EL DELITO INFORMÁTICO EN COLOMBIA: INSUFICIENCIAS REGULATIVAS

José Fernando Reyes Cuartas[*]

En frente de las necesidades de penalización de ciertas conductas que aparecen como lesivas de intereses comunes, se experimenta la actitud ambigua de si creer que el derecho penal debe ocuparse de ellas y en qué cantidad tendría que pretender incidir, con miras a lograr que el colectivo interiorizara el sentimiento de la prevención general. Este, particularmente, es una impresión que se experimenta en los diversos tópicos que expresa el llamado "derecho penal moderno". Y ello porque al amparo del modelo de Estado social y Democrático de derecho, las demandas de protección son altísimas, sin embargo, la necesaria consideración de criterios de proporcionalidad, obligan un uso racional del mecanismo sancionador. En los días que corren mucho se habla de la administrativización del derecho penal, para dar a entender que hechos disvaliosos que bien podrían ser tratados en sede de derecho administrativo, se trasladan al derecho penal por confiarse más en su se efectividad preventiva, convirtiendo de esa manera al *jus puniendi* en *prima et unica ratio*[1].

---

* Magistrado de la Sala Penal del Tribunal Superior de Manizales. Profesor de Derecho Penal en la Universidad de Caldas y de Derecho Disciplinario –Postgrado– en la Universidad Externado de Colombia. El autor quiere agradecer la colaboración en la revisión bibliográfica, efectuada por el Dr. JOSÉ MIGUEL RAMÍREZ JARAMILLO.

1 VID. MÁSSIMO DONINI, "¿Una nueva edad media penal? Lo viejo y lo nuevo en la expansión del derecho penal económico". En *Temas de derecho penal económico*. JUÁN M. TERRADILLOS-MARÍA ACALE SÁNCHEZ (Coords.). Madrid, Trotta, 2004, p. 201.

Es lo cierto que la alta complejización en la que discurre la vida moderna, y el elevado grado de valor otorgado a factores organizacionales, han exigido y exigen, respuestas punitivas a la vista, no ya de los daños materializados como resultado, sino de los peligros que ciertas conductas ofrecen para el mantenimiento de condiciones "normales" de vida en ciertos sectores, como es el caso de la fabricación y manipulación de artefactos químicos y en general la investigación en nuevas formas de energía, los efectos medioambientales de ciertas prácticas industriales, así como todo lo referente a los llamados derecho penal societario, derecho penal del mercado de valores, derecho penal del trabajo, las conductas observables dentro la llamada "nueva genética" y aquellas que tienen su auge en la globalizacion del mercado (lo que se ha dado en llamar la "criminalidad organizada") y cómo no, la llamada "*cibercriminalidad"* en la era de la sociedad globalizada[2].

La sociedad moderna ya depende en gran medida de sistemas automatizados, que controlan el tráfico terrestre y aéreo, la operatividad de ciertos servicios públicos domiciliarios, el discurrir de las personas en su vida de relación con pretensiones de crear ambientes de seguridad personal, y por supuesto, las operaciones bancarias, las comunicaciones personales, el entretenimiento[3]. Ya pocas diligencias hacemos cara a cara y todo se nos pide regularizarlo en formatos que obtenemos vía Internet.

Un tan alto nivel de dependencia de la *información* y de la *informática*, como el que se va alcanzado, ha justificado que el derecho penal se ocupe de ciertas conductas que se observan lesivas de intereses que, ciertamente, permiten y posibilitan las posibilidades de participación de las personas en su vida de relación. El advenimiento de la llamada *sociedad de riesgo* ha traído consigo una hiper inflación[4] del derecho penal, al punto que se ha convertido en paradigmático el delito imprudente. Con el progreso también ha venido una especie de mal presagio para la pervivencia del hombre, de allí que la preocupación apunte en la dirección de cómo prevenir los riesgos y en punto a lo que nos corresponde, la indagación es de qué manera y hasta dónde puede (y acaso debe) el derecho penal participar en esa tarea preventiva.

Pero como es fácil advertir, un tema tan absolutamente puntual y de una trasformación tan ágil –casi diaria— impide con mucho ser exhaustivos y actuales. Ello propicia, de

---

2 También se habla ahora de la "globalización de las comunicaciones"; cfr. JESÚS MARÍA SILVA SÁNCHEZ. "La política criminal y el derecho penal ante la globalización", en *La dogmática penal frente a la criminalidad en la administración pública*. Lima, Grijley, 2001, p. 62.

3 Esa es una realidad ya patente hace más de un cuarto de siglo, según lo relata MANFRED E. MÖHRENSCHLAGER en "El nuevo derecho penal informático en Alemania" (1986), en *Delincuencia informática.* Barcelona, PPU, 1992, p. 99

4 Al decir de C.J. MENDOZA BUERGO –*El derecho penal en la sociedad de riesgo,* Madrid, 2001, p. 24 ss–, uno de los puntos de criminalización, que han colaborado en la hipertrofia del derecho penal, al lado de las conductas alusivas al riesgo técnico-científico, a la manipulación genética, la manipulación de sustancias peligrosas, es el llamado *delito informático.*

una parte, el nacimiento de paraísos para el delito –por ausencia de regulación punitiva– y, de otra, el acudimiento a criterios de analogía y razonamiento extensivo, para llenar lagunas punitivas, lo que por supuesto resquebraja el principio "Estado social de derecho" al entrar así de manera decidida dentro del principio de legalidad, el cual se convierte en *rey de burlas*.

En lo que subsigue nos proponemos: (i) elaborar un planteamiento general sobre lo que ha dado en llamarse la sociedad de la información y los porqués justificativos de la vinculación del derecho penal a su protección en la sociedad moderna y globalizada (ii) los sectores en que la información y la informática, resultan relevantes para la regulación en sede de derecho penal (iii) las conductas de común regulación extranjera, en las citadas materias y (iv) lo que hoy se tiene en nuestro país según un criterio de comparación con lo ya descrito.

I. LA SOCIEDAD DE LA INFORMACIÓN

De los lugares comunes en que se afirmaba que la información significaba poder, hoy se ha pasado a decir que es la información ya, el centro del poder; el avanzar del hombre se marca –es un lugar común– con la invención de la rueda; prosigue con un segundo hito perceptible en la denominada "revolución industrial" y hoy asistimos a la *revolución* de los computadores.

Nada se hace sin ellos y pocas cosas son posibles sin su intermediación. Nos han acercado las fronteras; nos han hecho más dúctil la vida de relación pero asimismo, nos han colonizado porque nos han hecho dependientes de ellos. Vivimos en la era de la información[5] en la cual los datos, su creación, manipulación, transmisión y procesamiento se erigen en un nuevo y fundamental objeto jurídico, altamente valioso y de trascendencia mayúscula para la vida pacífica y organizada de las naciones.

Esto parece evidente y no son necesarias muchas razones para demostrarlo, pues a la vista tenemos su protagonismo, tanto desde las cosas elementales de la vida –por ej. la comunicación de una pareja de enamorados que vivan en dos extremos del mundo– como su rol en la organización, planeación y puesta en marcha de estrategias de guerra.

Para el derecho cobra especial importancia el asunto, si a la vista se tiene que con la manipulación de la información, vendrá no apenas la sofisticación de las delincuencias hasta ahora conocidas –por ejemplo las estafas[6]– sino además el surgimiento de nuevas

---

5 Sobre los conceptos "era electrónica", "era digital", "sociedad digital", y "era de la información", cfr. ENRIQUE ROVIRA DEL CANTO. *Delincuencia informática y fraudes informáticos*. Granada, Ed. Comares, 2002, p. 8 ss.

6 Cfr. "La estafa mediante computadoras en el Código Penal alemán (§236ª SGTB)", Urs KINDHÄUSER,

conductas que por su relevancia para la vida en común, exigirán por lo menos el que se discuta si es de su misión –del derecho penal– interesarse en ellas.

La llamada "globalización" significa –entre muchas cosas– el –de alguna manera– desvanecer las fronteras; la efervescencia del nuevo rey –el mercado– no alcanza siquiera confines menores si no es con la ayuda de la información que corre por la red –internet–; no sabemos si esto es el progreso, medido en cifras que no alcanzamos a imaginar y por ello entonces tampoco sabemos si el derecho penal, por ese solo hecho, tendría que acondicionar sus "herramientas de trabajo" o en todo caso, qué tanto debería hacerlo.

Con la globalización, nace también la complejización de las sociedades modernas, pues, al lado de ese ensancharse del mundo, la revolución tecnológica se erige en protagonista de primera línea. Y esto además porque –es ya un tópico decirlo– los asuntos del delito resultan incontrolables a nivel de un simple Estado[7]. Y con las tecnologías surgen los riesgos y con los riesgos nace la sensación de inseguridad, su hija primogénita. Y con esa palabra –"riesgos"– el libreto del Derecho penal se pone de patas arriba!

De la ilustración y sus principios que propugnan un Derecho penal mínimo –principio de necesidad– nace el concepto de bien jurídico y su pretensión reductora, que acude como paradigmático al modelo del injusto doloso de daño o lesión; con la llamada sociedad del riesgo, se erige ahora en emblemático, el delito imprudente de omisión! Se pretende entonces suplantar la necesidad de constatar la relación causal por la simple constatación probabilística, sin contar con la flexibilización de las garantías procesales.[8]

Y así, la anticipación de las barreras de protección, se convierten en la regla; todos somos ahora garantes de algo, en un ambiente en que la inseguridad, nos amilana[9]. Se asiste al funeral del bien jurídico, desmaterializado –por no decir, des-carnado– en el altar de la sociedad globalizada de los riesgos, construida por hombres intranquilos, presas del pánico y de la sensación de inseguridad.

Con todo, se puede observar con la proliferación de toda la literatura alusiva a la sociedad del riesgo, desde las obras de Beck, que no se ha tomado en cuenta que el devenir del hombre siempre y en todos sus momentos, ha estado signado por al existencia de

---

en Estudios de derecho penal económico. Santiago Mir Puig *et alt* (Coords.), Livrosca, Caracas, 2002, p. 649 ss.

7 Cfr. Mássimo Donini, "¿Una nueva edad media penal?... *cit.* . 198.

8 Esta es opinión de Carlos. J. Suárez González. "Derecho penal y riesgos tecnológicos", en *Crítica y justificación del derecho penal en el cambio de siglo.* Arroyo Zapatero et alt. (Coords.) Cuenca, edics. de la Univ. Castilla-La Mancha, 2003, p. 292.

9 Por ello una de las características de la llamada "sociedad del riesgo" es el incremento de la sensación de inseguridad por parte de la comunidad organizada que ve incrementada la llamada "sensibilidad al riesgo". Sobre ello cfr. Carlos. J. Suárez González. "Derecho penal y riesgos tecnológicos", en *Crítica y justificación* … cit., p. 291, 293.

serios riesgos para su pervivencia; su *sui géneris* existencia y naturaleza, depende de cada momento, como lo ha explicado Suárez G[10] –citando a Gil Calvo-– al mostrar cómo, desde hace doce mil años, los cazadores preagrícolas extinguieron la fauna del pleistoceno; hace 10 milenios la revolución agrícola inventó las epidemias contagiosas al crear las ciudades-estado neolíticas, y hace tres o cuatro milenios, los imperios hidráulicos, al trasformar los cursos fluviales, indujeron cambios climáticos.

En los estudios al uso en temas específicos referidos a la cibercriminalidad o, en todo caso, atinentes a la informática, hoy no sólo es problema bastante ya la tipicidad, sino el hallazgo de un referente material que sirva de bien jurídico, habida cuenta de la ideación de conductas fundamentalmente de peligro abstracto por motivo de la llamada sociedad de riesgo. Baste confrontar, para probar que ello es así, el estudio de Michael Bunzel, acerca de las limitaciones que deben imponerse a los procedimientos de encriptado de datos por la sofisticación alcanzada en ese procedimiento, lo cual impide la obtención de pruebas en el marco de una investigación con gastos técnicos justificables. Esa libertad de codificación merece especial limitación penal en punto de la utilización de procesos crípticos, en los cuales el bien jurídico se constituiría por la llamada "capacidad funcional de la Administración de Justicia penal"[11]!

Por ello hoy se asiste a la recreación del concepto de "delito informático", para ampliar su espectro, el cual se entiende reduccionista si apenas se le restringe a aquello referido a los sistemas de información, en la medida que lo que ahora importa con más vigor proteger, es el dato mismo y en general la fiabilidad en él y la seguridad de su conservación e indemnidad. Por ello también se pretenden tipificar las conductas, a partir del criterio del riesgo que la determinada conducta comporte para la llamada sociedad de la información[12].

No puede negarse que una perspectiva del derecho penal fincada en el delito de lesión, con un referente personalista del bien jurídico como objeto exclusivo de protección, tal como se concibió en la ilustración, no puede mantenerse inamovible, empero, tampoco puede pretenderse que lo pertinente es decirle *adiós al bien jurídico* en la medida que un derecho penal democrático, no puede concebirse sin referentes materiales. Por eso en otra parte sostuvimos que

---

10 Carlos. J. Suárez González. "Derecho penal y riesgos tecnológicos", en *Crítica y justificación* … cit., p. 294..

11 Para detalles, cfr. Michael Bunzel, *"La fuerza del principio constitucional de proporcionalidad como límite de la protección de bienes jurídicos en la sociedad de la información",* en "*La teoría del bien jurídico",* Roland Hefendelhl (ed), Madrid, Marcial Pons, 2007, p. 147 ss.

12 Detalles de la conceptualización en Enrique Rovira del Canto. *Delincuencia informática…* cit., p. 187 ss.

> "Acordamos con Schünemann[13] y Silva[14], que aquello que ha de imponerse es un punto intermedio que no desconozca la evidente evolución social pero que no flexibilice a tal punto las garantías, que las vacíe de contenido y las prive de todo carácter iluminador y limitador de la actuación de los poderes estatales. En ese sentido es suscribible una *"expansión razonable"*[15] esto es, la introducción de nuevas conductas delictivas que reparen en la trascendencia lesiva de los comportamientos que atentan contra nuevos intereses jurídicos (mercado de capitales, inversión, etc.)."[16]

II. LAS CONDUCTAS DE COMÚN REGULACIÓN EXTRANJERA

En doctrina se suelen distinguir los delitos que afectan como ente al PC, de aquellos que aluden a la información en ellas contenida o, ahora, a la que por ellos circula. Se ha evolucionado en la clasificación de las diversas delincuencias, caracterizada incluso por épocas, según la tecnología fue avanzando, y así de la preponderancia en la defensa de la intimidad de los años 70s y de las preocupaciones por lo económico hacia los 80s, se ha ido elevando tanto lo cualitativo como lo cuantitativo, sobre todo a partir del aparecimiento de la *red,* y lo que ella ha significado en el campo penal (el sabotaje informático, la pornografía, la alteración de los datos, la seguridad nacional, etc.).

Sin que sea posible aquí discriminar las discusiones, una de las últimas obras especializadas en la materia[17], que tiene ante todo el avance de introducir la discusión en punto de la llamada sociedad de riesgo, ha clasificado las tipologías del ciber delito de la siguiente manera:

(i) delitos no informáticos vinculados a la informática. Aquí se analizan los hechos que atacan al computador como ente físico *(hardware)* o en los cuales se utilizan medios informáticos sin que se afecte la información, como sería el hurto del PC o la estafas por

---

13 En efecto SCHÜNEMANN, Presentación a *Prolegómens*... cit., p. 17, estima la necesidad de modernizar los principios clásicos, "esto es, la evolución del Estado liberal de derecho hacia el Estado social de derecho que legitima y limita la expansión asociada de modo necesario con la modernización del derecho penal".

14 Opina SILVA en Presentación a *La insostenible*... cit., p. XII, que "si se pretende sacar al derecho penal de su situación, probablemente insostenible, deben formularse propuestas *posibilistas,* en vez de refugiarse numantinamente en el extremo opuesto de la defensa de una utopía (y ucronía) liberal radical". Esta crítica se amplía por SILVA, en *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales,* 2ª. ed. Madrid, 2001, p. 149 ss.

15 v. J.M. SILVA SÁNCHEZ. *La expansión...*, cit., p. 26.

16 J.F. REYES CUARTAS. *El Delito Socioeconómico En El Derecho Penal Colombiano*. Revista Jurídicas, Universidad de Caldas, Vol. 3 N.º 2, 2006.

17 ENRIQUE ROVIRA DEL CANTO. *Delincuencia informática*... cit., p. 119 ss.

medio de ordenadores. Esta problemática es cada vez menos importante, por lo pacífico de las discusiones y su casi nula extrapolación a la llamada ciber criminalidad.
(ii) Delitos informáticos impropios. En estos el objeto de protección lo es, preponderantemente, la información y su posibilidad de circulación, pero no de manera exclusiva, pues, de paso se protegen otros bienes jurídicos. Por ejemplo, se estudiarían aquí las manipulaciones de la información en las cuales se ocasionan daños patrimoniales.
(iii) Delitos informáticos propios. En estos el objeto de lesión lo es la información y el dato en sí mismo considerado.

Esta clasificación permite a su vez abrir la puerta de algunas especies del delito informático propio e impropio que fundamentalmente remiten a: (i) delincuencias que afectan el derecho a la intimidad (ii) delitos del ámbito socio-económico (iii) delitos alusivos a las comunicaciones telemáticas y otros ilícitos.

Los tipos de delito específicamente importantes en el área de la privacidad tienen que ver con la protección de los datos introducidos en bases de este tipo y que por fuerza o necesidad, las personas deben entregar, como sería el caso del registro civil, las historias clínicas, la historia del crédito personal; asimismo, las bases de datos de los empleadores, la seguridad social, los datos policiales y de seguridad (antecedentes, registros), y en el último tiempo, las bases construidas en el comercio con fines de *fidelización* de la clientela o los contentivos de datos de personas integrantes de un especial gremio, partido político o confesión religiosa, datos que entrañan aspectos del núcleo básico de la privacidad.

Estos datos alusivos a la intimidad, pueden generar delincuencias específicas (divulgación de datos que podrían perjudicar al interesado en su ámbito laboral, por ejemplo) o en todo caso ser ocasión de actividades comerciales como el delineamiento de perfiles de consumo, que se logra por medio de *"cookies"* y que generan el abusivo *"spamming"*.

Toda esta problemática alusiva a la protección de la intimidad, en punto de los datos almacenados en bases, nace en el derecho alemán de los 70s, se ve también en el italiano y español hacia los 80s y, en Colombia, se introduce en el año 90[18] con la regulación del *habeas data* que apenas hace semanas, se ha tratado de regular entre nosotros.

Fundamentalmente aquí se castigarían penalmente [19] (i) las llamadas infracciones de los derechos sustantivos de la intimidad, en punto del descubrimiento, difusión, obtención o acceso de forma ilegal a datos personales, su uso ilícito, la entrada, modificación ile-

---

18 Cfr. los estudios respecto al *habeas data* y en general, sobre el derecho a la intimidad, del recordado maestro Cirro Angarita Barón, en *El pensamiento jurídico de Ciro Angarita Barón,* Bogotá, Universidad de los Andes, 1999, *passim*.

19 E. Rovira del Canto. *Delincuencia…* cit. p. 153 ss.

gal, y/o falsificación de los mismos con intención de causar un perjuicio o incluso, los supuestos graves de almacenamiento, grabación o colección de datos o datos incorrectos de forma ilegal. Para las infracciones de los requisitos formales legales predispuestos para las actividades informáticas o telemáticas, fundamentalmente operarían sanciones civiles o de derecho penal administrativo. (ii) La negación al acceso a la información a la que se tiene derecho, comportaría sanción administrativa; en punto de la entrega de información falsa, podría comportar sanción penal. (iii) La negligencia para adoptar medidas de seguridad informáticas en el extranjero, no prevé sanciones penales o administrativas, salvo que se trate de ficheros de organizaciones públicas.

En España, el art. 197-1, castiga el *delito de apoderamiento de secretos documentales personales*. Su texto es del siguiente tenor:

> "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses." (subraya añadida).

Este tipo como es fácil colegir, posee una doble dificultad, primero se trata de una conducta de resultado con tendencia interna trascendente, pues, debe existir apoderamiento del documento con el fin de descubrir sus secretos o vulnerar la intimidad de su dueño, lo que por supuesto nos pone en la incertidumbre de entender si el nudo *hacking*, esto es, el acceso ilegal con el simple resultado de la vulneración de la privacidad, puede ser punido bajo este tipo[20]. La misma disposición, castiga la interceptación para descubrir secretos personales o vulnerar la intimidad de otro, esto es, la predisposición de artilugios y/o artefactos, que posibiliten la escucha, transmisión, grabación, reproducción del sonido o la imagen o de cualquier otra señal de telecomunicación. Este tipo posee también el elemento de la tendencia interna trascendente que se constituye en un elemento en contra de la sanción eficaz, y no parece tan claro que sea un tipo de mera actividad como opina Rovira del Canto.

Asimismo, la norma en su apartado 2 castiga el delito de vulneración del *habeas data*:

> "2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro públi-

20 Cfr. acerca de esta preocupación, Rovira del Canto, *Delincuencia...,* cit., p. 155.

> co o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

Esta norma no sanciona el simple *hacking*, pues exige la causación de un "perjuicio de tercero".

En punto de los delitos del ámbito económico, si bien ahora se trata de dar preponderancia a lo informático sobre lo económico[21], habida cuenta del espectro restrictivo que este ingrediente comporta, los delitos de este apartado fundamentalmente serían (i) el acceso ilegal o "*hacking*", (ii) el espionaje informático, (iii) la piratería de software y otras formas de piratería de productos (iv) el sabotaje y la extorsión informáticos y (v) el fraude informático.

Y en lo que atañe a los ilícitos de la comunicación telemática, han de introducirse las conductas relativas (i) al autor de materiales o declaraciones de contenido ilegal "o nocivo" emitidas o difundidas (ii) las del proveedor del servicio que ofrece el acceso a la red y servicios especiales al mismo tiempo y de cuyas redes y servidores abusan terceras personas. Fundamentalmente aquí se introducen las conductas relativas a la pornografía y delitos sexuales con menores y en general los tipos de apología y contenido racista o pornográfico, la apología de la violencia. En este acápite reviste interés la regulación de la responsabilidad de los administradores u operadores de Internet, pues es claro que no podría erigírseles en un garante de la licitud o adecuación de la información introducida, para así construir un tipo de omisión, pero en todo caso si habría de poder derivárseles responsabilidad sobre la permanencia del material en la red[22].

Adicionalmente, sería del caso ocuparse en este acápite, de otra serie de delitos en los cuales es determinante el uso de la telemática, pero que compromete intereses habituales de protección del derecho penal, como la vida, lo cual al decir de la doctrina[23], puede verse por ejemplo cuando se alteran los sistemas de control de aeronavegación, en que se pone en riesgo la vida, o en el caso de la gran criminalidad o criminalidad organizada que se vale de tales medios para perpetrar o agotar sus ilícitos (blanqueo de capitales, tráfico de drogas y de armas, terrorismo, etc.).

El Convenio sobre *cibercriminalidad* de Budapest del 23 de noviembre de 2001, ha previsto que las legislaciones nacionales tipifiquen las siguientes conductas:

---

21 Cfr. Rovira del Canto, *Delincuencia…*, cit. p. 157 ss.

22 Así, Morón Lerma, *Internet y Derecho Penal. Hacking y otras conductas ilícitas en la red.* Colección RdPD monográfico No. 1, Pamplona, Aranzadi, 1999, p. 139.

23 Vid. Rovira del Canto, *Delincuencia…*, cit. p. 169 ss.

1. Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Allí se introducirían las conductas que comporten el acceso ilícito doloso y sin autorización a todo o parte de un sistema informático; se dice que las partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.
2. La Interceptación ilícita, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos –en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Se prevé que las partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.
3. Atentados contra la integridad de los datos. Aquí se punirían la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos, aunque con criterios de fragmentariedad se dice que bien podría sólo acudirse al derecho sanción penal, si los daños ocasionados pueden calificarse de graves.
4. Atentados contra la integridad del sistema. Se prevén aquí las medidas legislativas penales, que sancionen la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
5. Abuso de equipos e instrumentos técnicos. *a)* la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición: i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones de acceso ilícito, interceptación ilícita o atentados contra la integridad de los datos o del sistema. ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para obtener acceso ilícito, interceptación ilícita o atentados contra la integridad de los datos o del sistema. *b.)* La posesión de alguno de los elementos descritos enantes, con la intención de utilizarlos como medio para cometer alguna de las infracciones de acceso ilícito, interceptación ilícita o atentados contra la integridad de los datos o del sistema. Estas conductas se encuentran excluidas de punición, si lo perseguido atañe a investigaciones propias de la prevención de riesgos en seguridad informática.
6. Infracciones informáticas. *a)* Falsedad informática. Se prevén aquí las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Se dice que las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal. b) Estafa informática. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción

penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: (i) la introducción, alteración, borrado o supresión de datos informáticos, (ii) cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.
7. Infracciones relativas al contenido. a) Infracciones relativas a la pornografía infantil. Se prevén aquí las medidas legislativas penales para prever tipificar las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización: (i) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; (ii) el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático; (iii) la difusión o la transmisión de pornografía infantil a través de un sistema informático; (iv) el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático; (v) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informático.
8. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines. A) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines, según los compromisos adoptados conforme a Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas; asimismo, el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático. También lo que se haya asumido según la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

III. LA REGULACIÓN COLOMBIANA

Es posible mantener la idea de que entre nosotros, los delitos relativos a la informática y a la información, conservan un carácter pluriofensivo, en el sentido de que si bien pueden tenerse como afectados derechos que tradicionalmente han sido de ocupación del derecho penal (la intimidad, el patrimonio económico) también es cierto que como se detalla a partir de los arts. 192 y ss. del C.P., el legislador se ha decantado por consagrar un plexo de conductas que responden a una cierta especialidad[24].

---

24 Entre nosotros el tema en realidad no ha sido de tratamiento profundo, como ya en 1993 lo ponían de

Esto por fuerza significa el que se ha alzaprimado el valor que en las sociedades modernas tiene la información, empero, la consagración del bien jurídico entre nosotros *"Intimidad, reserva e interceptación de comunicaciones"* deja harto que desear en la medida que se han dejado por fuera aspectos básicos como el de la "seguridad de las comunicaciones" pues, mantenerse a cubierto de las intromisiones en la intimidad, no parece protección suficiente.

En todo caso la tipificación hecha trata de la misma manera a quien simplemente intenta enterarse de los datos privados ajenos, que a quien por ejemplo, pone en riesgo la seguridad nacional o la estabilidad económica de un sector como el financiero o bancario. Ello exige pues, que se diferencie por el legislador y no apenas por el juzgador.

El bien jurídico consagrado entre nosotros se ha quedado corto y de allí que las posibilidades de generar espacios de impunidad son altamente factibles. Por ello sugerimos introducir los criterios que el Convenio sobre cibercriminalidad de Budapest del 23 de noviembre de 2001 ha previsto, a saber, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos.

Es necesaria la introducción de las palabras "confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos", lo que sin embargo abre la discusión acerca de si pueden considerarse las conductas como de peligro[25] o acaso mejor, de nuda conducta, discusión ciertamente profunda y que propicia una relativa expansión del derecho penal, aunque puede morigerarse en cada caso con los criterios de antijuridicidad material. Por ahora no existe espacio aquí para ahondar en ello.

Por otra parte y en lo que atañe al principio de legalidad, es claro que entre nosotros se extraña la inserción de un conjunto de definiciones que hagan más dúctil la aplicación y manejo de las diversas conductas susceptibles de alterar los sistemas de información. Ello sin duda se erige un blindaje que impida las soluciones por la vía de la analogía prohibida. Por ejemplo, el Convenio sobre cibercriminalidad de Budapest del 23 de noviembre de 2001, ha introducido esta terminología que bien podría introducirse legislativamente entre nosotros:

> Terminología. Artículo 1 – Definiciones. A los efectos del presente Convenio, la expresión: a. "sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos; b. "datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una

---

presente Ma. Fernanda Guerrero Mateus/Jaime Eduardo Santos Mera. *Fraude informático en la banca Aspectos criminológicos.* Ed. Jesma, Bogotá, 1993, p. 29.

25 Así, Rovira del Canto, *Delincuencia…*, cit. p. 187-188.

> forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función; c. "prestador de servicio" (1) designa: i. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático; ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios; d. "datos de tráfico" (2) designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

En el pasado reciente se ha observado cómo el avance de las tecnologías de la información, ha dejado en la zaga a las previsiones del legislador, quien debe acudir presto a solucionar lagunas de punibilidad, cuando no es que de manera inconstitucional el intérprete ha procurado salir al paso a la impunidad. Con todo, es preferible alguna cuota de impunidad a aceptar el siguiente criterio como orientador de la política criminal en esta materia:

> "Debido a la continua evolución de las nuevas tecnologías para su formulación tipológica requiere la creación de tipos delictivos amplios, utilizando conceptos jurídicos indeterminados o leyes penales en blanco y elaborados con criterios uniformes a nivel internacional"[26]

Ciertamente una manera de pensar como esta, arrasa toda la tradición jurídica continental de respeto por la libertad, la cual se vería expósita si el legislador pudiera simplemente acudir a esta técnica, a la vista del mayor interés puesto en el bien que se pretende proteger. No se desconoce que la mundialización de las conductas criminales en el ciberespacio y los riesgos a los que se ven expuestos las sociedades contemporáneas por razón de ellas, exigen y demandan respuestas eficaces. Pero acaso es hora de pensar en que los países deben empezar a armonizar (antes que unificar) sus legislaciones, y de esa manera prever herramientas globales que respeten en algún modo las identidades nacionales.

De cara a las sugerencias del Convenio sobre cibercriminalidad de Budapest del 23 de noviembre de 2001, en Colombia se tiene:

1. En lo atinente a las *Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos,* los arts. 192, 194 y 195 castigan a quien "ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido"; asimismo, a quien en provecho propio o ajeno o con perjuicio de otro divulgue

---

26 Rovira del Canto, *Delincuencia…*, cit. p. 188.

o emplee el contenido de un documento que deba permanecer en reserva; de otra parte, será sancionado penalmente quien ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial.

Como se puede ver, el art. 192 exige ilicitud en el acceso a la información, esto es, no demanda específicamente la vulneración de medidas de seguridad, por lo que cabe preguntarse si en el giro "ilícitamente" cabe entender la trasgresión de normas de seguridad. Nuestra respuesta es positiva en la medida que si lo que se protege es la intimidad, en cuanto espacio de albedrío que pretende ejercerse con exclusión de cualquiera otra persona, es lógico pensar que el ingreso, extravío, ocultación, sustracción, etc., de información privada comporta como consustancial, la ilicitud. Esta interpretación se ahorra en frente del art. 195 pues, allí si se demanda la protección con medida de seguridad.

La norma 192 no demanda la causación de perjuicio ni introduce una tendencia interna o de ánimo, específicos, lo que permite concluir que el simple hacking blanco cabe ya dentro del tipo. En todo caso la producción de daños, o el aprovechamiento de los datos o la revelación de los mismos, agrava la sanción (192-2º. CP), lo que cual confirma la anterior conclusión.

Asimismo, dentro del mentado 192, se pune la Interceptación ilícita no autorizada de datos y que se hallan protegidos por el derecho a la intimidad; asimismo, se castiga la violación del derecho a la reserva y confidencialidad de los datos privados. La norma carece de referentes de ánimo o de la exigencia de causación de perjuicios concretos, para su castigo.

Hoy se ha puesto de moda dentro de las conductas contrarias a la ética informática, la creación de virus, gusanos y troyanos[27]. Aunque la introducción maliciosa de cualquiera de estos programas *malware* puede leerse como un acceso ilícito, es lo cierto que cada

---

27 Los virus son programas minúsculos que se pegan a diferentes tipos de archivos y que de esta manera pueden viajar por diferentes medios (Disquetes, CDs, DVDs, la Red y Obviamente Internet y Correo electrónico). Su propósito principal es causar una acción en demérito del usuario del computador al que han afectado. Este daño puede ser desde un simple mensaje o una acción pícara, hasta el desarrollo de acciones mas complejas como el daño en los archivos y la misma configuración y programación del computador para obligarlo de manera remota o auto programada a producir envíos masivos de replicas y mensajes y la apertura de puertos de seguridad a través de los cuales los delincuentes pueden ampliar su capacidad de daño. En realidad los virus se han dividido en varias familias de acuerdo con sus características y muchos de los denominados parásitos y malware son evoluciones de esta cepa. Los gusanos son versiones más evolucionadas y eficientes de los mismos virus, pero estos tienen la capacidad de crear pequeños programas que se multiplican y se distribuyen por su propia cuenta, generando nuevos gusanos y desarrollando actividades más complejas generalmente para el envío de información confidencial o la programación de tareas. Los troyanos reciben su nombre del "caballo de Troya" con el que, de acuerdo con la Iliada, le permitió a los griegos entrar a Troya y destruirla. Su función es alojarse en la memoria del computador o en los programas sensibles de conexión y permitir que un tercero acceda a la información o incluso controle, manipule y obligue al computador a realizar tareas. De esta manera,

uno tiene fines diferentes. Por ejemplo, con insistencia se habla hoy del *"secuestro de datos"* o del "*secuestro del sistema"*, por medio de troyanos que convierten en autómatas a los CP, y se duda que quepa en alguna de las descripciones típicas anotadas. Por ello se ha pretendido en el proyecto de ley 152-Cámara de representantes, a iniciativa del Senador GERMÁN VARÓN C., que se castigue esta conducta y que además se agrave en algunos casos en que es observable un *plus* de injusto[28].

2. Respecto de los llamados *atentados contra la integridad de los datos*, el art. 192 sanciona la conducta de destruir comunicaciones privadas; empero, el daño a los datos contenidos en el sistema informático, no podrá punirse por la vía del art. 265 del CP, el cual consagra el delito de daño en bien ajeno, imponiendo castigo a quien destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble.

Comoquiera que los datos, *prima facie*, no son "bienes mueble o inmuebles", las conductas de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización datos informáticos, no parecen encuadrables en esta disposición ni tampoco en el art. 357 del CP [29], tipo destinado a proteger soportes materiales de ciertos servicios, en el

---

un computador infectado, se puede convertir en un zombie y realizar tareas para un delincuente. Entre estas tareas se pueden contar el envío de información y el envío de *spam.*

28 Artículo 4°. Se adiciona con un nuevo artículo el Capítulo VII Título III del Libro Segundo de la Ley 599 de 2000:
Artículo 195A. *Violación a la disponibilidad de datos informáticos.* El que sin autorización, por cualquier medio impida el acceso normal a un sistema informático o a los datos informáticos allí contenidos, incurrirá en prisión de doce (12) a treinta y seis (36) meses y multa de diez (10) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya un delito sancionado con pena mayor.
Artículo 5°. Se adiciona con un nuevo artículo el Capítulo VII Título III del Libro Segundo de la Ley 599 de 2000:
Artículo 195B. *Circunstancias de agravación punitiva.* Las penas previstas en los artículos 195 y 195A se duplicarán si concurriere alguna de las siguientes circunstancias:
1. Cuando se haya instalado un programa de ordenador o instalado un dispositivo que de cualquier manera atente contra la confidencialidad o integridad de los datos informáticos almacenados en el sistema informático.
2. Cuando los datos informáticos almacenados en el sistema informático pertenezcan a una entidad que cumpla funciones públicas.
3. Cuando los datos informáticos almacenados en el sistema informático pertenecen al sector financiero.
4. Cuando la acción se realizare por una persona con una relación contractual con el propietario de los datos.
5. Cuando la persona obtuviere provecho para sí o para un tercero.
6. Cuando se den a conocer a terceros los datos informáticos así obtenidos o se procese, recolecte o circule los datos personales o los datos de autorización o autenticación del sistema informático.
En todos los casos el juez podrá imponer como pena accesoria la interdicción de acceder o hacer uso de sistemas informáticos.

29 Art. 357. Daño en obras o elementos de los servicios de comunicaciones, energia y combustibles. <Penas aumentadas por el art. 14 de la Ley 890 de 2004, a partir del 1.º de enero de 2005. El texto con las

ámbito de la seguridad pública. Asimismo, tampoco parece encuadrable típicamente la conducta de obstaculizar el funcionamiento de un sistema informático.

Esto genera una evidente laguna punitiva que debe remediarse pronto, pues, los datos ante todo son elementos lógicos, inaprensibles, con un valor económico ciertamente, pero en todo caso de trascendencia inmaterial. Nótese como el legislador en el art. 199 consagró una especial conducta de sabotaje[30], en la cual se castiga la destrucción de datos y soportes lógicos, pero habida cuenta del bien jurídico protegido –"la libertad de trabajo y asociación"–, el dicho tipo especial de daño, sólo es punible en ese específico y claro ámbito, amén de que la conducta de dañar o destruir datos o soportes lógicos debe ser con el fin de suspender o paralizar el trabajo.

3. En relación con la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de un dispositivo apto para interceptar comunicaciones privadas, en la descripción comportamental del art. 193 no cabe la posesión de programas informáticos o de palabras de paso (contraseña o *password*), que permitan acceder a todo o parte de un sistema informático con el fin de a permitir la comisión de infracciones de acceso ilícito, interceptación ilícita o atentados contra la integridad de los datos o del sistema. Esta es una preocupante laguna, aunque bien podría tener soluciones por vías alternativas al derecho penal.

4. Respecto de las infracciones que aluden a la falsedad y la estafa, la redacción del art. 294 del CP, al prever que es documento para efectos penales, también, el soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria, bien permite concluir que es posible incurrir en cualquiera de los delitos de la rúbrica sea por la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos. Con todo, y de la mano de ROVIRA DEL CANTO[31] la simulación de una página WEB, conducta de alta ocurrencia en el último tiempo entre nosotros, no parece

---

penas aumentadas es el siguiente:> El que dañe obras u otros elementos destinados a comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales, radiales o similares, o a la producción y conducción de energía o combustible, o a su almacenamiento, incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de trece punto treinta y tres (13.33) a ciento cincuenta (150) salarios mínimos legales mensuales vigentes.
La pena se aumentará de una tercera parte a la mitad cuando la conducta se realice con fines terroristas.

30 Art. 199. Sabotaje. <Penas aumentadas por el artículo 14 de la Ley 890 de 2004, a partir del 1o. de enero de 2005. El texto con las penas aumentadas es el siguiente:> El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses y multa de seis punto sesenta y seis (6.66) a treinta (30) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor. Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspensión o cesación colectiva del trabajo, la pena se aumentará hasta en una tercera parte.

31 E. ROVIRA DEL CANTO, *Delincuencia informática…* cit., p. 181.

encuadrable entre nosotros como un acto falsario y más bien puede observarse como una tentativa de estafa, empero, resulta harto difícil enmarcarle aquí, ante la equivocidad de los actos o en todo caso porque no parece claro que la falsificación de la página constituya ya un acto típico ejecutivo, de la descripción de la estafa.

Por otra parte es claro que en la redacción del art. 246 CP. *–El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños–* son perfectamente encuadrables las conductas tendientes a obtener una defraudación patrimonial ajena, por medio de la introducción, alteración, borrado o supresión de datos informáticos, o en todo caso, por cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero, pues, tal espectro comportamental es leíble bajo el giro "induciendo o manteniendo a otro en error por medio de artificios o engaños".

5. Y en punto de las Infracciones relativas al contenido, en lo atinente aquéllas que se refieren a la pornografía infantil, el art. 218 del CP castiga con pena de prisión a quien fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad. Asimismo, está penado, según el art. 219-A., quien utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con éstos. Esto es, se castiga tanto la producción del material, su difusión, su comercialización. Empero, la redacción típica ofrece problemas frente a quien simplemente almacena la pornografía infantil en soporte informático, sin concurrir a su producción (sea por filmación, fotografía).