El delito de la suplantación de páginas web para capturar datos personales y el hurto por medios informáticos: necesidad y distinción.[*]

The crime of the impersonation of web pages to capture personal data: need and distinction.

David Nayib Puentes Beainny[**]

Resumen

En el mundo actual globalizado, encontramos nuevas formas de propiedad de las personas, hecho determinado por los avances tecnológicos. A su vez, se presentan nuevas formas de violentar estos derechos mediante conductas delictivas, razón por la cual es necesario identificar las normas aplicables a estos delitos y su desarrollo jurisprudencial, con el fin de distinguir la necesidad de la tipificación de estas nuevas conductas, y el acople con el desarrollo normativo internacional.

El trabajo intenta presentar y dar una posición respecto a las circunstancias que generan problemas al momento de estudiar estos nuevos delitos, como la confusión entre estos ellos y otras conductas delictivas, y la autopuesta en peligro por parte de la víctima; circunstancias que generan un mal desarrollo y aplicativo de la norma ante un escaso análisis jurisprudencial al respecto.

Abstract

In today's globalized world, we find new forms of ownership of people, a fact determined by technological advances. In turn, new ways of violating these rights through criminal behaviors are presented. Reason why it is necessary to identify the norms applicable to these crimes and their jurisprudential development and coupling with the international regulatory development, in order to distinguish the need of the classification of these new behaviors, as to present the circumstances

[*] El presente artículo se desarrolla dentro del semillero de investigación en política pública y control fiscal de los grupos Socio Humanística del derecho y Derecho Público Francisco de Vitoria dentro de la línea de corrupción en el programa de Derecho de la Universidad Santo Tomas. Sede Bogotá.

[**] Estudiante de pregrado de la Universidad Santo Tomas Facultad de Derecho, semestre X, perteneciente al semillero de investigación en política pública y control fiscal de los grupos Socio Humanística del derecho y Derecho Público Francisco de Vitoria dentro de la línea de corrupción. Correo electrónico davidpuentes@usantotomas.edu.co - davidpbeainy@gmail.com

that generate problems at the time of studying these typical adjustments of behavior, such as the confusion between criminal behavior or the actions of the victims of these grievances.

Palabras calve

Delito Informático, propiedad, globalización, tecnología, jurisprudencia.

Key Words

Computer crime, property, globalization, technology, jurisprudence.

Introducción

Podemos observar en el mundo actual un fenómeno que ha abarcado todos los ámbitos de las vida de la humanidad, siendo estos el económico, político, social, etc.; dicho fenómeno es conocido como la globalización, el cual a grandes rasgos, surgió de la aplicación de las nuevas tecnologías de información masivas, principalmente la internet, la cual es el punto de partida para nuevas concepciones de la forma de compartir información, bienes y servicios, sin la necesidad de la presencia física de los sujetos quienes pretenden realizar diferentes negocios jurídicos.

Ante el avance tecnológico e informático, la concepción del derecho de propiedad ha variado y se ha ampliado de forma significativa, logrando establecer que no solo existe la propiedad física sobre los bienes, sino una propiedad informática y de información, la cual no es visible por los sentidos pero que evidentemente hace parte del patrimonio de las personas.

Con esta nueva y ampliada forma de la propiedad privada, se presentan a su vez nuevas posibilidades de violentar dicho derecho. Entre ellos, encontramos la suplantación de sitios web para la recopilación de datos personales o el hurto por medios informáticos, el cual deberá ser establecido como otra forma de apropiarse de los bienes de una persona determinada. Así es que vemos que la información se ha convertido en un “bien” del cual dependen mucho los seres humanos, pues es a partir de ella que podemos realizar cualquier actividad en el mundo actual: cuentas de correo electrónico, cuentas de bancos, perfiles de redes sociales y las respectivas contraseñas de todos estos mecanismos electrónicos, son ahora el objetivo predilecto de aquellos delincuentes.

Por ello, el propósito de este artículo es poder evidenciar la necesidad de la creación de nuevos tipos penales, como lo son los delitos informáticos, haciendo énfasis en la suplantación de páginas web para captar información y el hurto informático. Se especificará, gracias al establecimiento de la propiedad informática y de información, el bien jurídico tutelado que se ve afectado por el tipo penal de la suplantación de páginas web para la recopilación de datos personales, y el hurto informático, presentando y poniendo en un estado de relevancia dicha conducta punible, que será estudiada desde la legislación colombiana y legislación internacional, siendo esta relativamente nueva y que por su parte, se actualiza constantemente debido al avance de la tecnología, además de prestar mayor atención al desarrollo jurisprudencial, que es la parte relevante de este escrito.

El derecho penal colombiano no ha quedado inerte ante estas circunstancias y por ello ha establecido tipos penales específicos a fin de proteger a la población del riesgo que inherente al manejo de las nuevas tecnologías y avances tecnológicos.

En el presente trabajo estará dividido en tres partes fundamentales, en un primer momento, se estudiará, analizará y comprenderá, cómo los avances científicos y tecnológicos, derivados del fenómeno de la globalización y la nueva forma de propiedad, han provocado la necesidad de la creación de nuevos tipos penales en Colombia, como los delitos informáticos. En un segundo momento se analizará la necesidad de la creación de estos nuevos tipos penales y las diferencias que existen entre éstos y los tipos penales que denominaremos “clásicos”. Por último, y en el tercer momento, analizaremos los artículos 269G y 269I, desde su jurisprudencia nacional e internacional.

Globalización y propiedad

Doctrinariamente, disponemos en primera medida de aspectos relativos a la propiedad y la globalización. Con respecto al análisis de la propiedad privada, hemos de tener en cuenta y dejar claro en qué consiste este derecho, por tal motivo, es necesario recurrir a la doctrina tradicional, encabezada por Valencia Zea (2016), quien realiza todo un estudio del derecho civil, en donde evidentemente se trata el tema de la propiedad y de los bienes. Dicho autor expone un concepto necesario en este trabajo pues pone de manifiesto una problemática a la propiedad, indicando que las relaciones que se presentan en el Derecho en donde una persona tiene relación con un objeto es una contradicción a las relaciones normales que son por regla general entre personas o sujetos

de derecho y que el ordenamiento jurídico se encarga de regular dichas relaciones en el sentido del surgimiento de derechos y sus respectivas obligaciones.

A su vez, Franceso Galgano (2005) nos presenta una mirada de lo que es a globalización y su relación con el derecho en la obra "*La globalización en el espejo del derecho*", el cual indica que la globalización, más allá de ser un fenómeno económico, es el resultado del derrumbamiento de las barreas comerciales y la aplicación del mercado como entidad superior de lo político, que transforma al derecho en un derecho universal, el cual no escapa de los avances tecnológicos.

Por su parte, Ulrich Beck (2004), y su obra *"¿Qué es la globalización?: falacias del globalismo, respuestas a la globalización*", indica la relación inescindible entre la globalización y la información; afirmando que ésta última, no puede ser limitada por el Estado, y por el contrario, Estado debe una protección a este bien denominado "universal".

Contexto Colombiano

El establecer de los delitos informáticos, son de reciente incorporación a la legislación colombiana. Nuestro país, al estar en vías de desarrollo, no cuenta con grandes avances tecnológicos e informáticos en relación a otros países, y por tal motivo, hasta hace poco, no se vio afectada por estas modalidades delictivas. Esa es la razón por la tardía incorporación de estos tipos penales en nuestro sistema positivo.

De esa forma se introducen las modificaciones al código penal mediante ley 1273 de 2009, y posteriormente el artículo 235 del Código de Procedimiento Penal, la Ley 1621 de 2013 que la del Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y otras disposiciones como la Ley 1581 de 2012 que dicta disposiciones generales para la protección de datos personales y la Ley 1266 de 2008, que regula el tema del Habeas Data y la información financiera.

En lo relativo al tipo penal del hurto informático, son varios los autores que han intentado realizar una delimitación conceptual de los delitos informáticos, como lo hace Leyre Hernández Díaz (2009) en "*El delito informático*" indicando que por el hecho de que en la actualidad todo se realiza mediante computadores y redes masivas de telecomunicación de datos, cualquier delito se debería considerar como informático, indicando al final que las conductas delictivas relacionadas con

sistemas informáticos son muchas y heterogenas, o Fernando Miró Llinares (2012) y su obra "*El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio*", dice que el cibercrimen, es una conducta delictiva realizada en el ciberespacio, para el cual es necesario que el uso de la tecnología y la información se relacione intrínsecamente con el delito a realizar, pues no todo uso de la tecnología configura un delito informático.

También se tendrá en cuenta la perspectiva de la afectación al derecho de intimidad planteado por María Fernanda Polo Castro (2009) en "*Los delitos informáticos: conflicto entre el derecho al honor y la intimidad y el derecho a la información*", donde manifiesta que son delitos informáticos todas las acciones u omisiones que sean típicas y antijurídicas, las cuales tengan como objetivo de atentado a la información o a las bases de datos o mecanismos que realicen su almacenaje, con el propósito de obtener un beneficio personal propio o causar un detrimento a los sujetos que tienen la información. Y con respecto a la intimidad, la misma autora señala que el derecho a la intimidad tiene como propósito mantener alejada la vida privada de las demás personas, sin que exista algún tipo de interferencia. Además, aparte de mantener alejados a los terceros, también tiene como meta que las personas sean cuidadosas con su información y datos privados que la afecten directamente. Por otro lado, Ricardo Posada Maya en *"El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual*" (2017), plantea la necesidad de la ampliación del concepto de propiedad a un concepto de propiedad virtual, caracterizada por la intangibilidad, potencia y necesidad de protección y regulación.

Sin embargo, el concepto más importante doctrinariamente es el de Posada Maya (2017) quien indica que los delitos informáticos ponen el peligro la "*seguridad informática*", sin tener en cuenta que pueden afectar otros bienes jurídicos. No se trata de delitos "*comunes o clásicos*", sino delitos específicos que se caracterizan por los métodos tecnólogos e informáticos, para lo cual se requiere una destreza, que se suma al ámbito virtual, afectando objetos intangibles y rompiendo los paradigmas teóricos y probatorios.

La insuficiencia de los tipos penales clásicos y la Necesidad de los tipos penales informáticos

Se ha discutido el porqué es necesario que se cree y especifiquen estos nuevos tipos penales (entre ellos el hurto por medios informáticos), puesto que estos podrían ser considerados como un agravante de los tipos penales clásicos. Es pues necesario que se establezca la relevancia de estos nuevos tipos penales, que, por el momento, diremos, van acorde al desarrollo tecnológico mundial.

Ante la importancia de la información en los tiempos contemporáneos y la insuficiencia de las regulaciones clásicas, se ha decidido en varios países, otorgarle a la información, la calidad de bien jurídico protegido. En ese sentido, el Código Penal Colombiano introduce este nuevo bien jurídico mediante ley 1273 de 2009. Esta norma sigue las directrices de convenios internacionales sobre la cibercriminalidad como el de Budapest del 2001; sobre este aspecto, Rodríguez Arbeláez (2011) señala que la ley 1273 de 2009 ha permitido el ingreso de Colombia en la protección económica y financiera que son ámbitos sometidos al cibercrimen, pues con el trabajo de delimitación de este tipo de conductas, se puede lograr una eficiencia en el control de amenazas.

La exposición del proyecto de ley y sus posteriores debates se guiaron desde su introducción, que fue presentada ante el Congreso de la Republica con fundamento en el texto creado por el juez Alexander Díaz, apoyado de los señores Fernando Velásquez y Jarvey Rincón, ambos teóricos del derecho, con el objetivo de facilitar la distinción y aplicación de nuevas conductas delictivas que debían ser consideradas como tipos penales (Arzuaga, T. 2013. p18). La ley con los nuevos tipos penales y el bien jurídico tutelado, eran necesarios entonces porque, en concepto de los creadores de la norma, existen personas que hacen uso de sus talentos en el manejo de los sistemas informáticos, para afectar a las demás personas de la sociedad, acudiendo a conductas novedosas que no se encuentran tipificadas, o que si lo están, no hay una efectiva aplicación para la determinación de la adecuación típica, requiriendo entonces una especificación lo suficientemente clara para poder juzgar a aquellas personas que incurran en las conductas que impliquen medios informáticos. A este punto se suma, la especial indefensión de la mayoría de los usuarios de medios electrónicos, que pone de manifiesto la necesidad de una especial protección al uso y manejo de la tecnología para reducir tal inseguridad.

Se presenta entonces que estos nuevos tipos penales se apartan de los clásicos delitos como el hurto y la estafa, en el ámbito colombiano claro está. Y es este punto el que nos hace más eco en por qué se deben considerar estas nuevas conductas delictivas, y no simples agravantes, aspecto que va de la mano con el sentido de los legisladores al presentar y aprobar el proyecto de ley, pues es claro que el primer argumento para la justificación de la tipificación de los delitos, es la especificidad para una correcta adecuación típica del comportamiento de sujetos que hacen uso de la tecnología informática en detrimento de la población. Es decir que, la ley 1273 de 2009, al introducir estos nuevos tipos penales, esclarecen el contenido del ámbito de lo prohibido, ya que

establecen de forma clara la conducta típica de manera que no es necesario para el juzgador o acusador, forzar interpretaciones abarcativas o analógicas que alcancen determinadas conductas antes inexistentes (Montañez, A. 2017. p82).

Otro punto a favor del establecimiento de estos nuevos tipos penales, es la concordancia con el desarrollo de los demás ordenamiento jurídico de Estados cercanos en la materia de los delitos informáticos, pues el adaptar normas al igual que países, nos permitirá realizar una mejor persecución y juzgamiento de delitos transnacionales. Este punto, según Cano Cuervo (2014), es muy importante ya que, gracias a la tecnología, es fácil para el autor, realizar la conducta prohibida en cualquier parte del mundo, pero si contamos con sistemas jurídicos avanzados y homogéneos en la persecución de estas conductas, en principio, conllevaría a una mayor celeridad en el procedimiento y sanción a los mismos.

También, y de acuerdo al concepto de no quedar el orden normativo colombiano rezagado, e insuficiente, Serrano Buitrago (2014), afirma que el derecho debe ser dinámico y acompañar los cambios trascendentales en sus sociedades; para ser efectivo a la hora de la resolución de los problemas que se le presentan y evitar otros problemas mayores, el derecho requiere adaptarse a los avances tecnológicos de su época. En el área financiera, por ejemplo, la protección estatal es sumamente necesaria debido a la grave afectación que tiene el sistema financiero sobre la economía de los países contemporáneos. Ojeda, Rincón, Arias y Daza (2010).

En igual sentido, la Superintendencia Financiera en su Informe de Actualidad del Sistema Financiero Colombiano de julio de 2018, señaló que Colombia realizó un trabajo de fortalecimiento en la administración de la ciberseguridad, agrupando a sectores industriales, académicos, militares y financieros con el fin de realizar estrategias de combate a las amenazas tecnológicas que afectan al país. “Colombia trabajó en los últimos años estableciendo lineamientos y fortaleciendo la gestión de la ciberseguridad, convocando mesas de trabajo que reúnen a expertos de diferentes campos (industria, academia, militar, financiera, entre otros) con el propósito de crear estrategias para contrarrestar las amenazas informáticas que lleguen a representar un riesgo para las infraestructuras críticas del país y protegiendo con ello, la seguridad económica financiera. El sector financiero ha dado pasos importantes para gestionar la ciberseguridad, pero tiene el reto de continuar con sus esfuerzos para mitigar un riesgo tan cambiante y dinámico y la Superintendencia Financiera deberá velar porque el sector implemente las mejores prácticas y estándares en la

materia, consolidando al país como un referente en la región, como parte de su visión 2025. Sobre esto, podemos decir que es gracias a la tipificación de los delitos informáticos que se pueda avanzar el tema de la ciberseguridad, hecho que sería imposible de conseguir si se consideraran los tipos penales de estudio, y en general todos los delitos informáticos, como meros agravantes de conductas delictivas clásicas.

Estas razones, nos parecen suficientes para establecer necesidad desde el punto de vista social de la existencia de estos tipos penales, más existen razones jurídicas importantes que debemos exponer para demostrar la insuficiencia de los tipos penales "clásicos" en estos casos. Para ello expondremos a modo de ejemplo, la diferencia entre estafa y hurto por medios informáticos introducido por la ley 1273 de 2009:

Es necesario poder establecer las diferencias más esenciales y sustancias entre los tipos penales de estafa y hurto por medios informáticos. Esto con el propósito de que se tenga certeza al momento de analizar los delitos informáticos, puesto que la forma en la que se realiza esta conducta delictiva se asemeja a lo que puede ocurrir en una estafa.

Mayer (2014), al respecto dice que la estafa se identifica por las propias limitaciones de este delito, mientras que, en campo del hurto, este se encuentra expresado de forma muy amplia, y que solo contempla situaciones determinadas, cuando este no es agravado o calificado y no simple.

Giménez García indica sobre la estafa *"La nota característica de la estafa se encuentra en el apoderamiento de bienes ajenos, mediante la astucia –versión mayúscula de la picaresca- porque es la propia víctima la que realiza el acto dispositivo de sus bienes, en su propio perjuicio en virtud del engaño del que ha sido objeto por el actor."* (Jiménez, T. 2016, p2)

Por el contrario, el hurto por medios informáticos posee de dos partes, señaladas por la disyuntiva "o", en donde se señala en la primera que se traspasan las medidas se seguridad de un sistema informático, para sacar provecho de un bien mueble ajeno, pero que en este tipo penal se amplia, pues no solo se trata de un bien mueble y su afectación al patrimonio económico, sino la afectación también del bien jurídico de la información y datos. La segunda parte es la que tiene que ver con la suplantación de un usuario luego de haber traspasado la seguridad informática. Es esta parte la que hace que el articulo 269I, sea confundido y no aplicado en su totalidad típica, debido a que se encuentran similitudes con la estafa, pues la utilización de los medios informáticos genera esa

disparidad. Pero como señalamos anteriormente, la característica de la estafa es la inducción de la víctima mediante la astucia a lo que se denomina un teatro engañoso, haciendo que esta incurra en un error y que por sus propios medios, termine entregando sus bienes al victimario.

Por otra parte, con respecto a la suplantación de páginas web para captar datos, si bien, puede creerse que la creación y el manejo de los medios informáticos para inducir a las víctimas en una equivocación, se asemeja a las maniobras engañosas, artificios, que generan un teatro engañoso, de la estafa, el hecho de que se realice por medio de la tecnología, hace que no pueda ser considerado como un agravante, puesto que los conceptos de engaño que se tienen en la estafa son comunes, situaciones previstas desde hace siglos, al igual que sus agravantes, que, en contraposición con los delitos informáticos, la novedad de los medios utilizados, es la razón de recurrir a este tipo penal y no a la estafa.

Vemos también, que la estafa se predica de un acercamiento, por lo general, del sujeto activo con la víctima, para que esta caiga en el error que el victimario desea y que como consecuencia, termine sacando provecho de los bienes de esta. Por el contrario, los delitos informáticos son mucho más impersonales, pues el contacto con la víctima no es tan directo y muchas ocasiones, por no decir que en todas, los sujetos activos se encuentran a miles de kilómetros de distancia, generando consigo una que no se conozco quien perpetuo el delito, diferencia que se tiene con la estafa, pues en ella, si se sabe quién fue la persona que realizó la conducta punible. Esta es otra razón para justificar la creación de un nuevo tipo penal, pues la especificación de los medios que se utilizan para la comisión del delito, permiten que al momento de la investigación judicial siguiente, aquellos actos investigativos que se utilicen, sean más pertinentes y vayan directo al encuentro de los victimarios, puesto que prácticamente se generan cuerpos investigativos que se dedican exclusivamente al uso de la tecnología para contrarrestar estos tipos penales, los cuales, no podrían ser analizados e investigados sin que se haya considerado necesaria su creación.

Esta característica fundamental permite establecer, que en el hurto por medios informáticos, no se está induciendo a una persona en un error, sino que el sujeto activo, realiza por su propia cuenta todas las acciones de violación de sistemas de seguridad o de suplantación de un usuario ante estos sistemas, con el propósito de hacerse con el bien jurídico de la información y datos, para su provecho o el de un tercero.

Para finalizar esta distinción, se reiteran las características del hurto por medios informáticos, en donde Sánchez, dice que "considera hurto a toda aquella acción ilícita en donde se busque apoderarse de un bien mueble o en este caso llevado a la informática, un archivo físico o digital conservado en una entidad." (Sánchez, Z. 2017, p32).

La legislación y la jurisprudencia reciente

Articulo 269G y Articulo 269I del Código Penal Colombiano

Empezamos entonces señalando los artículos a desarrollar y su contemplación en el Código Penal. El tipo penal de Suplantación de sitios web para capturar datos personales está regulado en el artículo 269G del código, el cual dispone que los verbos rectores son diseñar, desarrollar, traficar, vender, ejecutar, programar o enviar páginas web, links o pop ups. El objeto del delito por parte del sujeto activo es la recolección de información personal para lograr un fin ilícito en detrimento de la víctima, presentándose una clara violación de la intimidad.

La segunda parte del artículo indica que la persona que realice una maniobra cibernética que se manifiesta en el redireccionamiento de un usuario a una página que considere oficial como la de su banco o redes sociales, también hará parte del tipo penal de suplantación de páginas web.

Ambos incisos tienen como pena, en primer lugar de prisión, de 48 a 96 meses, y en segundo lugar, una multa de 100 a 1000 smlmv. A su vez, cuando sean utilizadas las víctimas en la cadena del delito, la pena anteriormente mencionada se agravara en una tercera parte o hasta la mitad.

Podemos ver que en dicho artículo se hace mención a las diferentes posibilidades que existen para capturar datos personales, convirtiendo este tipo penal en uno que posee más de un verbo rector de la conducta, lo cual permite que aquellos sujetos que incurran en esta conducta delictiva, no se puedan escudar en simples banalidades de redacción del artículo, pues se previó anteriormente para que agrupara en casi su totalidad, los actos o medios que se utilizan para delinquir en esta modalidad, situación que va acorde con la necesidad de especificar las novedosas manifestaciones delictivas.

A su vez, encontramos en el artículo 269H, el hurto por medios informáticos, que además del verbo rector del artículo 239, es decir el hurto simple, y de su objetivo ilícito, que es el provecho para sí o para otro, señala que esta conducta se presenta cuando se superan medidas de seguridad de

carácter informático, la cuales ocurren cuando se manipula un sistema informático, una red electrónica, telemático o algún otro medio similar. Pero el artículo continua diciendo que además de las anteriores formas de superar sistemas informáticos de seguridad, el suplantar a un usuario ante los sistemas de autorización y autenticación de dichos sistemas, también incurrirá en el tipo penal.

Como penas, se prevén las que dice el artículo 240 del Código Penal, la referente al hurto calificado, la cual es de 3 a 8 años de prisión.

El segundo inciso al presentar la posibilidad de que se suplanten a usuarios en páginas web, es una novedad en el aspecto del tipo penal clásico del hurto, puesto que nos deja ver cómo los medios informáticos y su protección generan una nueva forma de legislación, y que también van en concordancia con el espíritu del legislador al especificar las conductas delictivas. Además, vemos como esa especificidad y la ampliación del bien jurídico tutelado de la información, imposibilitan que sea considerado como un agravante, pues es necesario que sea tenido en cuenta como un tipo penal independiente.

Es preciso decir, que el hurto por medios informáticos guarda una estrecha relevancia con la suplantación de páginas web, más que todo en la descripción de los medios tecnológicos a utilizar, además de ampliar los bienes jurídicos que pueden ser violentados por el uso inadecuado de la tecnología.

Por otra parte, es necesario indicar que este tipo penal, al igual que los demás delitos informáticos, al ser nuevos por el tema de la tecnología, han afectado de manera significativa el ámbito internacional, pues es evidente que la tecnología no tiene fronteras, y que es posible que desde un país al otro extremo del mundo se esté cometiendo estas conductas delictivas.

Doctrinariamente, las autoras Carvajal y Rangel (2015) con respecto al artículo 269G señalan que este tipo penal se presenta en la práctica cuando un suplantador también llamado phisher, realiza una página con un dominio similar del establecimiento al que desea ingresar, ubicándolo luego en un servidor o hosting, en donde enviara emails basura o spam, con anuncios atractivos. Las personas en su ingenuidad de no saber distinguir una página original de una falsa, ingresan su información personal, entre ellas claves que pueden ser bancarias, las cuales serán guardadas en

una base de datos que posteriormente será utilizada para transferir los bienes patrimoniales, sobre todo dinero, a cuentas de los sujetos que sirven a los ciberdelincuentes.

Con respecto al artículo 269I, Carvajal Avellaneda y Rangel Ruiz (2015) señalan a su vez, que fortalece el Artículo 269G.

Agravante punitivo de las conductas

Estos tipos penales establecen la siguiente agravante:

Articulo 269H. Circunstancias de agravación punitiva. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

En resumen, las circunstancias de agravación se basan en si la información es financiera, la conducta fue cometida por un servidor público, debido a la confianza, la información es utilizada en perjuicio de otro, se saca provecho de ella, es usada para fines terroristas, se abusa de la buena fe, o se es el administrador de un medio electrónico.

Dichos agravantes van en concordancia con otros presentados a lo largo del Código, por lo cual ahondar en ellos no resulta relevante pues desvía de manera innecesaria el objetivo específico del delito en cuestión. Sin embargo, podemos establecer que a estos delitos informáticos se les trata de igual manera que otros tipos penales, estableciendo agravantes a la conducta delictiva, los cual es un avance en el desarrollo especial y legislativo del derecho colombiano.

Desarrollo Jurisprudencial

Proseguimos ahora con el desarrollo jurisprudencial de las diferentes cortes, las cuales permiten observar ya desde un determinado caso en concreto, el avance que se debe tener con respecto a la protección de los bienes informáticos como lo es la información personal. Las cortes que desarrollan un aparte de este tema son la Corte Constitucional y la Corte Suprema de Justicia, quienes por los temas y la jurisdicción a la que pertenecen, pueden con más propiedad hablar y desarrollar conceptos jurídicos al respecto. Siendo esto así, encontramos y podemos identificar de manera relevante las siguientes, iniciando por lo que dispone la Corte Constitucional. En la sentencia C – 1147 de 2001, la Corte hace referencia a la intimidad y el habeas data en páginas web. Dicha sentencia se refiere a la intromisión del Estado y la Administración en la órbita de la

vida privada de las personas, diciendo que se presenta un vicio en este derecho por tal intromisión del Estado, y que es necesario ponderar la necesidad del involucramiento de la Administración en la información que solo le debe interesar a la persona, con respecto a la necesidad que este presenta para su financiamiento para sus gastos.

Por otro lado, en sentencia C – 540 de 2012, la Corte hace un análisis de los procedimientos y actos de investigación que realizan las autoridades, entre ellas y principalmente la policía judicial, en aspectos de inteligencia y contrainteligencia. Indica que realizó el control de los proyectos de ley estatutaria no. 263/11 senado y 195/11 cámara, para llegar a la conclusión de que en ellos no se vulneran los derechos fundamentales de los sujetos investigados, y, por tanto, permite el ejercicio investigativo de inteligencia y contrainteligencia, el cual es por otro lado, una misión constitucional y legal.

Luego expuesta la postura de la Corte Constitucional con respecto a temas de informática y tecnología, es evidente que un desarrollo profundo de los delitos informáticos no se ha realizado, esto tal vez debido al interés por temas más controversiales y que afectan derechos fundamentales. Aunque, se hace presente la reiteración de la intimidad como un derecho fundamental.

Continuamos entonces con la disposición de la Corte Suprema de Justicia, presentado por la Sala de Casación Penal, en la sentencia 34564 del 2010, en donde se indica la nueva relación que hay en los conceptos de espacio/tiempo. Lo expuesto por la Corte Suprema de Justicia va en desarrollo con la norma que introdujo a los delitos informáticos en el Código Penal, resaltando que el avance tecnológico e informático es el punto de partida para desarrollar las nuevas normas que deberán ser tenidas en cuenta para la protección de derechos fundamentales como el de la intimidad y la información, así como el de la propiedad ya no física, sino por así decirlo, jurídica o informática.

Es entonces evidente, que las altas Cortes Colombianas no han desarrollado estos tipos penales pues no han logrado interpretar de la mejor manera lo que son los delitos informáticos, ni la necesidad de haber sido creados, cayendo estos en las confusiones anteriormente presentadas, lo cual genera que esa función de generadora de precedentes jurisprudenciales de aplicación como fuente de estudio de la ley, no se cumpla en su cabalidad, haciendo que los estudiosos del derecho se vean obligados a recurrir fuentes extranjeras.

Contexto Internacional

Se hace presente la necesidad de los organismos internacionales de desarrollar normas para combatir estas formas delictivas. Encontramos pues, que es la Organización de los Estados Americanos (OEA), el ente internacional que más reuniones internacionales ha organizado sobre el punto de los delitos informáticos, que como podremos observar, se actualizan periódicamente debido al constante avance de la tecnología. De esa manera, podemos citar como las más importantes la VIII Reunión (Sede de la OEA, 27 y 28 de febrero de 2014), VII Reunión (Sede de la OEA, 6 y 7 de febrero de 2012), VI Reunión (Sede de la OEA, 21 y 22 de enero de 2010), V Reunión (Sede de la OEA, 19 y 20 de noviembre de 2007), IV Reunión (Sede de la OEA, 27 y 28 de febrero de 2006), III Reunión (Sede de la OEA, 23 y 24 de junio de 2003), II Reunión (Sede de la OEA, 14 y 15 de octubre de 1999), I Reunión (Sede de la OEA, 12 de mayo de 1999), Observación General del Consejo de Derechos Humanos A/4rc/11/12, de 31 de marzo de 2009.

La discusión acerca de la Autopuesta en peligro en los delitos informáticos

Una problemática que se presenta en los delitos informáticos es la que tiene que ver con una autopuesta en peligro de la víctima. Esto se afirma por el hecho de que estos tipos penales informáticos se realizan mediante herramientas tecnológicas, las cuales están al alcance de la mayor parte de la población, quienes por hacer uso de las nuevas tecnologías traídas por la globalización y facilitar la realización de sus tareas mediante medios electrónicos e interconectividad, entregan sus datos e información personal al mundo cibernético y la internet, sin contar con ningún tipo de asesoramiento. Se señala por ello, que puede existir una autopuesta en peligro de las víctimas, que, sin saberlo, provocan, generan y facilitan estos tipos penales.

Para iniciar el análisis debemos diremos que la autopuesta en peligro, como indica Alas Rojas (2015), es cuando la víctima es la que asume el riesgo de que sus bienes jurídicos se vean afectados por la conducta del sujeto activo, cuando esta conducta se realiza efectivamente, haciendo que sea condenada la víctima y no el autor, lo que genera una discriminación de la normal tipicidad.

La autora española Andrea Perin (2016) señala que la autopuesta en peligro es la concurrencia de culpas; es una categoría que aparece dentro de la imputación objetiva y que es correcta de aplicar por las conductas de propia indefensión a la que han incurrido las víctimas.

Recurriendo a la doctrina clásica, Fabio Rey trae a colación a Roxín, quien, indicó que la autopuesta en peligro, ocurre cuando la víctima es quien decide estar en la posición de estar al frente de un suceso delictivo y del cual es que surge el riesgo de resultar afectado. La distingue de otro tema, no de relevancia pero que es necesario mencionar, que es la heteropuesta en peligro, la cual, siguiendo con Fabio Rey y su remisión a Roxin, ocurre cuando la víctima está de acuerdo con ser sometido a un riesgo debido al actuar de un tercero que no es el autor. (Rey, F. 2011. p134).

Ya desde la jurisprudencia, la Corte Suprema de Justicia, Sala de Casación Penal, Magistrada Ponente María Del Rosario González Muñoz, en sentencia del 27 de noviembre de 2013, ha establecido, sobre la autopuesta en peligro, que ésta se concreta cuando se presentan dos situaciones. La primera es que la víctima se pone a sí mismo en un riesgo. Y la segunda, cuando, al tener pleno discernimiento de la situación, se deja llevar a esa circunstancia por otro sujeto, situación en la que no se puede imputar al tercero el tipo objetivo puesto que quien estaba con pleno discernimiento, se expone a un hecho del que se hará responsable por su actuación de las consecuencias que puedan tener.

Como caso práctico y fehaciente de la autopuesta en peligro de los delitos, informáticos, (hurto informático, suplantación por medio de páginas web, etc.), Martin Javato nos presenta la situación en la que concurren los medios electrónicos de pago, como lo son las tarjetas de crédito. Dice entonces el caso *"el autor emplea los datos de otra persona mediante la utilización no autorizada de la tarjeta bancaria para hacerse a través del cajero automático con cantidades de dinero; y ello se cohonesta perfectamente con el concepto amplio de manipulación informática."* (Javato, 2008, p7). En este caso evidenciamos como se incurre en una autopuesta en peligro por parte de la víctima, puesto que las personas confían en muchas ocasiones, ciegamente en la utilización de métodos electrónicos de pago, sin saber, que pueden estar siendo rastreados, monitoreados o suplantados en sus bienes, con el objetivo de ser sometidos a las conductas punibles en detrimento de sus bienes jurídicamente tutelados como los es el patrimonio económico, y en específico de los delitos informáticos, la información y datos.

De acuerdo a estas definiciones y el caso presentado, es posible afirmar que en efecto, en los delitos informáticos en estudio y en general, las personas se ponen en esta situación de peligro. Es decir, la autopuesta en peligro influye en el momento en que la víctima se pone a sí misma en una

situación peligrosa o de riesgo, la cual no es tan evidente como en los delitos clásicos, puesto que no se distingue de forma tan sencilla como cuando una persona se pone en frente de otra que tenga un arma, o que deja la puerta de su casa abierta descubriendo todos sus bienes, sin embargo, como se ha presentado antes, el uso de la tecnología se ha ampliado de tal manera, que todas las personas tienen acceso a ella, utilizada de forma descontrolada en la mayoría de los casos, donde no se presenta una pedagogía para el correcto uso de las herramientas electrónicas, déficit que pone de manifiesto la facilidad que tienen los delincuentes informáticos para realizar sus conductas, pues esta falta de educación tecnológica, les pone en bandeja de plata la posibilidad de aprovecharse de la ingenuidad de las víctimas.

Pero debemos tener en cuenta también el aspecto objetivo de los delitos informáticos, pues en este aspecto podemos saber cuándo es posible evidenciar la autopuesta en peligro. Si tomamos como sujeto pasivo a una empresa multinacional, especializada en el desarrollo de software o en un banco que maneja cuentas internacionales de grandes conglomerados económicos, y lo comparamos con una mujer de 75 años, quien tiene en su computador del siglo XX archivos que contienen datos personales como contraseñas, podremos establecer quien será penalmente responsable de la comisión del delito. Es decir, las empresas y bancos, al manejar tantos datos importantes mediante el uso de las herramientas tecnológicas, se ven expuestas al posible ataque de cibercriminales, quienes realizaran alguna conducta señalada como delito informático. Estos sujetos (empresa o banco), en consecuencia, conocen los riesgos a los que se ven expuestos, razón por la cual es necesario que tomen las medidas necesarias para que no sufran este tipo de conductas punibles, como por ejemplo crear un sistema de seguridad informático tan fuerte que nadie pueda traspasarlo, ni siquiera el más hábil hacker. Sin embargo, en caso de no tomar estas medidas, se estará exponiendo a un riesgo, circunstancia que plasmaría de forma evidente la autopuesta en peligro, pasando a ser responsables del daño que pueda ocurrir por el actuar de algún sujeto activo.

Por otro lado, en el caso de la señora de la tercera edad, quien tiene información valiosa en su computadora, no es una persona que sepa los riesgos a los que se puede someter, razón por la cual muy seguramente no tenga protección en su dispositivo electrónico, como un antivirus, pero que igualmente estaría poniéndose en una situación de riesgo. Pero es en este tipo de situaciones, cuando la figura de la autopuesta en peligro no podría aplicarse y decretar que la señora es penalmente responsable, pues no tiene el suficiente conocimiento para identificar los peligros a los

que se expuso, y por lo tanto se debe excluir la figura y seguir a aquella persona que pudiese atentar contra los bienes jurídicos tutelados de la mujer de tercera edad.

Por tal motivo, debe tratarse a la autopuesta en peligro en los delitos informáticos no de la misma forma que en las demás conductas punibles, es decir, que se condene a la víctima y no al autor, esto en razón de la novedad de las conductas, las cuales necesitan ser compartidas y explicadas al pueblo o sociedad en general, lo que permitirá que en un futuro se evidencie de mejor manera cuando es que las víctimas se ponen a sí mismas en una situación de riesgo al igual que en los delitos clásicos. Terminamos diciendo que, con respecto a la necesidad de los delitos informáticos, como se afirmó antes, el hecho de que se hayan tipificado estas conductas y se realicen mayores especificaciones sobre cuándo se pueden presentar las acciones delictivas, permite que la gente del común, no se vea tan expuesta a estos ya que se tendrá un mínimo conocimiento o al menos un poco de ayuda al sentido común, para evitar ser víctimas.

Conclusiones

La globalización es un fenómeno el cual no podemos considerar como nuevo sino como actual y presente, el cual causó un cambio en el paradigma de la información y la propiedad, llevando a replantear dichas instituciones. Por tal motivo se comienza a tratar a la información personal como un derecho fundamental mediante la protección la intimidad, el cual está consagrado por la Constitución y demás normas internacionales que hacen crecer el bloque de constitucionalidad. Se evidencia entonces, que el uso de herramientas informáticas para la captación de datos personales y el hurto por medios informáticos, es una violación a un derecho fundamental, asemejando y acercando este tipo de delitos informáticos a tipos penales clásicos como el homicidio, el secuestro o el mismo hurto simple.

A su vez, el desarrollo tecnológico ha permitido un avance en todos los aspectos de la sociedad, permitiendo una mayor interconexión entre los ciudadanos y habitantes del mundo, pero que, sin embargo, se ha prestado para la consecución y creación de nuevas formas de afectar el bien de las personas, razón por la cual el derecho y sus diferentes áreas se han adaptado a estos desarrollos tecnológicos, intentando contrarrestar cualquier afectación a los bienes virtuales de las personas como lo es la información, logrando así no quedar obsoleto o inoperante. Es por este motivo que se hizo necesario la creación de una nueva normatividad que incluyera aquellas nuevas

tecnologías, las cuales fueron utilizadas para cometer crímenes, y que por la legislación clásica no podía resolver, pues faltaba especificación y tecnicidad en estos. Además, se indica que no es procedente que sean considerados estos tipos penales como agravantes de delitos más grandes y clásicos. Por tal motivo, el hurto informático debe estar aparte del hurto clásico, pues es la tecnicidad y el bien jurídico tutelado de la información y los datos, el que genera el requerimiento de regular por su parte los agravios que puedan sufrir. Por el mismo ámbito anda la suplantación por páginas web, pues no es lo mismo suplantar la identidad de una persona en el mundo físico, pues por el medio electrónico es más sencillo, y es entonces necesario que se distingan ambos casos, cada uno por separado, pues en caso de que sea un agravante, se optara por la concepción clásica de la conducta delictiva, y eso generara el no desarrollar como es debido la ley, lo cual se encuentra presente en la falta o escaza jurisprudencia que hay respecto al tema.

Bibliografía

Alas, D. (2015). *Comportamiento de la víctima del delito: la autopuesta en peligro.* Derecho y Cambio Social.

Arbuet, C. (2014). *Capitalismo y globalización: El capital en la era del capital tecnológico*. Desafíos, 26 (2), 97-124.

Aroncena, G. (2011). *La regulación de los delitos informáticos en el Código Penal Argentino.* Introducción a la ley nacional núm. 26.388. Argentina. Universidad de Córdoba.

Arzuaga, T. (2013). *La ley 1273 de 2009 y los delitos informáticos en Santiago de Cali.* Cali. Universidad San Buenaventura.

Cano, A. Díaz, J. Et al (2014). *Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes*. Bogotá. Universidad Libre.

Carreño, D. (2016). *Pensar en el derecho como derecho virtual.* Bogotá. Universidad Católica de Colombia.

Carvajal, M. & Rangel, N. (2015). *Análisis comparativo del tratamiento jurídico dado a los delitos informáticos en el derecho penal colombiano español.* Cúcuta. Universidad Libre de Colombia.

Castro, S. (2008). *Algunos aspectos dogmáticos de la delincuencia informática.* Bogotá. XXIX Jornadas internacionales de Derecho Penal. Universidad Externado de Colombia. Departamento de Derecho Penal y criminología.

Cuenca, H. (2014). *Cómo responder a un delito informático*. Revista Ciencia UNEMI.

Gimbernat, E. (2005). *Imputación objetiva y conducta de la víctima*. México.

Giménez, J. (2016). *El delito de estafa*. Magistrado Sala II - Tribunal Supremo. España.

Gómez, M. (2016). *Globalización y desarrollo económico, Colombia como caso de estudio. Medellín*. Universidad EAFIT.

Hernández, L. (2009). *El delito informático.* Eguzkilore. Número 23. San Sebastián.

Javato, A. (2008). *Estafa convencional, estafa informática, y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago.* Revista Electrónica de Ciencia Penal y Criminología (en línea). 2008, núm. 10-r5, p. r5:1 r5:9. Disponible en Internet: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf ISSN 1695-0194 [RECPC 10-r5 (2008), 12 dic].

Leyton, J. (2014). *Los elementos típicos del delito de estafa en la doctrina y jurisprudencia contemporáneas.* Santiago, Chile. ARS BONI ET AEQUI (Año 10, N° 2) PP. 123 – 161.

Mayer, L. (2016). *Las paradojas de la estafa. Polít. crim*. Vol. 11, Nº 21 (Julio 2016), Art. 7, pp. 173-201. [http://www.politicacriminal.cl/Vol_11/n_21/Vol11N21A7.pdf]

Miró, F. (2012). *El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio*. Buenos Aires.

Montañez, A. (2017). *Análisis de los delitos informáticos en el actual sistema penal colombiano.* 2017. Bogotá. Universidad Libre de Colombia.

Moya, M. (2011). *¿Se investiga el derecho penal en Colombia?* Revista Iusta Núm. 35, Julio 2011. Bogotá. Universidad Santo Tomas.

Ojeda, J. Arias, M. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Bogotá. USTA.

Ore, E. (1999). *Autopuesta en peligro y exclusión de comportamientos*. Perú.

Perin, A. (2016). *La contribución de la víctima y la imputación objetiva del resultado en la teoría del delito imprudente.* Revista Electrónica de Ciencia Penal y Criminología.

Polo, M. (2009). *Los delitos informáticos: conflicto entre el Derecho al honor y la intimidad y el Derecho a la información.* Cuenca, Ecuador. Universidad del Azuay.

Posada, R. (2013). *El delito de acceso abusivo a sistema informático: a propósito del artículo 269A del Código Penal de 2000.* Bogotá. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. Universidad de los Andes.

Posada, R. (2017). *El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual.* Universidad EAFIT.

Rey, F. (2011). *La corresponsabilidad de la víctima en la comisión de la conducta punible desde la victimologia a la victimodogmatica*. Tunja. Principia Iuris. USTA.

Reyes, J. (2007). *El delito informático en Colombia: insuficiencias regulativas.* Universidad Externado de Colombia.

Rodríguez, J. (2014). *Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación.*

Salazar, J. (2009). *Situación normativa de la Sociedad de la Información en Colombia*. Universidad Santiago de Cali.

Sánchez, Z. (2017). *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia.* Chiquinquirá. Universidad Nacional Abierta y a Distancia UNAD.

Sánchez, S. (2014). *Actuación de la víctima e imputación objetiva: Comentario a la sentencia de la Corte Suprema de Justicia 36.842 del (27) de noviembre de 2013*, M.P. María del Rosario González Muñoz. Medellín. Universidad EAFIT.

Serrano, E. (2014). *La práctica de delitos informáticos en Colombia*. Bogotá. Universidad Militar Nueva Granada.

Torregrosa, N. (2010). *Pluralismo jurídico: la conciliación en equidad. Otra justicia, real, posible.* Colombia. Universidad Libre Facultad de Derecho.

Valencia, A. Ortiz, Á. (2016). *Derecho Civil.* Editorial Temis.

Velásquez, O. Garrido, Y. (2016). *El ciberilícito en Colombia: ¿ante cuál juez acudir?*, 132 Vniversitas, 515-560. http://dx.doi.org/10.11144/Javeriana.vj132.ccac

Legislación.

Congreso de la República. Julio 24. Ley 599 de 2000. Por la cual se expide el Código

Penal.

Superintendencia Financiera. *Seguridad bancaria, protección en oficinas***.** Concepto 2010007753-001 del 22 de febrero de 2010.

Jurisprudencia.

Corte Constitucional. 31 de octubre de 2001. Sentencia C – 1147. MP Manuel José Cepeda Espinosa.

Corte Constitucional. 12 de julio de 2012. Sentencia C – 540. MP Jorge Iván Palacio.

Corte Suprema de Justicia, Sala de Casación Penal. 25 de agosto de 2010. Sentencia 34564. MP José Leónidas Bustos Martínez.

Corte Suprema de Justicia, Sala de Casación Penal. 27 de noviembre de 2013. Sentencia 36482. MP María del Rosario González Muñoz.