189 y ss.; id., *Introducción a las bases del Derecho penal,* pp. 153 y ss.; Velásquez Velásquez, Fernando, *Fundamentos de derecho penal, Parte general,* cit., pp. 314 y ss.

energía, siempre que esta sea realizada de manera *voluntaria, personal y consciente en un determinado lugar*[36]. Sorprende comprobar entonces, como esta evidencia dogmática contrasta con la mayoría de hipótesis de cibercrimen (o delito informático en sentido estricto y de manera limitada con algunos delitos tradicionales realizados utilizando sistemas informáticos o telemáticos), en las cuales la acción (esencialmente normativa), como objeto de valoración, se caracteriza por varios aspectos que es necesario mencionar:

En primer lugar, por su *virtualidad*. En efecto, la mayoría de esta clase de comportamientos son realizados en el *ciberespacio* por "cosas" o sistemas dominados por hombres, es decir, ejecutados en una *realidad virtual* que solo tiene existencia en sistemas y redes de dispositivos informáticos. En sentido material, dichos comportamientos digitales, aunque tienen origen físico en una acción-decisión humana (un Clic que algunos consideran un simple acto preparatorio del delito), producen resultados que no superan el mundo digital, pues se dan mediante el tratamiento, la manipulación y el almacenamiento de datos informáticos basados en el sistema binario que, aunque representan materia y ubicación, realmente son ondas de energía que forman *bytes* susceptibles de agruparse en archivos y que pueden ser leídos por software y "traducidos" por el sistema en signos comprensibles para los seres humanos. Se reitera que, en la mayoría de estos casos, los resultados lógicos no trascienden al mundo físico, aunque pueden impedir a los usuarios la disponibilidad posterior (acceso y funcionamiento normal) de los datos o los sistemas informáticos. Buenos ejemplos de ello son la interceptación de datos informáticos (CP, artículo 269C), pues la acción debe darse en su origen, destino o en el interior de un sistema informático; o la violación de datos o códigos personales (CP, artículo 269F) contenidos en ficheros, archivos o bases de datos virtuales (no en medios físicos de almacenamiento), que pueden ser realizados incluso por los mismos sistemas informáticos sin intervención humana directa).

Incluso, como consecuencia de lo dicho, algunos autores caracterizan los actos

36 Fernández Carrasquilla, Juan, *Derecho Penal, Principios y categorías dogmáticas,* cit., p. 186, señala que "En un derecho penal de acto, lo que cuenta como acto, conducta o hecho punible es una manifestación de voluntad final-valorativa que transcurre en el mundo externo físico y social y que es producto de una decisión interna del agente que lo realiza" y agrega, p. 190, que "La exterioridad o materialidad del acto entraña, pues, el carácter perceptible o empírico de la manifestación de voluntad final, así como de las consecuencias o resultados que el tipo engarce al hecho antecedente de a sanción penal". Zaffaroni, Eugenio Raúl, Alagia, Alejandro y Slokar, Alejandro, *Manual de Derecho Penal. Parte General,* Ediar, 2005, pp. 417-418: "Por otra parte, las acciones no pueden comprenderse, ni tampoco tienen sentido, si no están referidas a determinado lugar o paraje del mundo" (cursivas por fuera del texto original), lo que claramente no siempre ocurre, salvo por el lugar en donde se ha dado la instrucción informática, si es que resulta posible determinarlo.

preparatorios de esas fenomenologías criminales. Por ejemplo, Meek Neira sostiene que:

> De cara al concepto de delito informático, es importante también tener en cuenta que *los actos preparatorios del delito comienzan al momento en que el sujeto entra en contacto con alguna pieza del hardware, considerado como un puente entre el campo del mundo físico y el inmaterial de la información y los datos informáticos, siendo este elemento de donde parten impulsos o señales dirigidos a impartir órdenes al sistema tendentes a alcanzar la finalidad criminosa del agente, que no es distinta a lesionar el bien jurídico ya mencionado de carácter informático* y no a otros cuando, en primera instancia, el sujeto procede a captar dolosamente algún caudal informático para su provecho o el de terceros. De lo contrario, se tendrían en la definición elementos que la desvirtuarían como es usar a los ordenadores como medio para la comisión de cualquiera de los supuestos de hecho presentes en la Parte Especial del Código Penal[37].

En segundo lugar, la acción digital o virtual se caracteriza porque representa la ejecución *de instrucciones procesables por los sistemas informáticos*. Es más, la interacción directa o a distancia con el sistema no se da mediante una acción lineal sino claramente *interactiva/reactiva* que, mediante *links* asociados a páginas vinculadas a sitios web, permite buscar información (en distintos formatos: video, audio, texto, etcétera) según los intereses del usuario o realizar actividades que se pueden desplegar en distintos espacios de esta realidad, de manera indefinida e incluso automática.

En tercer lugar, a diferencia de las conductas analógicas como causar la muerte, daños en el cuerpo o en la salud, o apropiarse de bienes del Estado o los particulares, las acciones digitales o ciberinteracciones son conductas *deslocalizadas* o *desubicadas físicamente*, pues el ciberespacio como realidad virtual es precisamente un ámbito de interacción lógica. Esto no significa que el autor-usuario conectado, que domina objetiva y positivamente el sistema informático y, por consiguiente, el hecho virtual como tratamiento de información, no se encuentre en un lugar determinado o que siempre se desconozca el lugar en donde tienen origen las instrucciones informáticas. De hecho, la deslocalización ha tenido importantes repercusiones para definir la competencia de los jueces penales de conocimiento que deciden la responsabilidad penal sobre esta clase de comportamientos criminales. Así, usualmente tiene aplicación el artículo 43 del CPP, que literalmente señala que: "*Cuando no fuere posible determinar el lugar de ocurrencia del hecho, éste se hubiere realizado en varios lugares, en uno incierto o en el extranjero, la competencia del juez de conocimiento se fija por el lugar donde se formule acusación por parte de la Fiscalía General de la Nación, lo cual hará donde se encuentren los elementos*

37 Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., pp. 46 y 47.

fundamentales de la acusación". Nótese que, en principio, la referencia normativa se hace a lugares físicos en el territorio nacional o en el extranjero.

De igual manera, añádase que la ciberacción es fundamentalmente *automatizada y programable*. Por cuenta del primer aspecto, la acción sobresale por la aplicación de procedimientos a actos que antes se caracterizaban por sus propios componentes corporales y síquicos. La automatización de la ciberacción supone, entonces, que el origen lógico del delito sea imputable normativamente a la actuación de un sujeto físico que instruye el sistema informático o a la actividad de la inteligencia artificial, pero que en efecto (incluso previamente determinado) se produce por una acción instrumental que por sí misma carece de voluntariedad, voluntad ejecutiva, e incluso por la participación física, externa y concomitante de un ser humano (en todo caso distintos a los casos de actos automatizados que excluyen la conducta humana). Así sucede, por ejemplo, con la realización automática, repetida y simultanea de cientos de ataques cibernéticos por minuto a ordenadores ubicados físicamente en diferentes países, llevados a cabo por un sistema informático o por organizaciones colectivas criminales (incluso por OVT: *organizaciones virtuales transnacionales*), cuyo software ha sido especialmente diseñado para distribuir programas maliciosos o con efectos dañinos a equipos ubicados en todo el mundo[38].

En cuanto a la *programabilidad de la ciberacción*, hay que recordar que la conducta tradicional implica que el sujeto o bien realiza de manera instantánea la acción, la fracciona por instalamentos en momentos diferentes o prolonga su ejecución de manera ontológico-normativa y física (de manera que la unidad de acción suponga la realización en un contexto temporal y espacial determinado, unidad de fin o dolo y homogeneidad de los actos que realiza de manera permanente, continua u habitual con el propósito de cumplir con el plan criminal); mientras que la acción cibercriminal puede ser programada y flexible en distintos planos, esto es, realizada por los sistemas informáticos en la forma, tiempo, repetición y ocasión dispuestos por las instrucciones designadas por el hacker/cracker (se trata en todo caso de un concepto distinto del uso de elementos programables como una bomba con cuenta de tiempo). En el contexto de un ataque informático[39], las amenazas generalmente cumplen etapas que van desde la búsqueda de vulnerabilidades de los sistemas y los equipos, hasta actos delictivos concretos (ataques directos) utilizando el sistema contra los datos y la información allí registrada.

38 Por ejemplo, los casos de ataques distribuidos, en los que un sujeto utiliza una red Botnet (vinculando ordenadores infectados de víctimas inconscientes) para realizar un ataque DNS que puede afectar a miles de víctimas.

39 Posada Maya, Ricardo, *Delito continuado y concurso de delitos,* cit., pp. 60-186.

La posibilidad de programar los actos informáticos de ataque permite, inclusive, que los procesos virtuales sean realizados cuando el sujeto activo no se encuentra consciente, esté dormido o imposibilitado para tener una injerencia física o para desarrollar un control real sobre las conductas punibles.

Este tipo de acciones también ha promovido nuevas dinámicas criminales que se traducen en la instrumentalización de cadenas de víctimas inconscientes en la realización del delito, mediante el uso de sus sistemas informáticos. Se trata, técnicamente, de *ataques distribuidos*, mediante los cuales se utilizan automáticamente redes de computadores infectados (Botnet), sin conocimiento o (con la complicidad) de sus usuarios titulares; lo cual, desde la perspectiva del desvalor de acción objetivo, comporta una forma particular de ejecutar los delitos que facilita su comisión y la producción de sus efectos frente a la comunidad titular de los derechos a la disposición, el acceso y el tratamiento de información confiable e integral. Así ocurre, por ejemplo, en la suplantación de sitios web para capturar datos personales (CP, artículo 269g, inc. 3º y 269h, núm. 7)[40].

Dicho lo anterior, es evidente que la conducta humana, como base de la conducta en el cibercrimen ha cambiado como objeto que se desvalora en las distintas categorías del delito, por lo que sus características deben ser objeto de una precisa caracterización dogmática por parte de la doctrina nacional, que permita combatir y estudiar adecuadamente estas fenomenologías criminales.

3. Los sujetos activos del cibercrimen. Uno de los aspectos más interesantes y complejos de los ciberdelitos es, justamente, el sujeto activo o los autores (CP, artículo 29). Mientras que en los delitos tradicionales la relación entre los sujetos y el delito está mediada por su propia naturaleza y por la forma de llevar a cabo la acción u omisión externa que los produce; en los delitos informáticos (en sentido estricto y amplio) esta relación física, así sea mediada por una persona natural, no resulta suficiente para caracterizar adecuadamente al sujeto que puede realizar el delito.

Dicho en otras palabras, en algunos tipos penales, además de verificar la presencia del autor físico que produce un peligro o causa un resultado, es imprescindible que dicho autor realice la conducta en calidad de *usuario de un sistema informático* o en calidad de *ciberautor (cibernauta)*. De forma breve, un usuario es aquel sujeto funcional que utiliza su identidad digital y la de sus dispositivos, mediante una *conexión virtual a los sistemas que le otorgan* privilegios

40 Inc. 3º: "la pena prevista en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena de ese delito y 269h, núm. 7: "utilizando como instrumento a un tercero de buena fe."

informáticos y jurídicos, para interactuar en el ciberespacio (como realidad simulada) y manipular mediante instrucciones un sistema informático (operativo o aplicativo), con el fin de tratar información u obtener servicios para llevar a cabo determinados propósitos, que en este caso se materializan en actos delictivos dolosos[41]. No hay duda que esta característica es fundamental, por ejemplo, en las hipótesis típicas de acceso o mantenimiento abusivo a un sistema informático (CP, artículo 269A), o en los casos en los que el autor utiliza o emplea medios informáticos para realizar de manera remota violaciones de datos (sustracciones, obtenciones, interceptaciones, etcétera, CP, artículo 269C), obstrucciones a sistemas informáticos o a datos (CP, artículo 269B) y daños informáticos (CP, artículo 269D); sin que se trate de delito de infracción del deber.

Incluso, téngase en cuenta que, cuando se habla de un sujeto idóneo o capaz para la realización de cibercrímenes, no solo se está haciendo referencia a la necesidad ocasional de que un autor posea, en ciertas circunstancias, conocimientos especiales informáticos (un aspecto cada vez menos requerido para la ejecución de estos delitos), sino que realmente éste esté conectado virtualmente al sistema y pueda dominar lógicamente el tratamiento de información con fines ilícitos.

En la doctrina nacional, autores como Meek Neira hablan, por ejemplo, de la importancia de la *triada informática*, al señalar lo siguiente:

> […] dentro del concepto de tríada informática el primer elemento a tener en cuenta es el de usuario, esto es, la persona presta a satisfacer sus necesidades "informáticas" o de cualquier índole y que se sitúa frente a un ordenador dispuesta a impartirle órdenes para su funcionamiento; los ordenadores, recuérdese, no poseen motivación propia si bien es cierto que pueden operar de forma automática, a condición de que se les haya programado previamente para ejecutar determinadas funciones. Los mal denominados 'computadores' entre nosotros, entonces, al estar siempre operados o subordinados a la voluntad humana, para poder operar requieren de otro elemento que es el software, el segundo componente de la figura en examen. En la mitad de la triada se encuentra el tercer elemento, el hardware, que obra como un puente entre el campo del mundo físico y el de la información y los datos informáticos, por cuanto se refiere a los elementos del

41 Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., pp. 39 y 40, señala lo siguiente: "El Hardware es, entonces, una parte fundamental, a él se hace referencia con los teclados o mousses que envían al software distintos comandos, mismos que primero son percibidos por el hardware donde se cierra un circuito que emite una señal codificada al software, en forma del respectivo comando impartido desde el plano del mundo físico, pues, como se ha dicho, "para que los ordenadores puedan manipular datos, deben recibirlos codificados. Aunque pueden utilizarse códigos muy diversos, todos los códigos empleados en computación tienen una característica común: solo utilizan dos signos, los dígitos 0 y 1". Y es, justamente, del hardware de donde luego de su accionar, parten dichas señales".

sistema que podemos apreciar con nuestros sentidos, es decir, son las piezas o partes físicas del mismo. […] *Así las cosas, la tríada informática supone la conjunción, el especial vínculo de tres elementos necesarios y que deben estar o haber estado en contacto para que el sistema desarrolle alguna función; sin uno cualquiera de estos elementos el sistema sencillamente no opera*[42].

La prueba de lo dicho es que, para castigar exitosamente esta clase de comportamientos punibles, no solo es necesario demostrar que un cierto sistema informático fue accedido o manipulado desde un determinado dispositivo vinculado a una IP, sino también (y aquí reside la razón más frecuente de impunidad) vincular el empleo de dicho dispositivo o sistema con una persona natural a través de su identidad digital (siempre y cuando no haya sido víctima de una suplantación en el sistema por parte de un tercero). En la teoría, además, el verdadero problema para comprender a cabalidad la naturaleza de la acción, es que un buen sector de la doctrina, en un acto incomprensible de simplificación jurídica, asimila equivocadamente estos delitos a aquellos en los que el autor utiliza de manera natural un instrumento físico (el uso de un animal, el uso de un revolver, etcétera), cuando lo cierto es que el ciberespacio es mucho más que un medio o un instrumento, es una verdadera realidad simulada[43]. En este sentido, en estos delitos es fundamental no subestimar el papel que juegan los instrumentos informáticos y la realidad simulada, porque más allá del autor, es dudoso que un simple *Clic* causal sea equiparable a la realización ejecutiva completa y directa de todo el delito, aunque esta realización le deba/pueda ser imputada al autor-usuario. Por ello se habla, precisamente, de la tríada informática.

Otra característica importante de los sujetos activos en el cibercrimen es su creciente *anonimato*, propiciado no solo por las modernas técnicas de encriptación o cifrado, el uso de datos *pseudonimizados* que permiten separar los mensajes de la identidad del emisor, dificultar el sentido de los mensajes o el empleo de sistemas que entorpecen la trazabilidad de las acciones del atacante en los sistemas vulnerados; sino también, por la enorme dificultad para determinar la relación entre el uso de un equipo informático que se conecta mediante una determinada IP y un criminal. Ello sin contar con la posibilidad de suplantar a un usuario legítimo mediante el uso de software de efectos dañinos cuando se utilizan redes Wi-Fi. El anonimato también se

42 Ibíd., pp. 39 y 40.

43 En esta línea radical se expresa, Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., p. 49, al decir que "En fin, si se les llamara a todos esos fenómenos como "ciberdelitos" la criminalidad informática se perdía en la nebulosa al tener el sujeto activo que valerse para desplegar su conducta siempre de medios telemáticos. Cosa que, indiscutiblemente, refleja un fatal entendimiento de la telemática ajeno a su real sentido y esencia, que es simplemente prestar un vehículo de transmisión para la comunicación entre los sistemas informáticos […]".

favorece ampliamente por el uso de "espacios" informáticos como la Web profunda (*Deep web*) para realizar conductas delictivas graves, que usualmente son pagadas con moneda digital a través de transacciones anónimas, irreversibles, inmodificables e indetectables por su cifrado avanzado; e incluso el hecho de que la prueba sobre el autor o la trazabilidad de sus acciones se diluya por la comisión de esta clase de delitos por parte de las OVT u *organizaciones virtuales transnacionales*, que además de la metodología mafiosa transnacional utilizan la metodología virtual del cibercrimen. En conclusión, "El que…" de los sujetos activos del delito empieza a ser ampliamente superado por una realidad marcada por la *criminalidad organizada transnacional, transfronteriza y corporativa*.

Ahora bien, más allá del debate técnico y dogmático, la discusión sobre la naturaleza de los sujetos activos en el cibercrimen y delitos virtualmente conexos apenas comienza en el mundo. De esta manera, en Europa se empieza a discutir el fenómeno de la *inteligencia artificial* y la regulación de la responsabilidad jurídica por los perjuicios y atentados contra la seguridad física de las personas causados por sofisticados entes androides, bots y robots (incluso interconectados), debido a sus propias determinaciones (autónomas) o por fallos atribuibles a su programación. Se trata de enmarcar este fenómeno en el contexto de una nueva revolución industrial, en la que este tipo de entes tendría la capacidad de reemplazar al ser humano en sus actividades ordinarias (laborales), generando un impacto sin precedentes en la historia de la humanidad.

En otros términos, se plantea el problema de la posible responsabilidad derivada del uso de androides, o la muy debatida responsabilidad de los mismos androides al estilo de la responsabilidad de las personas jurídicas, para llegar a plantear incluso la existencia de hechos (y delitos) sin autor, causados por elementos técnicos autónomos como automóviles o drones, etcétera. Es una realidad que hoy las aplicaciones y los dispositivos informáticos pueden actuar y comunicarse entre ellos sin intervención humana e incluso sin que nadie tenga conocimiento de ello. De esta manera, *El proyecto de informe del Parlamento Europeo* (2014-2019), elaborado por la comisión de asuntos jurídicos con fecha del 31.05.2016, con recomendaciones destinadas a la Comisión sobre normas de derecho civil sobre robótica (2015/2103 (INL)44), agrega en sus considerandos interesantes cuestiones, entre las cuales vale la pena destacar las siguientes:

Primero, (considerando I), se reconoce la posibilidad de que la inteligencia artificial

44 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//ES

pueda superar la capacidad intelectual humana y sea un verdadero desafío para ella controlar dichas entidades, al punto de garantizar la existencia de la especie. Y considera que, "[…] hasta que los robots sean conscientes de su propia existencia o sean fabricados con esa cualidad, si es que ese momento llega algún día, debe entenderse que las leyes de Asimov van dirigidas a los diseñadores, fabricantes y operadores de robots, dado que dichas leyes no pueden traducirse en código de máquina"[45].

Segundo (considerando M), es necesario disponer de una serie de normas en materia de responsabilidad y deontología robótica que reflejen el pensamiento humano. Ello, exige reconocer que los robots han adquirido rasgos autónomos con la capacidad de aprender de la experiencia y tomar decisiones independientes, lo cual los hace asimilables a los agentes físicos que interactúan en su entorno. Agrega en el considerando (R), que "[…] *la autonomía de un robot puede definirse como la capacidad de tomar decisiones y aplicarlas en el mundo exterior, con independencia de cualquier control o influencia externa; que esa autonomía es puramente tecnológica y que su grado depende del grado de complejidad de la interacción del robot con su entorno que se haya previsto al diseñarlo*" (cursivas por fuera del texto original).

Tercero (considerando S), que mientras más autónomos sean los robots, *menos se les podrá considerar como simples instrumentos en manos humanas*, y en particular de sus fabricantes, propietarios o usuarios. Ello demuestra que toda la normativa en materia de responsabilidad es insuficiente y se requieren normas que "[…] *se centren en cómo una máquina puede considerarse parcial o totalmente responsable de sus actos u omisiones*" e incluso que permitan determinar cuándo una máquina debe tener "personalidad jurídica" a partir de su autonomía. Es más, el informe llega a presentar el debate acerca de la necesidad de crear para los robots autónomos más complejos, que puedan tomar decisiones inteligentes o interactuar con terceros de forma independiente, "una nueva categoría, con sus propias características y repercusiones en lo que se refiere a atribución de derechos y obligaciones, incluida la responsabilidad por daños". Esto es, sugiere "crear una personalidad jurídica específica para los robots, de modo que al menos puedan ser considerados personas electrónicas con derechos y obligaciones específicos".

Se trata de consideraciones que, sin duda, abren por completo nuevas dinámicas jurídicas en el mundo global que, a pesar de lo aterradoras que puedan

45 Las leyes de Isaac Asimov sobre la robótica están perfectamente descritas en su cuento el "Hombre Bicentenario", p. 656, así: "Las tres leyes de la robótica: 1. Un robot no debe dañar a un ser humano ni, por inacción permitir que un ser humano sufra daño. 2. Un robot debe obedecer las órdenes impartidas por los señores humanos, excepto cuando dichas órdenes estén reñidas con la Primera Ley. 3. Un robot debe proteger su propia especie, mientras dicha protección no esté reñida ni con la Primera ni con la Segunda Ley". Asimov, Isaac, *Hombre Bicentenario,* Estados Unidos, Flash, 1976, p. 656.

llegar a ser para muchos, lo cierto es que son una realidad que deberá discutirse en el algún momento en el derecho penal moderno, sin que este debate teórico pueda ser simplemente cercenado mediante un fraude de etiquetas basado en un derecho clásico, exclusivamente centrado en los seres humanos. Así, la ciencia ficción termina siendo realidad.

4. Los objetos sobre los cuales recae la acción y los medios tecnológicos en el cibercrimen. Otro de los aspectos que permiten distinguir los delitos comunes o informáticos en sentido amplio de los cibercrímenes es, precisamente, que los objetos digitales son al mismo tiempo medios virtuales (ámbitos) inherentes de ejecución del delito y el objeto final sobre el que se ejecuta la acción cibercriminal.

El cibercrimen es, entonces, un comportamiento tecnológico particular que no puede ser subsumido o consumido por otras conductas punibles diseñadas para proteger objetos físicos o materiales. Por ejemplo, el delito de hurto o el de estafa (CP., artículos 239 y ss. y 246), diseñados por el legislador para proteger bienes materiales muebles e inmuebles según el caso, no pueden cubrir adecuadamente el delito de transferencia no consentida de activos, no solo porque este recae esencialmente sobre datos inmateriales como software (aplicativo u operativo), sino también porque su procedimiento no consiste en el engaño directo a una persona ni en un apoderamiento de cosas empleando técnicas de ingeniería social. Nadie duda que la base de este tipo de comportamientos sea la manipulación del sistema informático. Igual consideración se puede hacer frente a los delitos de daño en bien ajeno (CP, artículo 265) y daño informático (CP, artículo 269D), pues las diferencias entre ambas hipótesis jurídicas implican usualmente la necesidad de crear delitos diametralmente opuestos.

Así las cosas, es menester reseñar los objetos propios de los ciberdelitos en nuestro medio jurídico:

a) Los datos informáticos. Son el principal objeto virtual de protección por parte de esta categoría de delitos. Generalmente –porque no es una definición unívoca— se entiende que los datos son representaciones e instrucciones simbólicas de hechos vinculados a un determinado emisor legítimo (como datos de personas naturales o jurídicas[46]) o desvinculadas (como datos impersonales o materiales), informaciones o

46 Los datos personales son definidos en Colombia por la Ley 1581 de 2012, artículo 3, literal c), como "cualquier información vinculada a o que pueda asociarse a una o varias personas naturales determinadas o determinables". En un sentido similar lo hacía la Ley 1266 de 2008, artículo 3, literal e). En el derecho extranjero, los datos personales son definidos, por ejemplo, por el artículo 4 (1) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de Europa del 27/04/2016, como "Toda información sobre una persona física identificada o identificable ("el interesado"); se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, datos de localización, un identificador

conceptos en sentido numérico, alfabético, alfanumérico o algorítmico[47].

Además de su inmaterialidad[48] , la principal característica de los datos (y por ello son informáticos) es que pueden ser utilizados de manera idónea como instrucciones o ser tratados, almacenados y transmitidos funcionalmente, etcétera, por los sistemas informáticos o telemáticos, haciendo explícita la señal binaria que los integra dentro de un contexto social determinado por medio del Hardware. En general, los datos tienen el sentido de poder transmitirle a los seres humanos conocimientos específicos a través de mensajes convencionales informáticos y simbólicos, identificables y organizados, que les permitan (como receptores) tomar decisiones efectivas en el marco de una interacción comunicativa. En todo caso, es necesario recordar que el *sistema penal de protección de datos* –personales e impersonales–, bajo los principios de *autodeterminación y prohibición de injerencia informática*, depende de la clasificación de los datos en las leyes de *Habeas Data*[49] vigentes en Colombia.

Naturalmente, al concepto de dato hay que agregar como objeto protegido a los metadatos, es decir, los datos localizados en sistemas indexados de creación, modificación, tratamiento, localización, etcétera. de otros datos de texto, imagen o voz que quedan almacenados en los archivos de salida. Los metadatos adjuntos permiten o facilitan la indexación, clasificación, tratamiento, etcétera. de los datos principales, y por eso su interceptación o violación ilícita supone un peligro para la intimidad de los usuarios-víctimas. En igual sentido se añaden las *cookies*, o archivos que guardan información de los usuarios al navegar por internet, relativa a su nombre, contraseñas, preferencias de navegación, etcétera, que facilitan el ingreso del sujeto

---

en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

47 Así, la Convención de Budapest de 2001 contra el Cibercrimen, Ch. I, artículo 1, señala: "b) Por «datos informáticos» se entenderá una "Unidad básica de información, ello es, cualquier representación de información, conocimiento, hechos, conceptos o instrucciones que pueden ser procesadas u operadas por sistemas automáticos de computadores, y cuya unión con otros datos conforma la información en un sentido estricto". Por su parte, el artículo 2 de la Directiva 2013/407UE del Parlamento Europeo y el Consejo de Europa de 12/08/2013, los define como "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función. En igual sentido se expresa la Decisión Marco 2005/222/JAI del 24/02/2005, artículo 1.

48 Posada Maya, Ricardo, "Interceptación informática y violación de datos personales", cit., pp. 207, agrega que "precisamente, la característica esencial del dato, como objeto principal sobre el cual recae la acción cibercriminal es su inmaterialidad, de modo tal que no es susceptible de visualización directa, para lo cual requiere de un procesamiento digital que haga explícita la señal binaria que los integran".

49 Sobre la clasificación de los datos en las leyes de habeas data, véase Remolina Angarita, Nelson, "Tratamiento de datos personales para fines estadísticos desde la perspectiva del gobierno electrónico" en *Revista Cuadernos de Derecho Público,* 2003, pp. 136.

a los sitios web ya visitados.

b) La información. Esta es definida en Colombia por la Ley 1712 de 2014, artículo 6, literal a), como "[…] *un conjunto organizado de datos contenidos en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen*". La información se compone de manera mínima, entonces, por datos esenciales que pueden conformar información compleja, compuesta por entramados de datos binarios (*bite* y *bytes* caracterizados por puntos magnéticos (1) o burbujas magnéticas (0)) que puedan ser procesados por sistemas informáticos o que se encuentren almacenados en bases y bancos de datos públicos y privados.

Dentro de este componente también se considera al c) *software* (subsistema lógico) o programas operativos y aplicativos que permiten dicho tratamiento, que usualmente son instrucciones que el equipo ejecuta para lograr un resultado informático determinado. Al programa se suman los procedimientos, reglas, documentación y datos asociados a la operación del sistema[50]. En Colombia, dicho elemento está definido por la Decisión 351 de 1993 de la Comunidad Andina de Naciones (CAN) artículo 3, como la "expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso".

d) Los sistemas informáticos. Se trata de dispositivos compuestos por *hardware* y *software* que, de manera independiente o en conexión en red con otros dispositivos, pueden retransmitir, transmitir, coordinar o controlar las comunicaciones de datos o programas (mensajes de datos)[51]. En este sentido, por ejemplo, la Convención de

50 Véase el 729-1983 - IEEE Standard Glossary of Software Engineering Terminology; Reporte Explicativo –ETS 185– Cybercrime, § 23. Precisamente, el artículo 2 del Dto. 1360 de 1989 Reglamentario de la Ley 23 de 1982, dice que "El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción del programa y el material auxiliar". Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., pp. 40, indica que el software "[…] se convierte en la parte o elemento esencial del sistema informático y es él el que le permite al hombre expresarse dolosamente y, de manera inmaterial, ante el sistema y frente a otros que se encuentran conectados a éste o a la red de redes, esto es, la internet".

51 Según el reporte Explicativo de la convención de Budapest de 2001 contra el Cibercrimen, un sistema informático: "23. [...] bajo la Convención es un dispositivo que consta de hardware y software desarrollado para el procesamiento automático de datos digitales. Puede incluir de entrada, salida y las instalaciones de almacenamiento. Puede ser independiente o estar conectados en red con otros dispositivos similares "Automático" significa sin intervención humana directa, "tratamiento de datos" significa que los datos en el sistema informático son operados por la ejecución de un programa de ordenador. […] Un sistema informático por lo general se compone de diferentes dispositivos, para ser

Budapest (artículo 1) los define como "[…] *todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa*". En un sentido similar se pronuncia el artículo 2 de la Directiva 2013/40/UE, que define los sistemas de información como "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento"[52]. La acción informática muchas veces no se concibe sin la actuación automática de los sistemas informáticos, por lo que tenemos acciones sin intervención humana directa.

5. El resultado. A diferencia de los conceptos tradicionales del delito, en la actualidad el concepto de resultado se entiende generalmente en un sentido jurídico[53], lo que comprende tanto los peligros (en abstracto y en concreto[54]) como los resultados propiamente dichos, entre los cuales usualmente se mencionan los materiales (la muerte, los daños en el cuerpo o en la salud, el apoderamiento de muebles, etcétera) y los psicológicos (como el convencimiento de estar obligado de tolerar, omitir o realizar alguna cosa, etcétera, y en general aquellas modificaciones que afectan la autonomía del sujeto como ocurre en la extorsión, el constreñimiento o la tortura). Esta visión, predominantemente analógica, supone que la mayoría de los delitos tengan una expresión ejecutiva y un resultado en el mundo exterior o físico, muy propia de los conceptos del delito de los siglos XIX y XX.

---

distinguido como el procesador o unidad central de procesamiento, y los periféricos [...]" (cursivas por fuera del texto original).

52 En sentido similar, véase el artículo 1 de la Decisión Marco 2005/222/JAI del 24/02/2005 del Consejo de la UE.

53 Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., p. 359, lo define como "el efecto y la consecuencia de la acción que se manifiestan en el mundo exterior, y que inciden tanto en el plano físico como en el psíquico". Agrega Berruezo, Rafael, *Delitos de dominio y de infracción del deber,* BdeF, 2009, p. 85; Fernández Carrasquilla, Juan, *Derecho Penal, Teoría del delito y de la pena,* Ibañez, 2012, pp. 134 y ss., indica que "Actuar es algo humano que implica necesariamente mutaciones en el mundo físico-causal y modificaciones en el mundo social (interacciones o interferencias con los otros no solo físicas sino también de sentido, significación o comunicación)"; Luzón Peña, Diego, *Lecciones de Derecho penal, parte general,* Tirant Lo Blanch, 3ª Edición, 2016, pp. 309 y 310; Zaffaroni, Eugenio Raúl, Alagia, Alejandro y Slokar, Alejandro, *Manual de Derecho Penal. Parte General,* cit., pp. 457 -458.

54 Sobre estos conceptos, véase Méndez Rodríguez, Cristina, *Los delitos de peligro y sus técnicas de tipificación,* Servicio Publicaciones Facultad Derecho, Universidad Complutense Madrid, 1993, pp. 118, al afirmar que "El tipo penal de peligro no hace otra cosa que recoger una regla de experiencia: se tipifican ciertas acciones que provocan resultados de peligro porque, precisamente en estos casos, se ha demostrado que la lesión es frecuente".

Como era de esperarse, esta relación ontológica o natural entre la ejecución física de la acción y la lesión o peligro de los bienes materiales ha sido complementada[55], *en primer lugar, por los delitos contra los derechos morales y patrimoniales de autor, y la violación a los mecanismos de protección de derechos de autor y derechos conexos y otras defraudaciones* (C.P., artículos 270, 271 mod. Ley 1032 de 2006, artículo 2 y 272 mod. Ley 1032 de 2006, artículo 3), que incorporan entre otros delitos los resultados de *carácter inmaterial*[56], por ejemplo, las modificaciones a las obras literarias de carácter inmaterial como el *software*, o a las obras científicas o artísticas en formato digital, sin que la acción criminal tenga que ser realizada por fuera de sistemas de tratamiento de información.

En segundo lugar, por los cibercrímenes[57], que no obstante exigir excepcionalmente algunos resultados materiales para consumar ciertos delitos, en general prevén categorías como el resultado lógico (como modalidad del resultado inmaterial). Piénsese, por ejemplo, en el delito de daño informático (C.P., artículo 269D) que castiga la destrucción, daño, borrado, deterioro, alteración, supresión de datos informáticos o de sistemas de tratamiento de información (o sus partes o componentes lógicos); el impedir el acceso normal a un sistema informático o a los datos (C.P., artículo 269B); la interceptación de datos informáticos (C.P., artículo 269C); la obtención, sustracción, interceptación o modificación de códigos personales o datos personales contenidos en ficheros o archivos (C.P., artículo 269F); la modificación del sistema de resolución de nombres de dominio (C.P., artículo 269G); y el conseguir la transferencia no consentida

55 Stratenwerth, Günter, *Derecho penal: Parte General I,* S.L. Civitas Ediciones, 2005, p. 126, precisa que "El resultado de que se trate, sin embargo, puede estar configurado de maneras muy distintas: desde la modificación puramente exterior del sustrato material de un bien jurídico, hasta la producción de un daño meramente inmaterial".

56 Se trata de un concepto que no coincide plenamente con el de resultado formal o ideal que proponen algunos autores como Luzón Peña, Diego, *Lecciones de Derecho penal, parte general,* cit., pp. 323, como aquel que "supone un cambio de la realidad inmaterial, captable lógica o intelectualmente —a veces mediante asignación de sentido o valoración—: p. ej. La creación de un objeto o una adscripción no veraz en las falsedades, o la producción de una situación de estimación deshonrosa en las injurias".

57 Se trata de actuaciones que realmente tienden a normalizar técnicas legislativas dudosas a la hora de consagrar este tipo de comportamientos, particularmente en tres aspectos: a) la creación de verdaderas cadenas de comportamientos técnicos que se solapan entre ellas, entre delitos medios y delitos fin. b) La consagración de tipos abiertos e hipernormativos (como sucede con el delito de violación de datos personales que consagra doce verbos rectores (C.P, artículo 269F), la suplantación de sitios web para capturar datos personales que prevé ocho verbos típicos (C.P, artículo 269G) y el uso de software malicioso que prevé siete verbos típicos (C.P, artículo 269E). Y c) la prevalencia de delitos de peligro que suponen una clara anticipación de las barreras de protección del derecho penal, ante una –y esto es importante resaltarlo– inexistente regulación administrativa en materia de infracciones informáticas que protejan la seguridad de la información, los sistemas y los datos informáticos. Posada Maya, Ricardo, "Una Aproximación a la Criminalidad informática en Colombia", ci., pp. 16 y ss.

de activos (C.P., artículo 269J). Se trata de verbos típicos caracterizados por superar las simples actuaciones informáticas del autor-usuario[58], y que exigen para su consumación *resultados inmateriales que suponen una modificación lógica de los objetos* sobre los cuales recae la acción criminal, naturalmente dentro de los sistemas informáticos, en la web o en medios de almacenamiento como la nube (*cloud computing*)[59]. Cambios virtuales que admiten aplicar dispositivos amplificadores como la tentativa (CP, artículo 27) y que pueden ser perfectamente *desistidos* por el atacante, en la medida en que domine el sistema de tratamiento de información.

En fin, se trata de resultados que no han sido plenamente desarrollados por la doctrina o que ha sido asimilado a los resultados tradicionales, pero que representan amenazas o lesiones colectivas e incluso masivas y de efectos catastróficos, pues una acción de esta naturaleza puede afectar a miles de usuarios en forma simultánea y automática[60]. Incluso hoy se habla del uso estratégico del internet en los conflictos armados y su limitación efectiva por parte del DIH[61].

6. Nexo de causalidad. Este aspecto objetivo del tipo también resulta polémico a partir de una simple pregunta: ¿qué relevancia puede tener una figura de naturaleza ontológica como el nexo de causalidad en el ámbito de una realidad simulada, que tiene existencia virtual dentro de computadores y redes informáticas? ¿Es necesario hablar de nexo de causalidad cuando muchos de estos delitos –como se dijo antes– en realidad producen resultados de naturaleza lógica o virtual? La respuesta no es sencilla, pero parece evidente que, en principio, la función de esta categoría es muy reducida. Y

58 Por el contrario, se advierten simples conductas en los eventos de acceso (o mantenimiento) a sistemas informáticos protegidos o no con medidas de seguridad (C.P, artículo 269A); la obstaculización del funcionamiento normal a un sistema informático o los datos informáticos allí registrados (C.P, artículo 269B); el tráfico, adquisición, distribución, venta, envío, introducción o extracción del territorio nacional de software malicioso u otros programas de efectos dañinos (C.P, artículo 269E); la compilación, ofrecimiento, venta, intercambio, envío, compra, divulgación y empleo de códigos o datos personales contenidos en ficheros, archivos o bases de datos (C.P, artículo 269F); el diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes sin estar facultado para ello (C.P, artículo 269G). Velásquez Velásquez, Fernando, *Fundamentos de derecho penal, parte general,* cit., p. 358, se trata de comportamientos "en los cuales al legislador no le interesa la producción de un resultado exterior". Suárez Sánchez, Alberto, *Manual de delitos informático en Colombia,* cit., p. 137, enlista los que a su entender son ciberdelitos de mera conducta.

59 Por su parte, Suárez Sánchez, Alberto, *Manual de delitos informático en Colombia,* cit., p. 137, los califica como delitos de resultado o de causación a secas, como delitos de detrimento a los datos o generadores de perjuicio para el bien jurídico.

60 Silva Sánchez, Jesús María, *La expansión del derecho penal, Aspectos de la Política Criminal en las sociedades postindustriales,* Editorial B de F, Buenos Aires, 2ª Edición, 2006, pp. 27 y 28.

61 Ambos, Kai, "Responsabilidad penal internacional en el ciberespacio" en *Cuadernos de Conferencias y artículos,* Vol. 47, Universidad Externado de Colombia, 2015, pp. 301-342.

ello es así, pues incluso contradiría su misma esencia al trabajar con hipótesis posibles de algoritmos en una realidad simulada.

Así las cosas, con el nacimiento de la *ciberacción* y la existencia de resultados lógicos e inmateriales, se puede constatar cómo en algunas de las modalidades de cibercrimen pierde relevancia el *nexo de causalidad tradicional*, como nexo natural de pertenencia entre la acción y el resultado material (o de otra índole)[62]. Por ello, algún sector de la doctrina considera que, más allá del *Clic* causal que propicia la acción informática, en los cibercrímenes es necesario determinar la existencia de *una conexión de naturaleza lógica y técnica entre el agente-usuario (cibernauta) y la infraestructura tecnológica*: "Esto es, un dialogo lógico entre el autor y el sistema informático consistente en la interacción *input-output* (instrucciones electrónicas respuestas por la máquina) dirigidas a manipular el sistema [...]"[63] y a producir un impacto tecnológico, la modificación o manipulación de los datos o de las funciones informáticas que se llevan a cabo sobre ellas. Como es evidente, dicho nexo lógico complementa el ontológico cuando sea necesario de cara a la estructura del tipo penal correspondiente.

En una reflexión de orden general, no se trata de establecer una relación de dependencia analógica o física entre una acción y un determinado resultado material, sino de determinar la relación de dependencia entre la *ciberacción* y el resultado cibernético, a partir del concepto fundamental de *conexión virtual*. La conexión lógica o digital es en realidad una clase de comunicación, por medio de la cual se transmiten datos como instrucciones o archivos, a través de canales o líneas informáticas preestablecidas (cable, satélite, redes inalámbricas, LMDS o *Local Multipoint*

62 Berruezo, *Delitos de dominio y de infracción del deber,* cit., p. 159; Cuello Contreras, *El Derecho Penal español,* cit., pp. 581 y ss.; Engisch, Karl, *La causalidad como elemento de los tipos penales,* Hammurabi, 2008, p. 19 y ss.; Fernández Carrasquilla, Juan, *Derecho Penal, Teoría del delito y de la pena,* cit., pp. 145 y ss., 163 y ss.; Jescheck, Hans-Heinrich y Weigend, Thomas, *Tratado de Derecho Penal, Parte General,* Granada, Comares, 1993, pp. 297 y ss.; Martínez Rincones, José F., *Causalidad y derecho penal: Una Reflexión Hermenéutica, Imputación objetiva y Dogmática Penal*, 2005, pp. 71 y ss.; Maurach, Reinhart,/ Gössel, Karl Heinz / Zipf, Heinz, *Derecho Penal,* Tomo 1, cit., pp. 306 y ss., 310 y ss.; Luzón Peña, Diego, *Lecciones de Derecho penal, parte general,* cit., pp. 335 y ss.; Muñoz Conde, Francisco/García Arán, Mercedes, *Derecho Penal,* cit., pp. 240 y 247; Roxin, *Derecho Penal, Parte General,* Tomo 1, cit., pp. 345 y 346; Salazar Marín, *Acción e imputación, Principio y concepto de culpabilidad, Escuela dialéctica del derecho penal*. Bogotá, Ibáñez, 2016, pp. 22 y 23; Welzel, Hans, *Derecho Penal alemán,* cit., pp. 50 y ss.; Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., pp. 360 y ss.; Zaffaroni, Eugenio Raúl, Alagia, Alejandro y Slokar, Alejandro, *Derecho penal,* cit., pp. 458-460.

63 Posada Maya, Ricardo, "Interceptación informática y violación de datos personales", cit., pp. 229 y 239; id., "El delito de transferencia no consentida de activos", cit., p. 236. Por su parte, Suárez Sánchez, Alberto, *Manual de delitos informático en Colombia,* cit., pp. 383 y 384, solo habla de nexo causal tratándose de la transferencia no consentida de activos, mientras que en los demás delitos no hace ningún tipo de referencia a ellos, por considerar que se trata, en su mayoría, de conductas de mera conducta que incluso admiten tentativa desde una perspectiva normativa.

Distribution System) entre un emisor y un sistema receptor que las procesa.

En cuanto a la *imputación objetiva*[64], si bien los niveles de análisis de esta forma de imputación del resultado jurídico al autor no cambian, es necesario tener en cuenta que los riesgos que se aportan y que deben ser desvalorados en concreto, deben ser de aquellos que puedan tener existencia en el ciberespacio y producir efectos idóneos en el mundo digital, directamente o como efecto lógico de los procesos de tratamiento de datos o información por medio los de sistemas informáticos.

La cuestión no es meramente formal, el reto de esta institución jurídica frente a los cibercrímenes consiste en perfeccionar los distintos niveles necesarios para acreditar sus elementos normativos. Por ejemplo: al ser el ciberespacio un medio desregulado, no siempre es claro cuándo un sujeto aporta un riesgo desaprobado real para los datos y la información (o para los sistemas informáticos). Por ejemplo, en nuestro medio no siempre es sencillo determinar, en términos técnicos, si ciertas actividades como ocurre con el análisis de vulnerabilidades o el escaneo de puertos de un equipo, realizados usualmente por ingenieros informáticos, son realmente desaprobadas, pues es dudoso si se trata de actos preparatorios para realizar otras conductas como el acceso abusivo, un sabotaje o de actividades neutrales. De igual manera, no es fácil precisar qué es o no tolerable jurídicamente en el ciberespacio, porque todavía es un tema en construcción que se dificulta cuando el legislador penal utiliza: a) técnicas de tipificación basadas en delitos de mera conducta y peligro en abstracto[65]; b) exceso de elementos normativos al redactar los tipos penales o demasiados verbos típicos al momento de determinar las conductas prohibidas, que mezclan hipótesis de mera conducta y de resultado, adoptando regímenes dogmáticos incluso incompatibles entre sí.

Los riesgos informáticos abren, por consiguiente, un nuevo espectro de análisis para la imputación objetiva. Otro ejemplo sería la limitada operatividad de figuras como la autopuesta en peligro, que en materia informática media entre el deber (y regla) de autoprotección informática de los datos y los sistemas informáticos y el derecho a la inviolabilidad de la intimidad, institución que en delitos como el acceso abusivo a sistema informático se ha evitado sin matices, al eliminar la exigencia de protección

64 Luzón Peña, Diego, *Lecciones de Derecho penal, parte general,* cit., 350 y ss.; Roxin, *Derecho Penal, Parte General,* Tomo 1, cit., pp. 362 y ss.; Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., pp. 364 y ss.

65 Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", cit., p. 217. Agrega Satzger, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia", p. 26, que "En definitiva, la regulación colombiana me parece demasiado amplia en cuanto a la punibilidad de actos preparatorios, por lo demás, el legislador colombiano supera claramente las obligaciones del artículo 6 del Convenio de Budapest".

de los sistemas con medidas de seguridad[66].

7. El dolo. Los cibercrímenes en Colombia conservan la estructura tradicional del dolo como conocimiento y voluntad (CP, artículo 22)[67], a pesar de lo cual, no es extraño que surjan dudas sobre sus requisitos, especialmente cuando se ha constatado la posibilidad de realizar el delito mediante acciones virtuales, automáticas y programadas total o parcialmente por el autor. Por ejemplo, cabe preguntarse si en los cibercrímenes es viable (a pesar de la necesidad) acreditar el conocimiento actual o actualizable del sujeto al momento de la ejecución del verbo típico, cuando esta es realizada de manera automática por dispositivos informáticos, o ¿si basta la previsión de los efectos lógicos que se desprenden de la acción física previa (con casi absoluta certeza), cuando es claro que estos han sido predeterminados en la programación del tratamiento de los datos o la información? Naturalmente estos problemas serán excepcionales, pues lo ordinario en los delitos informáticos supondría reconducir el dolo, como en los delitos tradicionales, al conocimiento actual o actualizable y a la voluntad (realizadora) del autor-usuario al momento de introducir las instrucciones que le permitirán manipular el sistema y producir la respectiva acción informática o el resultado lógico que ha sido previsto[68]. En cualquier caso, lo cierto es que dicha postura reafirma la involuntariedad y la confianza ciega del autor en que el sistema informático realizará aquellos ataques para los cuales fue programado. El problema planteado no existe, desde luego, cuando la manipulación del sistema sea en tiempo real.

8. El dominio del hecho y la autoría. También la teoría del dominio del hecho merece plantear algunas inquietudes de cara a estas fenomenologías criminales. Según la doctrina más aceptada[69], será autor con dominio del hecho en los delitos comisivos de resultado, aquel sujeto que realice por sí mismo todos los elementos del correspondiente tipo penal, siendo el protagonista (en términos objetivos y subjetivos)

66 Posada Maya, Ricardo, "El delito de acceso abusivo a sistema informático: a propósito del Art. 269A del CP de 2000" en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* 2013, pp. 131-132.

67 Luzón Peña, Diego, *Lecciones de Derecho penal, parte general,* cit., pp. 391 y ss.; Posada Maya, Ricardo, "El dolo en el Código Penal del 2000", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* 2009, pp. 5 y ss.; Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., pp. 389 y ss.

68 Stratenwerth, Günter, *Derecho Penal,* cit., p. 149.

69 Díaz y García Conlledo, Miguel, y Luzón Peña, Diego, *La autoría en Derecho penal*, Promociones y Publicaciones Universitarias (PPU), España, 1991, pp. 472 y ss.; Fernández Carrasquilla, Juan, *Derecho Penal, Teoría del delito y de la pena,* cit., pp. 829 y ss.; Mir Puig, *Derecho Penal: Parte General,* cit., pp. 383 y ss.; Roxin, Claus, *Autoría y dominio del hecho en derecho penal,* 7ª Edición, Editorial Marcial Pons, 2000, pp. 151 y ss., 359 y ss.; *Derecho Penal, Teoría del delito y de la pena*, Tomo 2, pp. 80 y ss.; Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., pp. 572 y ss.

en la realización del delito[70]. Bastaría para tales efectos determinar que el autor-usuario (conectado) ha tenido una influencia informática (una interacción o dominabilidad) determinante en el transcurso del tratamiento de datos e información y el resultado lógico a partir de su voluntad final[71]. Sin embargo, en este contexto no parece claro que el autor siempre sea quien realice (por completo o parcialmente) la acción principal en la realidad virtual o simulada, pues gran parte de ella puede ser realizada de manera autónoma y automática por parte del sistema informático, aunque el comportamiento virtual en realidad le sea imputable en el plano físico al autor-usuario que domina positiva y objetivamente la infraestructura[72].

En todo caso, hay que advertirlo, uno de los errores más comunes a la hora de verificar la autoría en este tipo de infracciones es menospreciar, como ya se ha señalado, el importante papel que juega el sistema informático al asimilarlo a un simple instrumento físico, pues de no existir su función virtual se excluiría la tipicidad de estos comportamientos delictivos (al no existir la tríada informática). Con todo, el diseño teórico variará sustancialmente mientras más autonomía tengan los entes (androides, bots, etcétera) en la ejecución de los comportamientos criminales.

En síntesis, en la esencia de los cibercrímenes, que no parecen ser delitos de infracción al deber, se encuentra la posible precisión sobre la teoría del dominio del hecho para determinar quién es (ciber) autor. Una consideración más precisa demuestra que, si únicamente pueden ser autores los usuarios informáticos (legítimos o ilegítimos, sin que se trate de delitos especiales o de propia mano), y bajo el entendido que los delitos informáticos en sentido estricto solo pueden tener lugar mediante sistemas automatizados individuales o en redes en el *ciberespacio*, se puede concluir que el dominio del hecho en los cibercrímenes no podría ser solo físico sino también (y por definición) lógico, materializado de manera objetiva y positiva a partir de la conexión virtual que permite materializar la voluntad (dominar) sobre el sistema mediante instrucciones informáticas muy precisas. Únicamente a través de la conexión virtual el sujeto-usuario adquiere y conserva la dirección final[73] o el control total o parcial (no solo potencial) del sistema informático que le permite decidir autónomamente el sí y el cómo éste ejecuta el hecho virtual, entendido el comportamiento complejo como un proceso de tratamiento de información que termina por producir el resultado lógico o inmaterial.

En los casos en los que los cibercrímenes puedan ser realizados por fuera del

70 Díaz y García Conlledo, Miguel y Luzón Peña, Diego, *La autoría en Derecho penal,* cit., pp. 472 y ss.

71 Roxin, Claus, *Autoría y dominio del hecho en derecho penal,* cit., pp. 338 y ss.

72 Díaz y García Conlledo, miguel y Luzón Peña, Diego, *La autoría en Derecho penal,* cit., p. 542.

73 Maurach, Reinhart,/ Gössel, Karl Heinz / Zipf, Heinz, *Derecho Penal,* Tomo 2, Editorial Astrea, 1995, pp. 317 y ss.

sistema informático (como cuando exijan la producción de un resultado físico o una determinada acción como compra, venta u ofrecimiento de datos o software malicioso), se aplicarán las categorías convencionales de dominio del hecho y la voluntad con sus correspondientes correctivos[74].

A lo anterior habría que señalar otra dificultad dogmática. Muchos de los cibercrímenes hoy son realizados por verdaderas organizaciones virtuales transnacionales (OVT) como bandas, organizaciones e incluso empresas criminales[75] (no necesariamente aparatos organizados de poder), en la medida en que el dominio informático derivado de la conexión virtual pertenece a varias personas que intervienen de común acuerdo según su especialidad (o mercado) o su función dentro de la respectiva organización criminal, de acuerdo con las políticas o los diseños criminales elaborados por ésta. La misma forma específica de la organización y su manera de actuar dificulta sobre manera, por ejemplo, la determinación de la responsabilidad de los dirigentes de la organización que no participan directamente en el hecho[76] y que, claramente, no han tenido el dominio específico de la ejecución de la acción cibercriminal, aunque lo aprueben de manera posterior, por no contar con una conexión directa con los sistemas informáticos.

9. Otras figuras. La pena. Finalmente, uno de los temas que difícilmente puede ser tratado con el suficiente rigor en estas pocas líneas es el de las penas o medidas de seguridad que se requieren en la transición de una sociedad prevalentemente analógica a una sociedad digital. La transformación jurídica que suponen los cibercrímenes respecto a la intervención del *ius puniendi* del Estado plantea la posibilidad de cuestionar, en términos preventivos generales y especiales[77], la eficacia (*ex ante*) de las penas tradicionales como la prisión en este tipo de conductas punibles. Todo indica que existen otras modalidades de restricciones de derechos (distintas a la privación de la libertad e incluso las penas pecuniarias) que pueden prevenir y de manera mucho más eficaz esta clase de actividades criminales como, por ejemplo, las *inhabilitaciones especiales* que le imposibiliten al autor conectarse virtualmente con el sistema informático o con la web (y con ello dominar el sistema o adquirir la posibilidad de manipularlo), para realizar en calidad de usuario conductas lesivas o peligrosas contra la seguridad de la información, los datos y los sistemas informáticos

74 Díaz y García Conlledo, Miguel y Luzón Peña, Diego, *La autoría en Derecho penal,* cit., pp. 512-514.

75 Roxin, Claus, *Autoría y dominio del hecho en derecho penal,* cit., p. 729; id., *Derecho Penal, Parte General,* Tomo 2, Editorial Civitas, España, 2014, p. 125.

76 Muñoz Conde, Francisco y García Arán, Mercedes, *Derecho Penal,* cit., pp. 480 y ss.

77 Hassemer, Winfried, *Viejo y nuevo derecho penal,* cit., p. 15.

(e incluso cometer delitos tradiciones por esta misma vía). De igual manera, en este amplio abanico de posibilidades se podrían contemplar algunas penas restrictivas diseñadas para que los ciudadanos, inclusive, no puedan obtener servicios de internet por parte de los proveedores nacionales o internacionales, para ejercer profesiones de naturaleza informática (CP, artículo 269H, numeral 8[78]), entre otras posibilidades cuyo diseño legislativo depende de los avances tecnológicos.

En esta línea, la incorporación legal de nuevas sanciones punitivas tiene dos retos fundamentales: *el primero*, que se trate de penas realmente controlables por parte del Estado, que al tiempo sean eficaces en tiempo real. Este quizá es el problema más difícil de solucionar, debido a la insuficiencia de capacidades técnicas para lograrlo. Probablemente en el futuro la biometría o los controles por vía del ADN permitan desarrollar técnicas de control para los criminales que garanticen un espacio virtual seguro para la sociedad y los usuarios. El *segundo reto*, y no por ello el menos importante, es lograr que este tipo de restricciones de derechos (informáticos) no afecten de manera desproporcionada e irrazonable los derechos constitucionales fundamentales de los ciudadanos o generen "consecuencias invisibles" y denigrantes para la dignidad humana (principio de indemnidad personal como consecuencia de la exigencia de humanidad de las penas[79]), pues, por esta vía, se podría incluso llegar a generar una muerte comunicativa para los ciudadanos (similar a la muerte civil), o controles desproporcionados al estilo "Gran hermano" en un marco de "colectivismo burocrático", como sucedió en la clásica y distópica novela "1984" del autor Inglés George Orwell, en la cual la intimidad, la dignidad y la imposibilidad de autodeterminación marcan una socialización absolutamente inviable.

78 CP, artículo 269H, núm. 8: "Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales" (cursivas por fuera del texto original). Sobre la gravedad de este tipo de penas se pronuncian Jescheck, Hans Heinrich/Weigend, Thomas, *Tratado de Derecho Penal,* p. 894 al afirmar que "[…] la mayoría de las veces priva al autor de su sustento económico dificultando con ello sustancialmente su resocialización, la inhabilitación profesional se presenta entonces como una medida sumamente drástica que solo puede ser admisible para evitar graves peligros que acechan a la colectividad".

79 Velásquez Velásquez, Fernando, *Fundamentos de derecho penal,* cit., pp. 662. También se desprende de lo dicho la necesidad de conservar la exigencia de necesidad que se deriva del CP, artículo 3, en el sentido de que debe reportar el mínimo daño posible para el condenado, en el marco del programa preventivo que diseñe el legislador de acuerdo con los principios constitucionales.

3. Conclusiones

1. El cambio social ha determinado el surgimiento de nuevos riesgos que se materializan en nuevas fenomenologías criminales. Los cibercrímenes representan, justamente, el nacimiento de comportamientos que, en su sentido puro, como delitos informáticos en sentido estricto, tienen lugar en realidades virtuales o simuladas como el ciberespacio, protegen objetos inmateriales como los datos y la información y tutelan nuevos bienes jurídicos intermedios. Si a ello se suma el hecho de que estos delitos son realizados mediante técnicas particulares (que en muchos casos consisten en la manipulación de energía o *bytes* basados en sistemas binarios, que pueden ser traducidos a los humanos mediante infraestructuras informáticas o Hardware), se aprecian delitos que distan mucho de ser asimilables a los delitos tradicionales.

2. Los cibercrímenes o delitos informáticos en sentido estricto se deben distinguir de los delitos comunes que son realizados por medio de sistemas informáticos o telemáticos. Los segundos suponen la existencia de tipos penales que protegen, en primera instancia, bienes jurídicos clásicos como el patrimonio económico, la honra, la integridad personal o formación sexual, la autonomía personal, etcétera (extorsiones, estafas, injurias utilizando redes sociales o el correo electrónico) y solo de manera secundaria protegen la seguridad de la información, los datos, los sistemas informáticos o las funciones informáticas (por el contrario, como sucede en el daño informático o en la obstaculización de sistemas informáticos ante conductas, por ejemplo, de denegación de servicios, el legislador pretende proteger de manera principal la seguridad de la información). Tampoco en los delitos informáticos son inherentes las características del cibercrimen, es decir, la posibilidad de realización de la acción sin intervención humana directa sobre el titular de los datos, o la afectación principal de las funciones informáticas (más allá del simple uso de los sistemas informáticos) y la virtualidad de los efectos. El mismo CP de 2000 distingue ambas modalidades, cuando en el artículo 58, numeral 17 (Ley 1273 de 2009, artículo 2), agrava los delitos comunes que utilicen medios informáticos, electrónicos o telemáticos. En los cibercrímenes, el ciberespacio y los medios informáticos no se pueden considerar como simples "medios ejecutivos", sino que son el ámbito digital en donde tiene lugar la realización lógica del delito.

3. Estas diferencias demuestran que la protección de las funciones informáticas como sustrato material del bien jurídico seguridad de la información (confidencialidad/confiabilidad, integridad, disponibilidad, no repudio y recuperación de información almacenada), marcan una diferencia esencial. En efecto, se trata de proteger un bien jurídico dinámico que exige cambios o mejoras en las estructuras formales y materiales de la tipicidad 'analógica', es decir, en los requisitos objetivos y subjetivos

que debe cumplir una acción física que usualmente tiene lugar y causa efectos en el mundo exterior. El primer cambio perceptible es el fortalecimiento de la ciberacción (o más bien de la interactuación virtual en el ciberespacio, como ámbito deslocalizado y desregulado que dificulta la determinación del tiempo y lugar de los delitos), entendida como aquella acción virtual, interactiva/reactiva, automática, programable, masiva, anónima, etcétera, que involucra la introducción de instrucciones lógicas por parte de un autor-usuario a un sistema informático o telemático con el fin de tratar información. Cuando se transforma la naturaleza de la acción se define de manera distinta la percepción del delito y su propia dinámica de ejecución.

4. El cambio en la acción produce varios efectos evidentes, que deben ser estudiados ampliamente por parte de la doctrina nacional:

a) ¿Quiénes son realmente los autores de los cibercrimenes? Sobre el particular se ha dicho que no se trata de simples sujetos físicos, sino de sujetos que tengan además la calidad de usuarios, es decir, que actúen bajo una conexión de naturaleza virtual con el sistema informático, que les permita dominar el tratamiento de información que realiza el sistema o la infraestructura, o impedir que los procesos que éste ejecuta se realicen de manera satisfactoria. El concepto de conexión virtual, así como el empleo de una cierta identidad digital, adquieren especial importancia en estas figuras criminales para acreditar el sujeto con suficientes privilegios para realizar la acción en el ciberespacio de manera idónea.

b) Si bien no todos los cibercrímenes tienen efectos en el mundo virtual (porque los tipos requieren efectos adicionales en el mundo exterior o porque son simples acciones), en la gran mayoría de ellos se exigen resultados o modificaciones inmateriales sobre objetos lógicos que no son perceptibles por los sentidos. Sin embargo, como no ocurren en el mundo físico, es necesario complementar el nexo de causalidad natural (cuando este sea necesario) con un nexo lógico o virtual determinado por las instrucciones de programación del autor para producir los efectos que han sido predeterminados por el Software y la decisión final del autor. Dicho nexo lógico, como ha quedado dicho, depende entonces del concepto de conexión directa o remota con los sistemas. Lo que además puede comportar la suplantación del verdadero titular de los datos, del sistema o de los usuarios autorizados para interactuar con estos.

c) De igual manera, la interactuación en el ciberespacio a través de los sistemas informáticos implica verificar, en cada caso, la existencia de requisitos tradicionales en materia del conocimiento del dolo, particularmente frente a acciones programables y automatizadas. Recuérdese que estas acciones son realizadas por sistemas informáticos programados o inteligentes (inteligencia artificial). También ese necesario

evaluar los conceptos materiales que permiten afirmar la autoría, como sucede con las teorías del dominio objetivo y positivo del hecho que, de nuevo, deben centrarse sobre el dominio lógico de los sistemas informáticos, mediante instrucciones o programaciones cuyos efectos pueden ser tanto virtuales como físicos. La idea, en todo caso, es no subestimar en esta clase de delitos el papel que juegan los instrumentos informáticos en las realidades simuladas, porque no es claro que un simple *Clic* causal sea equiparable a la ejecución completa y directa de todo el cibercrimen, aunque esta realización le deba ser imputada al autor-usuario.

5. Finalmente, parece necesario y relevante complementar las categorías tradicionales del delito en la tipicidad, con una perspectiva digital que, por cierto, ya no es la excepción a la regla sino que comienza a ser la regla general en la criminalidad moderna. Esto incluso en ámbitos hasta ahora reservados a la criminalidad física, como la criminalidad organizada y transnacional, que comienza a actuar mediante organizaciones virtuales transnacionales (OVT) que dificultan aún más combatir este tipo de delincuencia sin fronteras.

Bibliografía

Ambos, Kai. "Responsabilidad penal internacional en el ciberespacio", En: *Derecho penal y nuevas tecnologías.* A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 301-342.

Asimov, Isaac. "El Hombre Bicentenario", En: *Cuentos completos* II, Barcelona, Ediciones B, 2005 pp. 656 y ss.

Berruezo, Rafael. *Delitos de dominio y de infracción del deber*, 2ª edición, Montevideo-Buenos Aires, BdeF, 2016.

Cano Martínez, Jeimy. *Manual de un Chief Information Security Officer*, En Reflexiones no convencionales sobre la gerencia de la seguridad de la información en un mundo VICA (volátil, incierto, complejo y ambiguo), Bogotá, Ediciones de la U, 2016.

Castells, Manuel. *La era de la información*, Vol. 1: La sociedad red, Madrid, Alianza Editorial, 2001.

Corcoy Bidasolo, Mirentxu. *Delitos de peligro y protección de bienes jurídico-penales supraindividuales: nuevas formas de delincuencia [sic] y reinterpretación de tipos penales clásicos*, Valencia, Tirant lo Blanch, D.L. 1999.

Cuello Contreras, Joaquín. *El Derecho Penal español, Parte General*, 3ª ed., Madrid, Dykinson, 2002.

De La Cuesta Arzamendi, José Luis (Dir.) y De La Mata Barranco, Norberto J. (Coord.). *Derecho penal informático*, Madrid, Civitas-Thomson Reuters, 2010.

Delitala, Giacomo. *El "Hecho" en la teoría general del delito*, Maestros del Derecho Penal No. 29, Montevideo-Buenos Aires, BdeF, 2009.

Díaz y García Conlledo, Miguel. *La autoría en Derecho penal*, 2ª ed., Santiago, EJS, 2014.

Durham, Cole. "The emerging structures of criminal information law: tracing the contours of a new paradigm", En: Ulrich Sieber (Ed.). *Information, Technology, Crime.* National legislation and international initiatives, Ius informationis, Vol. 6, Köln-Berlín-Bonn-München, Heymann, 1994, pp. 533 y ss.

Fernández Carrasquilla, Juan, *Derecho Penal, Parte General*, Principios y categorías dogmáticas, Bogotá, Ibáñez, 2011.

Fernández Carrasquilla, Juan, *Derecho Penal, Parte General, Teoría del delito y de la pena*, Vol. 1, El delito, Bogotá, Ibáñez, 2012.

Fernández Carrasquilla, Juan, *Derecho Penal, Parte General, Teoría del delito y de la pena*, Vol. 2, Teoría del delito y de la pena, Dispositivos amplificadores concursos y pena, Bogotá, Ibáñez, 2012.

Fernández Carrasquilla, Juan, *Derecho Penal*, Principios y categorías dogmáticas, Ibañez, Bogotá, 2011

Fernández García, Emilio Manuel. "Fraudes y otros delitos patrimoniales relacionados con la informática e internet", en: *Estudios Jurídicos*, IV, Madrid, Consejo General del Poder Judicial, 1999, pp. 387-447.

Frisch, Wolfgang. *La imputación objetiva del resultado*, Desarrollo, fundamentos y cuestiones abiertas, Estudios preliminar de Ricardo Robles Planas, Traducción de Ivó Coca Vila, Barcelona, Atelier, 2015.

Galán Muñoz, Alfonso. *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P.*, Valencia, Tirant lo Blanch, 2005.

Gracia Martín, Luis, *Prolegómenos,* Madrid, Civitas, 2001.

Gutiérrez Francés, María Luz, "La privacidad en el espacio virtual (riesgos y cauces de protección)", en *Cuadernos de la Cátedra de Seguridad Salmantina*, Nº. 3, 2011.

Gutiérrez Francés, María Luz, *Fraude informático y estafa. Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos*, Madrid, Ministerio de Justicia, 1991.

Gutiérrez Francés, María Luz. "Delincuencia económica e informática en el nuevo Código Penal", En: *Ámbito jurídico de las tecnologías de la información*, Miguel Ángel Gallardo Ortiz (Dir.), Consejo General del Poder Judicial, Madrid, 1996, pp. 249-305.

Hassemer, Winfried. "Viejo y nuevo derecho penal", En: *Persona, mundo y responsabilidad*, Temis, Bogotá, 1999, pp. 15-38.

Jaén Vallejo, Manuel. *El concepto de acción en la dogmática penal*, Madrid, Colex, 1994.

Jescheck, Hans Heinrich/Weigend, Thomas. *Tratado de Derecho Penal, Parte General,* Miguel Olmedo Cardenete (trad.), 5ª ed., Granada, Comares, 2002.

Lezertua, Manuel. "El proyecto del convenio sobre el Cybercrimen del Consejo de Europa", En: López Ortega, Juan José (Dir). *Internet y derecho penal*, Cuadernos de Derecho judicial X, Madrid, Consejo General del Poder Judicial, 2001, pp. 15-62.

Luzón Peña, Diego Manuel. *Derecho penal, Parte general*, 3ª ed., ampliada y revisada, Montevideo-Buenos Aires, BdeF, 2016.

Martínez Rincones, José Francisco. "Causalidad y derecho penal: Una reflexión hermenéutica", En: *Imputación objetiva y dogmática penal*, Mireya Bolaños González (Comp.), Mérida, Universidad de Los Andes Venezuela, 2005, pp. 71 y ss.

Mata y Martín, Ricardo M. *Bienes jurídicos intermedios y delitos de peligro*, Granada, Comares, 1997.

Matellanes Rodríguez, Nuria. "Algunas notas sobre las formas de delincuencia informática en el Código penal", En: *Hacia un Derecho penal sin fronteras*, Coord. María Rosario Diego Díaz-Santos y Virginia Sánchez López, XII Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2000, pp. 129-147.

Maurach, Reinhart; Gössel, Karl Heinz y Zipf, Heinz. *Derecho Penal, Parte General*, 2 vol., de Jorge Bofill Genzsch (trad.) 7ª ed. alemana, Buenos Aires, Astrea, 1994 y 1995.

Meek Neira, Michael, *Delito informático y cadena de custodia*, Universidad Sergio Arboleda, Bogotá, 2013.

Méndez Rodríguez, Cristina, *Los delitos de peligro y sus técnicas de tipificación*, Madrid, Universidad Complutense 1993.

Mir Puig, Santiago. *Derecho Penal, Parte General*, 10ª ed., Barcelona, Reppertor, 2016.

Mir Puig, Santiago. *Introducción a las bases del derecho penal*, Maestros del Derecho penal No. 5, Montevideo-Buenos Aires, BdeF, 2003.

Miró Llinares, Fernando. "La cibercriminalidad 2.0: falacias y realidades", En: *Derecho penal y nuevas tecnologías*. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 55-117.

Miró Llinares, Fernando. *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.

Morales García, Oscar. "Apuntes de política criminal en el contexto tecnológico. Una

aproximación a la convención del Consejo de Europa sobre Cybercrimen", En: *Delincuencia informática*. Problemas de responsabilidad, Oscar Morales García (Dir.), Cuadernos de derecho judicial IX-2002, Madrid, Consejo General del Poder Judicial, 2002, pp. 11-34.

Morón Lerma, Esther. "Nuevas tecnologías e instrumentos internacionales. Consecuencias penales", En: *Derecho penal y nuevas tecnologías*. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 33-54.

Muñoz Conde, Francisco/García Arán, Mercedes. *Derecho Penal, Parte General*, 9ª ed., Valencia, Tirant lo Blanch, 2015.

Pérez Luño, Antonio Enrique. *Manual de informática y derecho*, Barcelona, Ariel, 1996.

Pomante, Gianluca. *Internet e criminalità*, Aggiornato al D.Lg. 6 maggio 1999, n, 169, Torino, Giappichelli Editore, 1999.

Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", en Revista de *Derecho, Comunicaciones y Nuevas Tecnologías*, Bogotá, 2012.

Posada Maya, Ricardo. "El delito de trasferencia no consentida de activos", En: *Estudios de Derecho Penal* No. 2, Carlos Andrés Gómez González y Carlos Alberto Suárez López (Coords.), Universidad de Bogotá Jorge Tadeo Lozano, Facultad de Relaciones Internacionales y Ciencias jurídicas y Políticas, Bogotá, 2012, pp. 209–250. (Revista de Derecho, Comunicaciones y Nuevas Tecnologías n. 8, 2012).

Posada Maya, Ricardo. "Aproximación a la Criminalidad informática en Colombia", En: *Revista de derecho, comunicaciones y nuevas tecnologías*, núm. 2, Cijus-Gecti, Universidad de los Andes, Bogotá, 2006, pp. 13–60.

Posada Maya, Ricardo. "El delito de acceso abusivo a sistema informático", En: *Derecho Penal Contemporáneo*, Revista Internacional, No. 44, Bogotá, Legis, 2013, pp. 97-142.

Posada Maya, Ricardo. "El dolo en el Código Penal de 2000", en *Temas de Derecho Penal*, Ricardo Posada Maya (Coord.), Bogotá, Biblioteca Jurídica Uniandina, Facultad de Derecho-Ed. Temis, Universidad de Los Andes, 2008, pp. 1-74.

Posada Maya, Ricardo. "Libertad de información e independencia judicial", En: Discriminación, principio de jurisdicción universal y temas de derecho penal, Ricardo Posada Maya (Coord.), Bogotá, Uniandes, 2013, pp. 677-694.

Posada Maya, Ricardo. *Delito continuado y concurso de delitos.* Colección Ciencias Penales, Ricardo Posada Maya (Dir.), Bogotá, Ed. Uniandes-Ed. Ibáñez, 2012.

Remolina Angarita, Nelson. *Tratamiento de datos personales*, aproximación nacional y comentarios a la Ley 1581 de 2012, Bogotá, Legis, 2013.

Romeo Casabona, Carlos María. "Los datos de carácter personal como bienes jurídicos penalmente protegidos", En: AA.VV. *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Carlos María Romeo Casabona (coord.), Estudios de derecho penal y criminología núm. 78, Granada, Comares, 2006, pp. 167 a 190.

Romeo Casabona, Carlos María. "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", En: AA.VV. *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Carlos María Romeo Casabona (coord.), Estudios de derecho penal y criminología, núm. 78, Granada, Comares, 2006, pp. 3 y ss.

Rovira del Canto, Enrique, "Hacia una expansión doctrinal y fáctico del fraude informático" en *Revista Aranzadi de derecho y nuevas tecnologías*, Nº3, 2003.

Rovira Del Canto, Enrique. *Delincuencia informática y fraudes informáticos,* Estudios de Derecho penal No. 33, (Dir.) Carlos María Romeo Casabona, Comares, Granada, 2002.

Roxin, Claus. *Derecho Penal, Parte General*, t. 2, Especiales formas de aparición del delito Madrid, Civitas, 2014

Roxin, Claus. *Derecho Penal, Parte General*, t. i, Madrid, Civitas, 1997.

Roxin, Claus. *Imputación objetiva en el derecho penal,* 2ª ed., Manuel A. Abanto Vásquez (trad.), Lima, Grijley, 2012.

Salazar Marín, Mario. *Acción e imputación,* Principio y concepto de culpabilidad. Bogotá, Ibáñez, 2016.

Satzger, Helmut. "La protección de datos y sistemas informáticos en el derecho penal alemán Europeo. Tentativa de una comparación con la situación legal en Colombia", En: *Derecho penal y nuevas tecnologías.* A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 11 y ss.

Sieber, Ulrich, "Documentación para una aproximación al delito informático" en *Delincuencia informática,* 1992.

Sieber, Ulrich. *Computerkriminalität und Strafrecht.* Neue Entwicklungen in Technik und Recht, 2a ed., Köln-Berlin-Bonn-München, Heymanns, 1980.

Silva Sánchez, Jesús María. *La expansión del derecho penal.* Aspectos de la política criminal en las sociedades postindustriales, 2 ed., Madrid, Civitas, 2001.

Stratenwerth, Günter, *Strafrecht. Allgemeiner Teil I.* Die Straftat, 4 Auf., Köln/Berlin/Bonn/München, Heymanns, 2000. 5ª ed. de 2004 a cargo de Lothar Kuhlen. Hay traducción al castellano: *Derecho Penal, Parte General I, El hecho punible, tratados y manuales*, Manuel Cancio Meliá y Marcelo A. Sancinetti (trad. 4ª ed., 2000),

Thomson-Civitas, 2005.

Suárez Sánchez, Alberto. *Manual de delitos informático en Colombia.* Análisis dogmático de la ley 1273 de 2009, Bogotá, Universidad Externado de Colombia, 2016.

Tiedemann, Klaus, *Poder económico y delito*, Ariel, Barcelona, 1985.

Tiedemann, Klaus. "Criminalidad mediante computadoras", trad. de Amelia Mantilla viuda de Sandoval, En: *Nuevo Foro Penal* No. 30, octubre–diciembre de 1985, Bogotá, Temis, pp. 481 a 492.

Unión Internacional de Telecomunicaciones (UIT/ITU), *Undestanding Cybercrime: phenomena, challenges and legal response*, Ginebra, UIT, 2012. On line: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Unión Internacional de Telecomunicaciones (UIT/ITU). *El ciberdelito*, Guía para los países en desarrollo, División de aplicaciones TIC y cibercriminalidad, Departamento de Estrategias, Ginebra, UIT, 2009.

Velásquez Velásquez, Fernando, *Fundamentos de derecho penal. Parte General*, Bogotá, Andrés Morales, 2017.

Velásquez Velásquez, Fernando. "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos", En: *Derecho penal y nuevas tecnologías*. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), Bogotá, Universidad Sergio Arboleda, 2016, pp. 353-382.

Von Liszt, Franz. *Tratado de derecho penal*, Trad. De la 20 ed. alemana por Luis Jimenez de Asúa y adicionado con el Derecho Penal Español por Quintiliano Saldaña, T. 2, 2 ed., Madrid, Reus, 1927.

Wall, David S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity Press, 2007.

Wall, David, "Criminalizing cyberspace: the rise of the Internet as a 'crime problem'", En: Yvone Jewkes/Madij Yar, *Handbook of Internet Crime*, U.K., William Publishing, 2010, pp. 22-103.

Welzel, Hans. *Derecho Penal alemán*, Parte General, 11 ed. Alemana y 4ª Castellana, Juan Bustos Ramírez y Sergio Yáñez P. (trads.), Santiago, Jurídica de Chile, 1997.

Zaffaroni, Eugenio Raúl y Alagia, Alejandro/Slokar, Alejandro, *Derecho Penal, Parte General*, 2ª ed., Ediar, Buenos Aires, 2002.

Zagrebelsky, Gustavo, *El derecho dúctil. Ley, derechos, justicia*, 5ª edición, Editorial Trotta, Madrid, 2003.