XXXVI JORNADAS INTERNACIONALES DE DERECHO PENAL

LA EVOLUCIÓN DE LOS DERECHOS A LA INTIMIDAD Y AL *PRIVACY* ANALIZADOS DESDE LA PERSPECTIVA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA CONSECUENTE INSUFICIENCIA DE LA REGULACIÓN JURÍDICO-PENAL EN LA MATERIA

AUTOR: DARÍO BAZZANI MONTOYA*

Profesor Titular de la Catedra de Derecho

Procesal Penal de la Universidad Externado de Colombia

(Este documento está sujeto a posteriores revisiones previo a su publicación)

UNIVERSIDAD EXTERNADO DE COLOMBIA

2014

I. La evolución del derecho a la intimidad y del derecho a la privacidad

El primer aspecto por establecer, a efectos de determinar la efectividad del marco regulatorio jurídico penal de la información y las tecnologías de la información, es el fundamento de la intervención del sistema penal.

En ese sentido, la mayoría de constituciones se ocupan de proteger la inviolabilidad de las comunicaciones y la protección del habeas data, pero poco se interesan en reconocer, con una entidad autónoma e independiente, el derecho a la intimidad frente a la obtención de la información y el uso que se le puede dar a dicha información por parte de un tercero y, mucho menos, en tratándose del nuevo mundo virtual.

Para abordar el tema, es necesario recordar los antecedentes y la evolución del concepto de intimidad, propio del sistema jurídico europeo continental y compararlo con la noción de privacidad que ha desarrollado el sistema jurídico anglosajón y, más exactamente, la doctrina y la jurisprudencia norteamericana, a las luces de la teoría del precedente judicial.

A. La privacidad americana frente a la europea

La sociedad de antaño y me refiero a tan solo medio siglo atrás, sólo se ocupaba de proteger la esfera privada de las personas de los ataques provenientes del Estado y, marginalmente, de la intrusión por parte de terceros, con fines de información periodística.

Es sin duda, la aparición de nuevos inventos y su evolución, la que ha marcado nuevos problemas jurídicos frente al objeto de protección, que ya no es el patrimonio

o la simple autonomía personal, sino que plantea un nuevo concepto como centro de atención: La información.

De la cámara fotográfica inventada en 1826 por Charles y Vincent Chevalier, se pasó a la posibilidad de preservar las imagenes capturadas y la fotografía como un arte y oficio de interés generalizado y popular, a finales del siglo XIX, cuando se incorporó el carrete al artefacto y gracias a la portabilidad del instrumento.

Luego, con las bases de la fotografía se le dió movimiento visual a las imágenes estáticas y surgió el cine, pero, sin lugar a dudas, la revolución del mundo moderno y de la información y las tecnoloías, ocurrió este siglo en la década de los años 40s cuando John Vincent Atanassoff inventó el computador y, más adelante, a finales de la década de 1960, con la invención del arpanet y luego internet. A partir de ese momento, la sociedad moderna cuenta con la capacidad no sólo de almacenar grandes cantidades de información sino de compartirla a través del mundo virtual.

"Se puede comprender que, en un primer momento, el ámbito de lo privado haya tenido como pilares el respeto a la inviolabilidad del domicilio, el secreto de las comunicaciones y la tutela de la reputación de las personas. Ello era concebible en una sociedad en la que el individuo burgués era la medida de todas las cosas y el progreso, como diría Zagrebelsky, una verdadera necesidad fisiológica. Los derechos debían ordenarse, en consecuencia, en función de tal necesidad, concebidos como derechos—autonomía, vinculados al patrimonio y sujetos a escasos limites interferencias."[1]

Sin embargo, las sociedades evolucionan y los ordenamientos jurídicos lo hacen a la par con estas, por lo cual, las regulaciones jurídicas y los contenidos de los derechos mutan con el pasar de los años. Este es el caso de los derechos de la

---

*Darío Bazzani Montoya es abogado de la Universidad Externado de Colombia, con especialización en Derecho Penal y Ciencias Criminológicas de la misma casa de estudios. También adelantó estudios de especialización en materia procesal penal en La Universitá Degli Studi Di Roma Tor Vergata y es candidato a Doctor en Derecho de la Universidad Externado de Colombia. Actualmente es profesor titular de la catedra de Derecho Procesal Penal de la facultad de Derecho del Externado, y es profesor de posgrado en programas de Especialización y Maestría en la misma Universidad.

[1] SUAREZ Crothers, Christian, *El Concepto de Derecho a la Vida Privada en el Derecho Anglosajón Europeo,* Revista de Derecho, Vol. XI, diciembre de 2000, p. 104

privacidad y de la intimidad, que han evolucionado con la progresiva incursión de las tecnologías de la información dentro de nuestra sociedad, razón por la cual resulta necesario e importante su estudio desde esta nueva óptica del derecho.

El contenido de los derechos de la intimidad y la privacidad varían diametralmente según donde se estudien[2], las cortes estadounidenses y las europeas, para el caso específico, asumen a la privacidad como un derecho con un contenido distinto en cada país y, por lo tanto, meritorio de una protección diferente en cada ordenamiento jurídico.

Ahora bien, la privacidad debe ser abordada y estudiada de forma distinta cuando se trata del entorno informático. No puede decirse, bajo ningún motivo, que la privacidad debe medirse con el mismo rasero en el mundo real que en el mundo virtual. Ello es así, por cuanto las posibilidades de comunicación, transmisión y volatilidad de la información son distintas cuando se trata de un entorno digital.

La privacidad puede ser comprendida desde dos dimensiones distintas de protección de derechos: en primer lugar, como un mecanismo de control como expresión de la libertad, es decir, es la libertad individual de elegir quien puede tener acceso a mi información. En segundo lugar, se puede abordar la privacidad desde la perspectiva de la protección a la dignidad humana[3].

La noción de privacidad cambia de legislación a legislación y de Estado a Estado. Esto indica que no existe un concepto unitario sobre la privacidad y que por lo tanto, en las legislaciones y en la academia se encuentran tantas definiciones como instrumentos de protección al respecto. Sin embargo, puede decirse que los dos

[2] En el mismo sentido, Patricia S. Abril y Eugenio Pizarro en La Intimidad Europea Frente a la Intimidad Americana: *"(…) la princesa Carolina de Mónaco es fotografiada junto a sus hijos menores sin su consentimiento, el Presidente de la Federación Internacional de Automóviles es calumniado por un periódico británico que proveyó de una cámara oculta a una prostituta para tomarle fotografías durante actos sexuales sadomasoquistas con supuestos temas nazis; o Lorena McKennitt, una famosa cantante canadiense, es amenazada por la publicación de un libro sobre sus asuntos privados escrito por una antigua amiga y empleada. Casos como los anteriores suceden en todas partes del mundo y, ante los mismos, las Cortes han reaccionado de disímiles maneras. Dichas reacciones son muchas veces el producto de las nociones de privacidad que el sistema legal ha acogido."*

[3] Ibíd., p. 7

conceptos prevalecientes son los adoptados por el sistema norteamericano y el sistema europeo.

Los estadounidenses se refieren a la privacidad como una forma de control sobre la información personal mientras que en la jurisprudencia europea la privacidad es entendida desde la noción propia de la dignidad humana, casi como un atributo de la misma, en el marco del Estado Social de Derecho.[4]

La privacidad como posibilidad de control sobre los datos personales, debe ser entendida, más exactamente, como la posibilidad de decidir quién tiene acceso a esta.

James Q. Whitman, en su artículo titulado "*The Two Western Cultures of Privacy: Dignity Versus Liberty*"[5], plantea dos interrogantes llamativos al respecto: ¿Por qué los franceses evaden hablar sobre sus salarios, y sin embargo, se quitan la parte superior de su bikini?, o ¿Por qué los americanos se someten a extensivos reportes de crédito sin revelarse? Para este autor, es evidente que la libertad vista desde el sistema americano, es entendida como la *"libertad de rechazar la intromisión gubernamental en la esfera privada",* mientras que para los europeos, la privacidad debe ser entendida como una expresión de dignidad.

A.1. La intimidad

Ahora bien, la comunidad europea, como se ha dicho, le da a la privacidad una calidad distinta, más bien entendida como una manifestación de la dignidad[6]. Esto

---

[4] Citado en un muy completo ensayo por ABRIL, Patricia y PIZARRO, Eugenio en *La intimidad europea frente a la privacidad norteamericana, quienes* señalan: *"Las dos nociones prevalentes, como se evidencia de las legislaciones occidentales modernas y del discurso legal, son las mencionadas supra: privacidad entendida como control y la privacidad como dignidad. La jurisprudencia estadounidense otorga un lugar cimero a la noción de privacidad como control sobre la información personal y, por tanto, la autonomía de decidir con quién compartirla. Por el contrario, la jurisprudencia europea adopta la noción de privacidad como dignidad, o sea, como un derecho humano a la vida privada, un derecho y valor sustantivos de primer orden."*

[5] WHITMAN, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty, 2004, p. 1161

[6] Debe decirse que los españoles no acuden al término privacidad en la legislación civil y penal, y por el contrario hacen referencia a la expresión de intimidad. Es decir, intimidad en contraposición de la vida privada. Así se entiende la interpretación dada, al artículo 8 del Convenio Europeo de Derechos Humanos, firmado en Roma el 4 de noviembre de 1950, que señala: *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una*

es relevante porque actualmente la dignidad humana no es un simple derecho individual sino un atributo de la humanidad.

Autores como Samuel Warren y Louis Brandeis en un artículo que data de 1890[7] señalaban que la privacidad debía ser protegida por la ley bajo "el principio de la inviolabilidad de la personalidad"[8]. Estos autores han entendido que la razón por la cual la privacidad debe ser entendida como una manifestación de la dignidad se debe a que el individuo debe poder manejar en su esfera personal aspectos que controlados de otro modo podrían afectar su imagen, su nombre y su honra, pues el individuo podría quedar a merced del escarnio público y de la opinión de la sociedad. Esto puede considerarse como un clarísimo menoscabo a la dignidad[9] del individuo.

La definición del concepto de intimidad ha superado la más variada cantidad de definiciones; Kant, por ejemplo, estructuraba el concepto de intimidad sobre el edificio de libertades del individuo, en dicha época las libertades del individuo eran una manifestación derivada de la personalidad o incluso de la propiedad.[10]

En tiempos modernos se ha optado por un concepto de intimidad distinto. Por ejemplo, el derecho francés lo define como "el derecho del individuo de tener una esfera secreta de vida de la que tenga el poder de alejar a los demás"[11]. Para los

---

medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

[7] Samuel WARREN & Louis BRANDEIS (1890), "The Right to Privacy", Harvard Law Review, Vol. IV, núm. 15, pp. 2303-2312.

[8] Cfr. de ABRIL, Patricia y PIZARRO, Eugenio en *La intimidad europea frente a la privacidad norteamericana,* p. 8

[9] En el mismo sentido, de ABRIL, Patricia y PIZARRO, Eugenio en *La intimidad europea frente a la privacidad norteamericana,* señalan: "Una mirada a la privacidad enfocándose en el aspecto de la dignidad humana implica inevitablemente el reflejo del desarrollo de la personalidad per se y del "yo interior". Desde este punto de vista, la privacidad implica el derecho de mantener ciertos aspectos de la vida privada fuera del alcance de otros y, por lo tanto, el derecho a construir diferentes "personalidades situacionales". Al hacer esto, el individuo divulga aspectos de su privacidad en diferentes ambientes y en diferentes contextos. El riesgo mayor es la falta de capacidad de libremente administrar qué información privada fue divulgada y en qué contexto, lo cual conlleva a consecuencias sociales catastróficas."

[10] Cfr. SUAREZ Crothers, Christian, *El Concepto de Derecho a la Vida Privada en el Derecho Anglosajón Europeo,* Revista de Derecho, Vol. XI, diciembre de 2000, p. 107

[11] Ibíd., p. 107

italianos, se conoce como el derecho a la riservatezza y se define como "la pretensión del individuo de ver impedida la curiosidad de otros, prohibiéndose la indiscreción y la publicidad no querida, el conocimiento y la divulgación de las vicisitudes personales y familiares"[12].

Para Loebenstein, siguiendo a Suarez, el derecho a la vida privada se manifiesta "en el respeto al cuerpo y al alma del individuo, y conforme a ello debe asegurarse su protección frente a problemas tales como la indagación de la paternidad, las encuestas de opinión, los test de proyección psicológica, etc."

Quiere decir esto, que el derecho a la intimidad es comprendido como una manifestación de la dignidad humana por cuanto se impone una esfera de protección a lo que hace parte de la mismidad del individuo, su identidad como ser, es decir, sobre todo aquello que hace parte de su más importante espacio personal y que, estrictamente constituye su vida privada. Puede decirse que el derecho a la intimidad reconoce el carácter unitario del individuo y encarna la manifestación por el respecto de la personalidad de tal y de sus más profundos y concretos intereses.

Puede concluirse, que la protección que exige la intimidad está dirigida exclusivamente a controlar el acceso a la información, pues el objetivo es que ningún individuo ajeno al que la persona autorice para ello conozca de las situaciones que hacen parte del propio ámbito de la intimidad de una persona.

A.2. La privacidad o privacy norteamericano

La evolución de la privacidad, debe ser entendida desde la perspectiva del desarrollo y avance humano. El crecimiento de las ciudades, el mayor número de población educada y los mecanismos de difusión de información de la actualidad[13]

[12] Ibíd., 107

[13] ABRIL, Patricia y PIZARRO, Eugenio, al respecto apuntan lo siguiente: "Desde finales del siglo XIX, el concepto de privacidad se adueñó progresivamente de la conciencia estadounidense. Historiadores han atribuido aquel despertar al incremento en la densidad de población en las ciudades, en el número de la población alfabetizada y a la difusión de la información. Todos estos factores contribuyeron a un enfoque social de la privacidad y al cuestionamiento inevitable de cómo la ley podría responder a la misma."

permiten entender como este derecho ha pasado a ocupar un espacio tan importante en la sociedad moderna.

En el derecho estadounidense la privacidad no aparece mencionada ni en la Constitución ni en la Carta de Derechos. Por el contrario, el concepto fue desarrollado por la jurisprudencia de la Suprema Corte, quien entendió que la garantía y el derecho de privacidad estaban relacionados con otros derechos, tales como la libertad de asociarse, la integridad corporal, la vida familiar y sexual, entre otras[14].

En ese sentido, en el sistema norteamericano el derecho a la privacidad se ha relacionado con el derecho a la libertad y se ha creado una línea jurisprudencial de protección al mismo a partir del precedente judicial en lo tocante a las acciones civiles con fines indemnizatorios.

El contenido particular del *privacy* fue producto de un largo desarrollo de la jurisprudencia de la Suprema Corte, pasando de la protección de los lugares a la protección de las personas, y superando la protección física para concentrase en la protección virtual de la privacidad.[15]No obstante, los límites a la protección y los requisitos son sustancialmente más exigentes que en el sistema europeo continental, en atención a la especial protección a las libertades públicas, al interés público y a la seguridad nacional.

---

[14] Ibíd., p. 13

[15] En ese mismo sentido, SUAREZ, Christian, señala: *"Sin embargo, hacia fines de los años veinte, el contenido de la privacy comenzó a ser más confuso, toda vez que las cortes afirmaban o negaba el derecho dándole los más diversos contenidos, pero siempre bajo el resabio patrimonialista que consideraba que debía existir una efectiva intrusión física ("actual physical invasión"), para que se configurara una violación a la Cuarta Enmienda, sobre la cual se había construido este derecho. Pero, precisamente cuando la Corte Suprema había comenzado a prescindir de este requisito, desvinculándose de la interpretación tradicional y propietaria, en el año 1928, en el caso Olmstead v. United States, cambió su interpretación, considerando que no se violaba la Cuarta Enmienda cuando, por ejemplo, las interceptaciones utilizaban cables telefónicos colocados al exterior de una casa, o cuando los micrófonos habían sido puestos en el muro de una habitación colindante con la del indagado.*

Será necesario llegar al año 1967 para que la Corte, en el caso Katz, afirme que la "Cuarta Enmienda protege a las personas y no a los lugares" y, en consecuencia, declare ilegítimo el registro de una conversación telefónica efectuada por medios electrónicos colocados al exterior de una cabina pública."

Su desarrollo y evolución, como se ha mencionado, ha pasado por las más variadas y diversas definiciones. Así, el concepto del *privacy* surge originalmente como un derecho a prevenir la publicación de notificas personales; mas adelante, se erige como una garantía del derecho al nombre, y en un caso posterior, se asumió como una premisa a la libertad de asociación. Finalmente, se le concibió como premisa a la libertad de opinión.[16]

Es por ello que se han creado distintas acciones civiles dirigidas a proteger las diferentes formas en las que se puede producir una afectación o menoscabo grave a la dignidad, pero no concebida como derecho absoluto, sino como esfera de control de l individuo: Privacidad.

A.3. La invasión a la privacidad desde la jurisprudencia americana

Se han desarrollado cuatro tipos de acciones civiles para proteger la privacidad. Así, con el pasar de los años se han implantado las acciones de intromisión a la reclusión, (esfera privada), la apropiación, la distorsión de la imagen y finalmente, la difusión pública de hechos privados.

a) **Intromisión a la reclusión:** El derecho civil norteamericano ha recogido prácticas invasivas sobre la recolección de la información. Esta acción se utiliza en los casos en los que la información ha sido descubierta o recolectada de manera furtiva o en lugares catalogados como privados.[17] Los efectos de esta acción se han extendido a lugares no físicos, como puede considerarse el ámbito virtual o de las telecomunicaciones.

b) **Apropiación del nombre o la figura:** Esta acción está enfocada a proteger el uso comercial no autorizado de la identidad de una persona y sus

[16] Cfr., SUAREZ, Christian, , *El Concepto de Derecho a la Vida Privada en el Derecho Anglosajón Europeo,* Revista de Derecho, Vol. XI, diciembre de 2000, p. 117

[17] Los requisitos para interponer esta acción son: "La misma requiere que el demandante muestre que el defendido (a) intencionalmente se inmiscuyó, físicamente o de otra manera, (b) en la reclusión o soledad de otro o en sus asuntos o problemas privados, (c) en una manera altamente ofensiva a una persona razonable." Según lo afirman Abril y Pizarro.

consecuentes daños a la dignidad. Esta acción se diseñó con el propósito de identificar un cierto derecho de propiedad sobre el nombre o la figura.

c) **Distorsión de la imagen:** Esta acción es utilizada para aquellos eventos en los que se difunde información falsa o engañosa sobre un sujeto. Se sanciona cuando se considera que la información difundida sea altamente ofensiva y cuando se pueda demostrar que quien decidió difundirla tenía conocimiento sobre su falsedad.

d) **Difusión pública de hechos privados:** Opera cuando hechos altamente ofensivos y de carácter privado son difundidos de manera injustificada. *"La acción de difusión pública de hechos privados da lugar a una compensación por la publicación injustificada de hechos verdaderos pero sin valor informativo, privados, y ofensivos".*[18]

Para que tal acción prospere es necesario probar que: el demandado dio publicidad, a un hecho privado, que no es de interés legítimo del público y donde tal información es altamente ofensiva para una persona, en términos razonables.

e) **Límites**

Hecho el ejercicio de ponderación de derechos que pueden encontrarse en conflicto, se han considerado algunos límites para la procedencia de estas acciones civiles. Entre ellos se pueden identificar, principalmente, la expectativa razonable de intimidad, la ausencia de interés público o informativo y la naturaleza de la información, debe tratarse de información oprobiosa.

- **Sobre la expectativa razonable de privacidad:** Previo a establecer la existencia de cualquier menoscabo, debe valorarse si la información que se pretende proteger es privada de acuerdo a su pristina naturaleza. Para ello se hace necesario hacer una valoración de carácter objetivo: establecer si existe una expectativa razonable de privacidad.

[18] Ibíd., p. 19

Para establecer esto, en la mayoría de ocasiones se acude a un criterio espacial, es decir, establecer si en el lugar donde ocurrió el hecho se podía predicar una expectativa razonable de intimidad. Aun así, este límite tiene sus dificultades prácticas por cuanto la expectativa de privacidad se debe definir de caso a caso a través de ejercicios de ponderación.

- **Ausencia de interés público o informativo:** En este punto se ha discutido sobre la validez de la intromisión en la intimidad cuando se trata de información que puede ser catalogada como de interés público o, que al menos, se trate de información respecto de la cual las personas tengan derecho de conocer en ejercicio del derecho a la información. Cuando se está frente a este escenario, la jurisprudencia norteamericana ha señalado que no es posible interponer las acciones anteriomente mencionadas.

- **Demostrar que se trata de información oprobiosa:** Como ya se ha señalado, la protección sobre estas esferas personales solamente puede reclamarse cuando se demuestra que realmente exitió o se presentó abuso sobre información que sea catalogada como altamente ofensiva.

B. La privacidad de la información en las redes sociales

Las redes sociales plantean un reto enorme frente a la privacidad: un control extremo sobre la privacidad impide que los internautas puedan desenvolverse naturalmente dentro de la red puesto que la interacción parte del supuesto de que la información personal sea compartida. Los participantes de las redes sociales divulgan y comparten información sin importarles, aparentemente, la pérdida de control sobre la misma. Aun a pesar de ello y no obstante la confianza en la funcionalidad de la red, las personas reclaman nuevamente su intimidad cuando la información personal es accedida, usada o divulgada por terceros ajenos a la red social o cuando pertenecen a otras redes sociales.

En un artículo publicado por Abril y Lavin se determinó que los participantes de las redes sociales en internet pueden tener una expectativa legitima de privacidad, la

que la red otorga y la que de la red se puede esperar. En ese sentido la información puede entenderse como privada siempre y cuando no sea divulgada por fuera de la red donde fue inicialmente difundida, si la misma fue originada entre ellos, o si no afecta la integridad del internauta de haber sido originada por otros.[19] Sin embargo, la red enfrenta un problema que los individuos no tenían acentuado en la sociedad no informática. La pérdida de control sobre la información que ya ha sido compartida y la cantidad de personas que pueden acceder a la misma.

II. De la información

La sociedad moderna se mueve indefectiblemente sobre la base de la información.[20] Éste, sin lugar a dudas es uno de los bienes jurídicos más importantes que tenemos hoy en día, en términos de categorización de su valor social y económico.[21] La necesidad de una rápida comunicación, el comercio transfronterizo, de producción eficaz y en masa, el manejo de comportamientos sociales, los costos de publicidad y acceso a los medios de comunicación, han sido algunos de los factores determinantes que han llevado a lo que hoy conocemos como internet, y a lo que hoy tenemos como la estructura de comunicaciones más grande, capaz y eficaz del mundo.

Cuando se trata de internet, encontramos que la evolución del "World Wide Web", ha tenido un crecimiento desmesurado en las últimas dos décadas. Este fenómeno responde a diferentes variables; por un lado, encontramos que la cantidad de negocios que se volcó a la red, no se pensó nunca, dada la masificación del servicio, la facilidad de infraestructura y los bajos costos[22]. Así, encontramos compañías de

[19] Patricia SÁNCHEZ ABRIL & Avner LEVIN (2009), "Dos Nociones sobre la Privacidad Online", Vanderbilt Journal of Entertainment & Technology Law, Vol. 11, pp. 1001-1051.

[20] PEÑA VALENZUELA, DANIEL. XXXII Jornadas de derecho penal. 2010 Derecho de la seguridad de los sistemas de la información: parámetros para la construcción del ciberdelito.

[21] En ese sentido, RINCON RIOS, Jarvey y NARANJO DUQUE, Victoria afirman: "*La era actual ha sido denominada como la sociedad del conocimiento o economía del conocimiento, en razón a que la información adquiere un valor relevante desde todos los puntos de vista, siendo uno de los relevantes el económico; en ese sentido la Informática se ha convertido en el nuevo paradigma que se constituye a la vez como una herramienta de poder."* En El Delito Informático Electrónico de las Telecomunicaciones y de los Derechos de Autor, ed. Ibáñez 2012, p. 49

[22] Una encuesta de Consumo Digital publicada por el periódico El Espectador el 14 de febrero de 2013 reveló el aumento del consumo de los servicios de internet en Colombia en los últimos años. La encuesta mostraba

todo tipo de mercado en internet: *"deremate.com", "mercadolibre.com", "amazon.com", "e-bay.com", etc.* que terminaron optando por este modelo de negocio.[23]

Por otro lado, el avance de la tecnología aumenta día a día la cantidad de posibilidades de utilización de la red, de los servicios, de disponibilidad de la información; elementos que se traducen en rapidez, inmediatez y eficacia, y que han sido factores determinantes en el crecimiento de este fenómeno y en la importancia que ha generado, principalmente en el mundo de los negocios.

Sin duda, el hecho de que el *boom* del internet se haya dado de esa forma como un fenómeno emergente e incidente en la sociedad, que comenzó a hacer parte de la vida cotidiana de las personas, trajo consigo una cantidad de nuevos problemas que a lo largo de estas dos décadas de evolución, hemos tenido que tratar de resolver. Esta aclaración se hace, como quiera que, si bien es cierto que el derecho tiene que ir a la par del avance social, el "boom" del Internet cada día nos lleva hacia fronteras que ni siquiera nos habríamos planteado o imaginado, por lo que este ejercicio de adecuación del derecho a la informática se vuelve cada vez más difícil.[24]

III. De la seguridad

Hemos mencionado que la información ha adquirido un especial valor en la sociedad moderna. Las posibilidades de acceso a ésta, han aumentado para todos. Esto tiene implicaciones positivas muy importantes, en punto de velocidad de comunicación, de accesibilidad y producción de la misma. Pero el hecho de poder acceder a la información de una forma tal que se encuentra al alcance de todos, trae consigo el problema de dejarla en una altísima situación de vulnerabilidad. De allí que, los

como el 54 % de los colombianos que usan internet, lo hacen todos los días y en un promedio de 2,6 horas de navegación aproximada. Así mismo señaló que, el 64 % de las casas en las ciudades con poblaciones superiores a las dos mil personas tienen acceso a internet. Finalmente, de la población encuestada se concluyó que el 71 % de esas personas acceden a internet desde sus casas y el 20 % desde cafés. Artículo consultado el 17 de agosto de 2014. Ver link: [http://www.elespectador.com/tecnologia/encuesta-revela-aumenta-el-uso-de-internet-entre-los-co-articulo-404845]

[23] PEÑA VALENZUELA, DANIEL. Aspectos legales de internet y del comercio electrónico. 2001 p. 25

[24] Es así como ha ocurrido con lo que hoy en día se conoce como computación en la nube o cloud computing.

desarrolladores de sistemas (software y hardware), trabajen permanentemente en el desarrollo de sistemas de seguridad que puedan garantizar la protección y la seguridad misma de la información con la finalidad última de poder asegurar las garantías fundamentales de quienes navegan en internet.

En la red es posible encontrar infinidad de conductas delictivas y de peligros que pueden atentar contra la información. En realidad el problema apunta a la noción de confianza. El hecho de que confiemos nuestra información a la red, se debe a que creemos que en cierta medida la información que dejamos librada a un sistema informático está segura y que las posibilidades de violabilidad de la información son bajas, como ocurre, verbigracia con la información que guardamos en nuestros correos electrónicos.[25] La confianza en los sistemas informáticos puede ser el aspecto más importante que toca directamente lo que compete a la seguridad, pues, dado que se trata de un servicio que está diseñado para las masas, este debe ofrecer la garantía de su correcto funcionamiento, en cuanto a lo que se refiere a la protección de la información y a la eficacia de funcionamiento de los servicios prestados allí mismo.[26] Es, si se quiere, una renuncia condicionada al control sobre la información que queremos compartir.

De acuerdo a lo anterior, hemos encontrado que la primera dificultad para acercarnos al concepto de los delitos informáticos es la tan mentada "cifra negra"[27], que no es cosa diferente que la cantidad de delitos que se cometen a diario en la red, de robos de información, de accesos a bases de datos ajenas, de destrucción, modificación o alteración de la información, etc.

Es decir, si se hiciera un análisis estadístico de la criminalidad informática, podría encontrarse que es sencillamente imposible hacer al menos un cálculo aproximado, pues no es solo la dificultad de medir con precisión la cantidad de crímenes en la red, sino que las mismas compañías y los mismo actores fuertes de la red se

[25] PEÑA VALENZUELA, DANIEL. XXXII Jornadas de derecho penal. 2010 Derecho de la seguridad de los sistemas de la información: parámetros para la construcción del ciberdelito.

[26] Es así como se ha constituido lo referente a los pánicos financieros, que aunque tocan directamente un hecho distinto, se asemejan al hecho de que la confianza es lo que determina el funcionamiento de los sistemas financieros e informáticos.

[27] Cita ALBERTO SUAREZ SANCHEZ, La estafa informática, Grupo editorial Ibáñez, ed. 2009,

encargan de esconder estos resultados como medida preventiva a la pérdida de confianza en sus sistemas informáticos y sus bases de datos. Imagínese la situación a que daría lugar que un banco confesara que sus sistemas no son lo suficientemente fuertes y por razón de ello, han sufrido alteración en sus balances financieros, o que a través del acceso irregular a su infraestructura, se produzcan transferencias no consentidas de activos financieros de particulares; esto tendría un efecto inmediato de desconfianza que llevaría directamente a las personas a cambiar de asesor bancario donde su dinero esté mejor asegurado.

Lo mismo ocurriría con las empresas que hacen contratos de "hosting" para manejar sus servicios e infraestructuras de venta por internet y/o alquilan servidores en la nube (de Cloud Computing) por ejemplo, para almacenar y procesar su información. El hecho de saber que la información importante de una empresa está siquiera cerca de poder ser atacada, implica un aspecto directo de desconfianza que lleva a que los diferentes consumidores de servicios en internet prefieran acudir a otras formas de comercio, y de protección de su información.

En conclusión, al menos en lo que se refiere al aspecto de la seguridad, encontramos que se presenta una dicotomía de acuerdo a la protección de datos y de su correcto funcionamiento, pues, por un lado, interesa saber cuáles y como son las conductas que se cometen de forma repetitiva en internet para evitarlas, pero el hecho de denunciar esta información conlleva implícito un elemento deslegitimador de los sistemas informáticos que lleva a los usuarios a pensar en la no conveniencia de dejar su información libre en la red.

En definitiva, el aspecto de la seguridad toca un punto tanto sociológico como técnico, el primero cuando se trata de mantener en constante funcionamiento los sistemas informáticos con la participación de los usuarios; y el segundo de mantener siempre vigentes sistemas de seguridad que comprendan una mayor garantía para la protección que debe tener la información. Simplemente para dejar a manera de interrogante, se pregunta: ¿que podría pensarse a nivel de responsabilidad penal, con aquellos *Internet Service Providers* (ISP), *hosters,* y en general todas aquellas compañías de servicios de internet que están encargadas de mantener los

parámetros de seguridad para la protección de la información, cuando tratamos de analizar el problema desde un punto de vista de protección de información, con posiciones de garante por asumir los riesgos que implica la prestación de los diferentes servicios?[28]

En resumen, quienes alimentan la red con información de terceros, se encargan del control para evitar el acceso ilegal a la información a través del mejoramiento de sus sistemas de seguridad a través de la prevención, en vez de dejar en manos del Estado la prevención y la sanción para no perder confianza y con ello usuarios de la información.

IV. De la sociedad de la información

La sociedad de la información, aunque valga la aclaración, es un concepto más amplio de lo que aquí se expone, es la sociedad que pertenece y depende de la conectividad a internet y sus servicios para poder funcionar normalmente, es decir, que gracias a las posibilidades tecnológicas ofrecidas e insertadas en el sistema, la nueva sociedad está obligada, depende y debe acudir siempre a los servicios que están dispuestos *"on-line".*

"Colombia aún no se ha insertado de manera plena en la sociedad global de la información y el conocimiento; no obstante, se debe reconocer que se están dando pasos tácticos y estratégicos para ello. El gobierno y el sector privado parecen conscientes de la necesidad de lograr ese objetivo y a través de él conseguir una mayor competitividad para el sector productivo y para el país en general. También se pretende disminuir la brecha digital y, por ende, que la mayoría de ciudadanos colombianos tenga acceso a Internet, por cualquier medio o infraestructura a su

[28] JORGE FERNANDO PERDOMO, en su artículo sobre "Pornografía infantil por internet", se dirige hacia el mismo planteamiento cuando sostiene que: *"Se puede decir, sin lugar a dudas, que de acuerdo a esta normatividad, los oferentes de servicios tienen una posición de garante de evitación del menoscabo al derecho a la integridad y formación sexuales del menor, de manera que si este incumple porque se aloja dicho material o no se toman las medidas para evitar que otra persona lo haga, podría pensarse, en alguna forma, de responsabilidad penal.",* p. 168

alcance, y así a los contenidos digitales y a los servicios de la nueva economía digital tales como e-medicina y e-educación."[29]

A diario encontramos más y más productos electrónicos diseñados para que estemos en permanente conexión con la red. Los desarrollos tecnológicos han traido como resultado la disminución de los costes de accesibilidad y conectividad a estos servicios, lo que lleva implícito el hecho de que día a día sea mayor la cantidad de población que pueda acceder a Internet y por ende, hacer parte de la sociedad de la información.

Como se señaló en la cita anterior, Colombia está trabajando en mejorar de forma estratégica y técnica estos aspectos, elemento que tiene incidencia directa en el desarrollo de políticas de gobierno, de economía y en general del desarrollo y avance social. Eso significa que camino al desarrollo, nos volvemos al mismo tiempo más vulnerables en la protección de la información.

Pero eso no es todo. La sociedad de la información tiene otros problemas adicionales que obligan a examinar patrones diferentes del comportamiento humano con incidencia en el campo del derecho. Se generan adicciones y problemas reales que se desprenden de la cantidad de tiempo que pasamos allí, como por ejemplo, los jóvenes que se comienzan a apartar de la sociedad real por el hecho de gastar tanto tiempo navegando en la red, bien por la ansiedad que despierta tener la información al alcance o bien por el acceso cada vez mas popular a las redes sociales a través de páginas como facebook, twitter, myspace, second-life, Windows Life Msn, etc. lo que implica una esfera de doble generación de necesidad de acceso a la red, pues ya no solo los gobiernos intentan disponer de servicios para la comunidad de forma digital[30], sino que las personas en su afanosa necesidad de pertenecer a la red, comienzan a aportar a esta todo lo que puedan, en este caso, su información.

---

[29] PEÑA VALENZUELA, DANIEL. La sociedad de la información y la ley de tecnologías de la información y las comunicaciones. Obra, Comentarios a la ley de tecnologías de la información y las comunicaciones – TIC (ley 1341 de 2009) Pg. 199

[30] En el mismo sentido, JUAN DAVID BAZZANI MONTOYA. Sociología cibernética. Obra, Los blogs jurídicos y la web 2.0 para la difusión y la enseñanza del derecho. 2010 Pg. 283

Es así como ahora no solo la información de grandes empresas, o negocios, o gobiernos se encuentra en la red, sino que incluso los datos más íntimos y personales de cada persona se encuentran por ahí en la nube dando vueltas, al libre albedrío de quien los quieran utilizar.

De acuerdo a estos elementos debe analizarse cómo la sociedad de la información es uno de los presupuestos básicos para argumentar la necesidad de una regulación jurídico-penal respecto de la criminalidad informática, pues es una clara muestra de cómo no es un selecto sector de la sociedad la que está sujeta a estas conductas, sino que por el contrario, como se intentó demostrar arriba, la sociedad hoy pertenece a la red, y es ésta – la red- quien dicta las reglas de convivencia de la actualidad, por lo que el derecho debe estar a la vanguardia y entrar a regular todas las conductas que allí se desarrollen, pues solo de esa manera se puede proteger la legitimidad de los sistemas informáticos del boom del Internet y de los usuarios.

En ese sentido, es necesario repensar nuestro ordenamiento jurídico, no ya únicamente desde el derecho penal, sino desde todo el sistema constitucional de principios y valores para readecuarlo a la sociedad moderna de la información y poder ofrecer protecciones jurídicas suficientes a las necesidades de nuestra sociedad.

V. La legislación colombiana solo protege el acceso de la información pero no protege el uso que se dé a esa información.

En Colombia se ha trabajado de forma intensiva en controlar y regular jurídicamente todas las situaciones que se presentan en internet, sin embargo, a pesar de los buenos esfuerzos el trabajo sigue siendo insuficiente frente a la multiplicidad de situaciones que pueden ocurrir en la web.

La Ley 1273 de 2009 conocida como la ley de delitos informáticos, creó varios tipos penales especiales para regular la comisión de conductas punibles a través de

medios telemáticos. Este cuerpo normativo, se estructuró sobre la base de tres pilares fundamentales para la protección de la información digital: la confidencialidad, la disponibilidad y la integralidad de la información.

Aun cuando la remisión a estas estructuras generales sobre la protección de la información digital resultó un tema novedoso para la expedición de la legislación sobre delincuencia informática, la misma omitió regular algunos aspectos que resultan esenciales en esta materia, debido a que, si bien las normas señaladas regulan todo lo relativo al acceso de la información, no abordan una regulación específica sobre el uso debido de la información.

La norma técnica ISO/IEC 2702:2005[31], desarrolla y regula múltiples aspectos sobre las políticas de seguridad informática a nivel internacional; sobre el concepto de confidencialidad de la información específicamente señala*: "[la confidencialidad] garantiza que la información es accesible, sólo para aquellos autorizados". Así mismo, sob*re la disponibilidad de la información, la legislación colombiana y las normas internacionales hacen referencia a la posibilidad de asegurar el acceso a la información en el momento que sea requerida sin que se impida éste por ningún medio. Y finalmente, por integralidad, se entiende fundamentalmente que la información no sea afectada en su composición, es decir, que no sea ni dañada ni modificada.

Consideramos que es acertada esta posición por cuanto se intenta proteger la información desde diferentes perspectivas, la pregunta que nos hacemos es: ¿sobre esos presupuestos, dónde queda regulado el uso que se le dé a la información?

Parece ser que la norma no tuvo en cuenta lo concerniente al uso de la información, únicamente se concentró en proteger la integridad, la disponibilidad y el acceso únicamente a quienes están autorizados para ello. Sin embargo, se reitera, no hay

[31] El ISO/IEC 27002:2005 es una norma técnica estándar de carácter internacional adoptada en Colombia por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) para la seguridad de la información. Esta norma fue publicada por primera vez como ISO/IEC 17799:2000 por la Internacional Organization for Standarization en conjunto con la Comisión Electrotécnica Internacional en el año 2000 bajo el nombre en inglés de *"Information technology - Security techniques - Code of practice for information security management."*

ninguna regulación específica respecto del uso indebido de la información que se haya obtenido legal o ilegalmente. Este es el aspecto fundamental relacionado con la diferencia conceptual existente entre privacidad e intimidad que se abordaba con anterioridad. El mayor caso de atentados contra la intimidad no provienen de quien accedió ilegalmente a la información, se trata de individuos que la encontraron en la red, la encontraron circulando libremente y la subieron a la red o accedieron a un grupo no autorizado pero el dueño de la información la había difundido voluntariamente.

Esta situación, es producto de haber desarrollado una legislación que estuviera pensada mayormente sobre la integridad de los sistemas informáticos que en las realidades jurídicas que proponían los sistemas informáticos. Es por ello, que aunque la norma tiene un objeto de regulación que resulta ser muy importante y avanzado en términos técnnicos para nuestro ordenamiento jurídico, ya se evidencian las falencias respecto de una serie de situaciones en las cuales los tipos penales no tienen cabida y otras que rápidamente caerán en desuso por el cambio de las prácticas en las modalidades de criminalidad informática.

El problema está formulado en términos de comprensión del objeto de regulación de la legislación[32], y es en este punto, donde el fundamento inicial de este texto –la intimidad vs. la privacidad- adquiere sentido[33].

Cuando internet no tenía un papel tan representativo en nuestro ordenamiento jurídico el objeto principal de protección era la intimidad, puesto que el interés estaba puesto sobre la confidencialidad de la información, es decir, sobre la protección de la información analizada desde la no intromisión de terceros en ella. Ahora bien, con la masificación de los medios informáticos, las dinámicas propuestas por el internet, la nube, y las redes sociales, el objeto de protección de la información pierde sentido, puesto que la información está constantemente expuesta frente a terceros y por lo tanto resulta imposible controlar el acceso a la misma. Y en tanto ello es imposible, se convierte en innecesario.

Así, las personas hoy en día están acostumbradas y aceptan el hecho de que su información pueda ser, en mayor o menor medida accedida por terceros a través de la red. Su preocupación en la actualidad es que no se proteja la privacidad de la información, entendida como ya vimos, desde la noción norteamericana, como la libertad de control sobre la misma. Esto nos lleva a un escenario en el cual el

---

[32] Esta posición es incluso compartida por la doctrina, pues algunos autores cuando se refieren a la criminalidad informática relativa a la intimidad sostienen: *"Infracciones a la intimidad: Dentro de esta área de datos que contienen información relativa a la intimidad o privacidad de las personas, siguiendo a Sieber, diferencia los siguientes grupos: a) infracciones de los derechos sustantivos de la intimidad, relacionadas con el descubrimiento, difusión, obtención, o acceso de forma ilegal de datos personales, su uso ilícito, la entrada, modificación ilegal y/o falsificación de los mismos con el propósito de causas un perjuicio, y los supuestos graves de almacenamiento, grabación o colección de datos; b) infracciones de los requisitos formales legales impuestos por las autoridades administrativas supervisoras de las actividades informáticas o telemáticas, o por disposiciones civiles o administrativas, las cuales configuran ilícitos administrativos o civiles; c) infracciones de los derechos de acceso a la información o a la libertad de información, a través de conductas como las de dar información falsa o negar a la que se tiene derecho y, d) negligencia en la adopción en las medidas de seguridad."* Tomado de: SUAREZ Sanchez, Alberto, La Estafa Informática, p. 50. Véase como cuando el autor se refiere a las infracciones sobre la intimidad, hace referencia de manera insistente sobre la protección a la intimidad desde el acceso a la información, pero no hace mención a la protección del individuo desde su privacidad y la consecuente protección de la información desde su uso. Únicamente se hace un señalamiento al uso de la información pero cuando ésta es utilizada de manera ilícita. Surge entonces la pregunta, ¿Acaso no debe haber una protección especial incluso para los eventos en los que este uso sea en principio legal?

[33] La dicotomía entre la intimidad y la privacidad, muestran como la privacidad se entiende como una forma de evolución de los intereses de protección de la sociedad. Mientras que en una sociedad que no está inundada por las tecnologías de la información y no está sometida a fenómenos elevados de exposición de información, lo importante es que se proteja el acceso a la información. En un escenario de exposición plena a la información, el interés principal está dado en términos del uso que se dé a la información.

individuo no se molesta porque su información sea accedida por terceros, sino porque sea reproducida y utilizada indebida e indiscriminadamente por terceros. Situación que adquiere relevancia en la medida en la que los medios informáticos permiten una mayor y más rápida difusión de cualquier tipo de dato a través de la red.

Muchas de las problemáticas que se presentan actualmente no están relacionadas directamente con la obtención o el acceso a la información (intimidad), sino por el contrario, con la forma y el tipo de información que sea divulgada y el uso posterior que se le de a esa información (privacidad).

VI. Dificultades del derecho penal en materia informática

A. Dificultades sustanciales

Son múltiples las dificultades que enfrenta el derecho para poder regular de forma correcta las situaciones ocurridas al interior de las diferentes sociedades. Sin embargo, la problemática se hace mucho más evidente cuando se trata de aspectos relacionados con las tecnologías de la información debido a la velocidad de desarrollo.

El problema de la criminalidad en Internet, se origina en dos causas principales: en primer lugar, por la imposibilidad empírica que enfrenta el derecho para poder regular las incipientes modalidades de criminalidad en la red; y en segundo lugar, debido a la dificultad que supone la persecución de este tipo de conductas y la ineficiencia de las instituciones para poder investigar y establecer a los autores de este tipo de delitos.

Adicionalmente, debe tenerse en cuenta que la principal dificultad en materia de delitos informáticos para efectos de la protección de la intimidad y la privacidad, está en que la legislación penal actual no está dirigida a controlar el uso que se dé a la información sino simplemente a controlar la confidencialidad (acceso), y la disponibilidad de la información. Igualmente, a la delincuencia cibernética se identifica un universo nuevo de situaciones que no son propias del mundo físico y

que político-criminalmente también podrían ser consideradas como un delito, pues a pesar de no constituir ataques a la información o a los medios informáticos, su protección resulta relevante en tanto son nuevas costumbres necesarias para el adecuado funcionamiento del comercio, la economía, etc.

A.1. Dificultades identificadas desde la tipicidad objetiva de la conducta

En Colombia se ha penalizado el acceso abusivo a un sistema informático, la obstaculización ilegitima de sistema informático o de red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitio web para capturar datos personales, el hurto por medios informáticos y semejantes, y la transferencia no consentida de activos.

Estas conductas, se han estructurado sobre la base de la protección de los sistemas informáticos y de la seguridad jurídica para su correcta utilización por la sociedad. Sin embargo, estos tipos penales están estructurados de tal forma que únicamente pueden utilizarse para los concretos casos para los que han sido creados, sin poder aplicarse en casos diversos que no se hayan contemplado en su momento por la norma.

Es conclusión, los avances tecnológicos son siempre superiores a los avances jurídicos y más veloces, y, en definitiva, el derecho no puede operar nunca a la misma velocidad que los cambios sociales virtuales. Además, el secreto propio de la fase de invensión, impide que el derecho se vaya preparando para el momento en que se estrena el nuevo instrumento en la red.

Esto genera que haya una desproporcionada y denotada desactualización de los tipos penales frente a las modalidades de criminalidad informática que se pueden encontrar en la actualidad.

Un ejemplo de esta situación es el secuestro de información cibernética; los delincuentes informáticos, tienen la capacidad para capturar toda la información de un usuario, tienen la posibilidad de apropiarse de todas sus cuentas de red, correos electrónicos, redes sociales, medios de comunicación, acceso a sitios web, manejo

de contraseñas. En esta modalidad a la víctima se le captura toda su información y se le exige una recompensa remuneratoria para devolvérsela[34].

Este caso evidencia como las normas actualmente señaladas en la legislación son insuficientes para atender esta problemática, pues se trata de una situación muy similar al secuestro extorsivo, pero que claramente no puede confundirse con un secuestro puesto que no hay una privación de la libertad física, sino que se trata de un caso de privación del acceso y sobre todo del uso de la información, a cambio de una exigencia remuneratoria.

Puede que la conducta se pueda adecuar a través de alguno de los delitos informáticos establecidos en el código actualmente, pero sería una solución parcial al problema, pues el reproche no corresponde a la complejidad de la situación criminal planteada. Tampoco resultaría lógico tratarla como una extorsión o un constreñimiento, pues se repite, lo grave no es restar autonomía al sujeto, es impedirle que utilice su propia información con el daño que a el se le produce y a los demás usuarios de la información. Ello por cuanto se trata de una conducta punible pluriofensiva que desde la política criminal del Estado debería estar protegida desde todos sus ámbitos de afectación.

Otro ejemplo que nos permitiría evidenciar el tema, es el caso actual del Bit Coin. Bit Coin, es una moneda digital que no tiene respaldo monetario en ninguna banca central ni en dinero físico. El Bit Coin es una moneda que en la actualidad ha comenzado a hacer parte natural del tráfico jurídico y comercial de los medios informáticos[35].

Esta moneda se genera a partir del préstamo de energía y capacidad de procesamiento de las maquinas que después de una enorme labor de producción

[34] Entre otros artículos relacionados: Secuestro de datos: ¿Tienes tu información respaldada?, Consultado el 18 de agosto de 2014, ver link:
[http://www.cert.uy/inicio/novedades/amenazas_y_alertas/secuestro+de+datos]

[35] Se puede consultar entre otros: ¿Un mundo sin bancos? En semana.com, ver link: [http://www.semana.com/economia/articulo/autoridades-advierten-sobre-el-uso-de-bitcoin-en-colombia/383846-3]. Así mismo, puede consultarse en Eltiempo.com, Una moneda virtual llamada Bitcoin, ver link: [http://www.eltiempo.com/archivo/documento/CMS-12753084].

generan un dato informático con un código específico del cual se guarda un registro, denominado Bit Coin.

Como quiera que esta moneda digital no tiene una regulación dirigida por ningún ente, su valor depende exclusivamente de la oferta y la demanda. En ese sentido, estamos ante un activo económico que no tiene regulación en el mercado, que no se puede entender como moneda, pero que es un bien susceptible de valoración económica real y que puede ser hurtado por hackers a través de internet y causar verdaderas defraudaciones económicas.

De hecho, la razón por la cual el Bitcoin se ha hecho famoso en el mundo no ha sido precisamente por el éxito de la salida al mercado de este activo, sino por el escandaloso hurto de Bitcoin que se produjo en una casa de cambios virtual a la cual le sustrajeron un monto de 420 millones de dólares en Bitcoin[36].

Un tercer ejemplo es lo que ocurre con los *sniffers* y los *netbots.* Los primeros, los *sniffers,* están catalogados como programas que pueden acceder a la información de un disco duro e identificar toda la información de un correo electrónico personal. Los *netbots*, son programas que operan a partir de principio de inteligencia artificial que a partir de la información recolectada por los *sniffers* pueden crear perfiles personales de los individuos y así acertar sobre el tipo de ofertas que una persona podría preferir[37]. En principio, no hay ningún problema con estos programas, salvo

---

[36] "*La moneda alcanzó titulares de primera página en las últimas semanas debido no a su éxito, sino a su más sonado fracaso, la quiebra de la casa de cambios virtual Mt.Gox, de la cual fueron sustraídos por acción de hackers 850.000 bitcoins, equivalentes a 420 millones de dólares. Las autoridades de medio mundo, incluído Colombia, lanzaron comunicados oficiales en varios países para advertir al público de los riesgos*." En ¿Un mundo sin bancos? En semana.com, ver link: [http://www.semana.com/economia/articulo/autoridades-advierten-sobre-el-uso-de-bitcoin-en-colombia/383846-3], consultado el 18 de agosto de 2014.

[37] En ese sentido, CALLE D' Alemán, Beatriz, Protección de Datos de Carácter Personal en el Comercio Electrónico. Allí sostuvo: *"Los llamados Sniffers son programas que monitorean las comunicaciones a través de la red para capturar el tráfico que circula a través de ella. Tales dispositivos permiten entrar al disco duro del computador, recoger los correos electrónicos almacenados, leerlos y ejercer control sobre a información allí contenida. Inicialmente podría pensarse que un seguimiento de tal naturaleza resulta inocuo. Sin embargo, el rastreo que se hace en diversos sitios puede combinarse, y con un software es posible hacer un cruce de datos que permita identificar plenamente a una persona y construir un perfil completo de su personalidad. Dentro de las herramientas más sofisticadas de búsqueda en la red se encuentran hoy los llamados netbots, que consisten en dispositivos con principios de inteligencia artificial, destinados a buscar ofertas de productos, comparar precios y ofrecer información clasificada según el interés y las preferencias del usuario.",* p. 246

los casos de acceso abusivo de los *sniffers* a información restringida bajo contraseñas. Pero puede considerarse aceptable que una maquina pueda utilizar toda mi información librada en la red para elaborar un perfil personal mío y así usarlo en beneficio de un tercero. ¿Qué pasa si este interés no es lícito?, ¿Qué permite que un tercero acuda a mi información para determinar mis intereses cuando esto puede implicar de alguna forma la coacción de mi voluntad?

Nótese como esta es una situación en la que hay un uso de la información privada de una persona y no está regulada por la legislación actual permitiendo, entre otras, prácticas abusivas del mercado que de forma agresiva intentan campañas publicitarias a partir de información obtenida de forma dudosa de sus potenciales clientes.

Estos son solamente algunos ejemplos que sirven para evidenciar la situación que se presenta por la insuficiencia de los delitos informáticos contemplados por la legislación actual.

Consideramos que se pueden hallar soluciones a los problemas planteados; para ello, puede acudirse a una legislación distinta que responda a tipos penales abiertos, específicamente tipos penales en blanco, que impliquen remisiones a otro tipo de regulaciones especializadas en la materia que puedan ser rápidamente actualizadas conforme a las mecánicas de criminalidad que se vayan presentando.

En materia de control a los delitos informáticos Colombia a avanzado a través de la nueva concepción del Ministerio de Tecnologías de la Información y las Comunicaciones así como la creación de la Delegada para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, entidad que aportará a la regulación en materia de protección de la información y podría ser el ente encargado de llenar los espacios en blanco de los tipos penales informáticos. No obstante, el ideal sería que centraramos la atención en la protección de la información que circula en la red y no solo en las bases de datos privadas y públicas y además, que el problema se abordara no sólo desde la perspectiva del comercio.

Ahora bien, esa regulación, tal y como se advirtió, debe contener tipos en blanco que no se ocupen exclusivamente de custodiar e impedir el acceso abusivo o la manipulación de la información protegiendo el medio informático sino la información misma, tratando de evitar su uso indebido.

A.2. Dificultades identificadas desde la antijuridicidad de la conducta

La primera situación que debe analizarse es el objeto de protección de los bienes jurídicos. La Ley 1273 de 2009, se diseñó sobre la base de la protección de la información desde sus dimensiones de integralidad, confidencialidad y disponibilidad[38]. En esencia, el legislador de la época buscaba proteger la información, pero desde su dimensión digital, desde su manifestación como sistema informático debido a su creciente y denotada importancia en la sociedad actual.

La inclusión de los sistemas de información en la sociedad moderna ha producido un cambio significativo en la forma en la que nuestra sociedad opera. La vulnerabilidad de los sistemas digitales y la sensibilidad de la información que transita por la red, ha generado que este medio se haya convertido en uno de los escenarios de mayor cantidad de ataques criminales. De allí que Colombia así como otros países haya decidido regular desde el derecho penal los ataques producidos contra los sistemas informáticos, por cuanto, éstos representan un pilar esencial del funcionamiento social actual y por lo tanto se convierten en aspecto de esencial importancia en los intereses de la política criminal de un estado.

Dicha intención marcó un hito importante para su época, puesto que por primera vez en el país se trataba de regular de manera especializada y focalizada el problema derivado de la delincuencia informática.

Sin embargo, no es difícil acertar en que la criminalidad informática es un fenómeno tan cambiante como la misma evolución de los medios informáticos. En este punto, es claro que la variación sobre los objetos de protección es de tal magnitud, que

[38] Ley 1273 de 2009, Ley sobre delitos informáticos.

incluso aquí se denota una insuficiencia desde el mismo objeto de protección del bien jurídico tutelado.

La protección desarrollada estaba dirigida a limitar y controlar el acceso a la información y no a proteger el uso de la información, ni la información en si misma, es decir, tal y como se explicó atrás, hay un enorme espectro de privacidad que no está cobijado por la legislación actual en materia de delincuencia informática.

En ese sentido, conviene reformular el bien jurídico objeto de protección penal para que sea la información en si misma y ello cobije tanto los medios informáticos como el acceso a la información y su uso indebido.

B. Dificultades procesales

Así como se presentan dificultades en materia sustancial, la delincuencia informática plantea enormes problemas a nivel de investigación criminal. Han existido avances en la consecusión de tecnología avanzada para nvestigar estos delitos. Sin embargo, esta labor plantea retos cuyas soluciones desde el punto de vista de la investigación, pueden considerarse como muy complejas y en algunos casos, incluso, imposibles.

El principal problema que se encuentra en materia de delitos informáticos está relacionado con la rastreabilidad y la trazabilidad de los delincuentes que incurren en las conductas delictivas. Es cierto, como muchos lo saben que las maquinas conectadas en la red se identifican y diferencian las unas de otras a través de direcciones IP (*Internet Protocol*) que permiten rastrear la actividad de una maquina en cualquier momento en la red.

Estas direcciones IP, permiten identificar las horas en las que una maquina se conecta, el lugar donde está ubicada, las actividades que realizan, etc., y están cobijadas por unos mecanismo que registran de forma casi infalible la actividad producida desde una maquina en la red.[39]

[39] En el mismo sentido, CALLE D' Alemán, Sol Beatriz, señaló: "Lo que si puede ser objeto de regulación por este tipo de normas son las conductas tendientes a interrelacionar direcciones IO, con el fin de crear perfiles del individuo. En efecto, a través de programas informáticos es posible saber, por ejemplo, el proveedor del

Sin embargo, debe recordarse que las maquinas no delinquen, sino que por el contrario son las personas quienes incurren en conductas delictivas. Por lo tanto, un primer paso es rastrear la máquina, pero lo segundo, y lo más difícil en la mayoría de los casos, es identificar quien es el responsable de ejecutar la conducta delictiva a través del servidor.

Esta situación se agrava, si se tiene en cuenta la gran cantidad de equipos que existen en la actualidad que no tienen un dueño identificable, es el caso de los sitios de acceso a internet público (café internet), los equipos hurtados como celulares, portátiles o tablets hurtados que se usan para cometer conductas delictivas además de la gran cantidad de situaciones en las cuales se aprovechan los descuidos de algunas personas para cometer delitos desde servidores personales, de trabajo o privados.

Eso genera unos problemas enormes cuando se trata de la judicialización de los delincuentes informáticos, lo que dificulta enormemente la persecución de estas conductas.

La única forma de controlar dichas situaciones es estableciendo controles que aseguren el conocimiento del usuario del equipo, cuando el mismo pueda ser accedido por distintas personas, claves dactilares, visuales, en fin, mecanismos que ya están al alcance de la sociedad y que deben ser implementados como una obligación de los usuarios.

La situación es tan grave, que incluso la criminalidad informática refleja un fenómeno social muy delicado en términos de persecución penal, esto es, la denominada popularmente “cifra negra.”

servicio de internet, el país en que reside, el titular del servicio, la hora, fecha y día en el cual hizo conexión, la maquina desde la cual accedió y, en fin, toda una serie de datos para formar bases a partir de las cuales se puede hacer un uso inadecuado o violatorio de la intimidad.” En *Protección de Datos de Carácter personal en el comercio electrónico,* Sociedad de la Información Digital: Perspectivas y alcances, Compilador Daniel Peña Valenzuela, ed. Universidad Externado 2006, pp. 243-244

Este dato corresponde al elevado número de denuncias que no llegan a los entes investigadores y acusadores debido al bajo incentivo que hay en la población para denunciar estas conductas.

La situación se presenta por cuanto, la sociedad es consciente de las dificultades que hay para que un caso de delincuencia informática tenga éxito por lo cual empresas y bancos, entre otros, prefieren no hacer de público conocimiento una defraudación informática para que sus clientes no se sientan en un escenario de desconfianza que pueda afectar a la empresa. En ese sentido, convendría pensar en hacer obligatoria la denuncia, con independencia del delito que se haya cometido y de la disponibilidad sobre el bien jurídico y en la centralización de un observatorio de conductas criminales informáticas que permita estar cerca de los avances de la criminalidad informática a las autoridades encargadas de efectuar el control.

C. **Situaciones que actualmente no están reguladas por el derecho penal. (Puntos grises)**

Existen un sin número de manifestaciones que tocan con la intimidad y que no son objeto de protección actualmente. Un ejemplo lo constituye el denominado derecho al olvido que se puede considerar como uno de los derechos producto de la sociedad de la información. Gracias a las posibilidades de comunicación que hoy en día nos ofrece la tecnología, mantenernos informados y acceder a la información se hace mucho más sencillo y rápido.

Así mismo, la velocidad y la capacidad exponencial en la que hoy crece y circula la información, lleva que la misma se comporte de forma distinta y por lo tanto genere consecuencias diferentes en la sociedad.

El derecho al olvido se ha forjado como un derecho a través del cual, las personas tienen la libertad y el derecho de elegir que quieren que pase con su información, sobre todo la información de contenido negativo, incluyendo el elemento temporal.

Es posible que una persona tenga cierta información no deseada o que sencillamente no quiera compartir con los demás, pero que debido al derecho de información la misma pueda ser comunicada y expresada al resto de la sociedad.

Aun a pesar de esa situación, lo que si debe quedar claro es que las personas no están obligadas a que esa información se conozca de forma indefinida y que se mantenga circulando permanentemente de tal manera que pueda afectar su imagen frente a la sociedad de por vida.

En estos términos se expresan Patricia Abril y Eugenio Pizarro sobre el derecho al olvido:

> *En este entorno y con las manifestaciones que acabamos de hacer, se va abriendo paso —no ciertamente, una nueva noción de privacidad— sino más bien un derecho retrospectivo (con carácter retroactivo, diríamos jurídicamente) para cribar aquellos datos personales susceptibles de minar los derechos de la personalidad: honor, intimidad e imagen. Pero, ¿cómo y para qué instaurar ese derecho? "No creo que la sociedad entienda lo que sucede cuando todo está disponible, listo para ser conocido y almacenado indefinidamente"22. Es probable que haya pasado ya el tiempo en que teníamos poder de disposición y control absoluto sobre nuestra intimidad; es probable que uno de los efectos colaterales de la banalización de la información que se publica en la Red sea una pérdida irremisible de una intimidad que, no sólo ha dejado de pertenecernos en parte, sino que —es probable—cuando queramos recuperarla, se encuentre ya grabada con tinta indeleble en cualquier computadora del mundo: con estos parámetros, ¿podemos pretender que se instaure un derecho al olvido o a ser olvidado (right to be forgotten-right to oblivion) haciendo un borrado selectivo de la información online que —presuntamente— nos perjudica?*

La forma a la que nos vemos expuestos hoy a la información, nos lleva indudablemente a un escenario en el cual el control sobre nuestra intimidad es casi imposible de ejercer, sin embargo, ello no nos obliga a aceptar las situaciones a las que nos expone. En ese sentido, debe limitarse esta intromisión, pero ya no vista desde la afección a la intimidad sino analizada desde el derecho a la privacidad y por lo tanto a que mi información no sea constantemente divulgada ni socializada, pues debe garantizarse mi derecho a mantener ciertas situaciones en mi orbita de

conocimiento personal. Es la posibilidad de recuperar el control sobre la información a posteriori.

Eso es lo que ocurre con un gran número de los resultados en las búsquedas de motores de búsqueda, donde permanece perenne información que a pesar de ser cierta y que corresponda a un ejercicio del libre derecho de la información, no puede dejarse de forma indefinida en el tiempo por cuanto podría afectarse gravemente a las personas involucradas. Es lo mismo que crear un antecedente perpetuo de conducta socialmente desaprobada.

Un precedente importante lo constituye el reciente pronunciamiento del Tribunal Superior de Justicia de la Unión Europea el pasado 13 de Mayo de 2014, que le ha ordenado a Google que retire de sus motores de búsqueda información que ya no es suficientemente útil socialmente pero que causa un grave perjuicio a una persona por mantener de forma indefinida información que la afecta y le otorga el derecho a las personas de solicitar directamente a Google el retiro de los criterios de búsqueda para que no seleccione esa información. Es un avance en tanto el responsable de incluir la información no es el único destinatario de control para proteger a la persona perjudicada con una información sino que quien la selecciona y la arroja al usuario también es responsable, incluso frente a información legítimamente introducida a la red. Si bien es cierto, a partir de allí se han presentado cantidades de solicitudes de personas perjudicadas para que se retire cierta información existe una realidad. Resulta imposible responder en un tiempo breve tantas solicitudes, el hecho resulta publicitado y con ello hay un daño mayor y no existen criterios objetivos para resolver el conflicto entre el derecho de la sociedad a estar informada y el derecho de la persona a que se retire su información del motor. Además, la información no desaparece, porque el motor no tiene disponibilidad sobre la misma ya que le pertence a la red, lo único que se le puede pedir al motor es retirar los criterios de selección para que no la ordene y se la arroje a los usuarios y, finalmente, dicha omisión no tiene consecuencias penales hasta no estar contenida en una orden judicial.

Muy famoso se ha hecho en este aspecto, lo ocurrido con las famosas 'listas negras' de pasajeros, donde las aerolíneas crean bases de datos donde incluyen a las personas que han manifestado insatisfacción por los servicios prestados para limitar su relación con las aerolíneas en futuras ocasiones.

La Corte Constitucional colombiana en distintos pronunciamientos se ha referido a la materia, vale la pena destacar al respecto la sentencia de tutela T- 987 de 2012 en la cual el alto tribunal descalifica que las aerolíneas consoliden bases de datos con información exclusivamente desfavorable para denegar la prestación del servicio público a los pasajeros. En dicho pronunciamiento la Corte señala que el habeas data funge como un límite a dicho manejo de la información y tilda estas prácticas como abusivas sobre el manejo de los datos personales.

Como consecuencia de ello, la corporación se ha pronunciado respecto de algunas empresas ordenando la eliminación de estas bases de datos por atentar contra el derecho del buen nombre de las personas así como por la privación injustificada al acceso de un servicio público. No obstante, obsérvese que el fundamento es limitado ya que reposa en el habeas data y no en la privacidad en general ni en la protección de la información en si misma.

Todo esto está dirigido a mencionar simplemente, que en efecto a nivel constitucional ya se reconocen otras manifestaciones de los derechos fundamentales que son producto de la sociedad de la información y del manejo de las tecnologías y la red. Aun cuando ya se está trabajando en una protección por vía constitucional de estos derechos, esta situación evidencia como el derecho penal aún no ha podido percibir el fenómeno desde su órbita de acción y por lo tanto no ha podido desarrollar una legislación coherente que permita abordar el tratamiento de estos fenómenos. Claro está, antes de emprender la tarea, convendría reformular el objeto mismo de protección en la Constitución Política, desde la perspectiva de la intimidad, la privacidad y la información.

VII. Conclusiones

- La evolución de las tecnologías de la información y, en general de toda la informática se presenta como un fenómeno que nos ha llevado indudablemente a lo que podríamos considerar como una “sociedad de la información”.

- Esta sociedad de la información en la que nos vemos involucrados exige que el derecho y los operadores jurídicos deban repensar todo el sistema normativo para ajustarlo a las nuevas situaciones que se presentan con los nuevos fenómenos sociales que se derivan de las posibilidades que nos ofrece la tecnología.

- En esa medida, específicamente el derecho penal juega un papel muy importante, y es evidente que a pesar de los incansables y buenos esfuerzos todavía nos queda mucho trabajo por hacer y un largo camino por recorrer para poder adecuar nuestras instituciones jurídicas a las necesidades que este fenómeno exige.

- Un ejemplo claro de la evolución de los derechos y de su comprensión dentro del ordenamiento jurídico, es la ocurrida con el desarrollo de los derechos a la intimidad y al *privacy.* Adquiriendo este segundo un papel importante en este nuevo esquema social.

- Para poder atender los problemas de delincuencia informática debemos pensar nuestra legislación penal de forma distinta, de tal forma que nuestros tipos penales puedan adecuarse constantemente a las nuevas modalidades de delincuencia que aparecen para que no pase lo que actualmente ocurre: cuando el derecho penal logra regular una situación de criminalidad informática, por lo general, la modalidad criminal ya ha migrado a otras formas más complejas, más avanzadas y más difíciles de regular.

- Como se evidenció en la actualidad ya se presentan múltiples escenarios en los cuales resulta evidente que el derecho aún no tiene una correcta regulación. Así las cosas, deben analizase las nuevas tendencias, como ocurre con el derecho al olvido, para poder regular todas las nuevas problemáticas jurídicas y que el derecho penal estudie si debe tomar o no, parte en la discusión.

- Así mismo ocurre con la capacidad de análisis criminal que nos propone enormes retos en términos de autoría y participación y nos exige repensar nuestras estructuras jurídicas para poder judicializar y hacer responder a los criminales por estos comportamientos.

- En ultimas, lo único evidente es que el trabajo es arduo, exige cambios metodológicos, dogmáticos y prácticos a nivel constitucional, legal y procedimental para que en algún punto nuestro ordenamiento jurídico pueda ofrecer un escenario de seguridad real a las personas que participan de esta denominada sociedad de la información.

- Finalmente, de manera inevitable tendremos que irnos acostumbrando a que cada día se reduce más el espectro de intimidad y que algún día va a desaparecer. Solo nos quedará preocuparnos por qué se hace con la información y no por cómo se obtiene. Estamos cerca de que cualquier persona se acerque y con un dispositivo pueda saber que pensamos y que sentimos, como lo relatan los últimos avances de la neurociencia y ello seguramente será compartido en la red. Valdrá la pena seguir preocupándonos por el acceso a la información?