DELITOS INFORMATICOS - CIBERCRIMEN

Autor:

Derian Vásquez Maldonado [1]

RESUMEN

El presente artículo se encargará de analizar con mayor detalle los nuevos desafíos teóricos y prácticos que nos plantea la actualidad a partir de la Revolución Industrial 4.0 y los cambios que esta nueva era digital representa, exigiéndonos un cambio de paradigma en la concepción de la configuración de nuevos delitos que se producen en relación con diferentes bienes jurídicos y principios como lo son la integridad moral, intimidad personal, libertad, confidencialidad, territorialidad, habeas data, suplantación, entre muchos otros y que deben ser protegidos tal como lo indica nuestra constitución al referirse al carácter social del Estado social de Derecho en Colombia y siendo este el pilar de los Derechos Fundamentales; precisamente son estos bienes jurídicos los llamados a proteger y respetar asegurando así los derechos ciudadanos, es entonces que el Estado debe realizar el mayor esfuerzo para garantizar los mismos frente a los cambios que

[1] Estudiante Especialización en Sistema Procesal Penal, Pensum de Derecho finalizado en Universidad de Manizales, correo electrónico: derianvas@gmail.com

representa esta Revolución Industrial 4.0 de nuevas tecnologías. Por lo tanto, obliga a entender y avanzar en materia del tratamiento a los delitos informáticos y su regulación bajo la creación de herramientas jurídicas que haga más fácil la clasificación de nuevas conductas delictivas y claro está que es en este punto donde el Derecho Penal se debe ocupar de esas conductas que se observan lesivas.

Todo lo anterior aunado al crecimiento constante de estos delitos tanto nacional como internacionalmente fue creada en Colombia el 5 de enero de 2009 por el congreso de la república, la Ley 1273 de 2009 denominada "De la protección de la información y de los datos", la cual modifica el código penal creando un nuevo mecanismo legal, teniendo como objetivo sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país, de esta ley también se comentara en este artículo ya que a pesar de estar catalogada como una de las más completas leyes en cuanto a delitos informáticos se refiere en el continente no se está tratando de una manera correcta ni eficiente y se está llegando con imprecisiones a la sala de audiencias donde se confunden términos y conceptos, llevando en algunos casos a la vulneración de normas ya establecidas en el ordenamiento jurídico y que se deben de asegurar, más aun cuando el delito informático se debe razonar de una manera global ya que no hay límites, ni fronteras que se interpongan y solo basta un aparato electrónico para entrar en un mundo virtual totalmente diferente en el cual se pueden generar delitos informáticos que por ultimo generen violaciones y daños en la sociedad.

Palabras clave:

Delitos informáticos, tecnología, Derecho Penal, código penal colombiano. Revolución Industrial 4.0, Cibercrimen.

ABSTRAC

This article will analyze in greater detail the new theoretical and practical challenges posed by the present from the Industrial Revolution 4.0 and the changes that this new digital era represents, demanding a paradigm shift in the conception of the configuration of new crimes that occur in relation to different legal assets and principles such as moral integrity, personal privacy, freedom, confidentiality, territoriality, habeas data, impersonation among many others and that must be protected as indicated by our constitution when referring to the social character of the social State of Law in Colombia and this being the pillar of Fundamental Rights; It is precisely these legal assets that are called to protect and respect, thus ensuring citizens' rights, it is then that the State must make the greatest effort to guarantee them in the face of the changes that this Industrial Revolution 4.0 of new technologies represent. Therefore, it forces us to understand and advance in the matter of the treatment of computer crimes and their regulation under the creation of legal tools that make it easier to classify new criminal behaviors and of course, it is at this point where Criminal Law is due. deal with those behaviors that are observed harmful.

All of the above coupled with the constant growth of these crimes both internationally and nationally is that in Colombia was created on January 5, 2009 by the Congress of the Republic, the law 1273 of 2009 called "On the protection of information and data ", which modifies the penal code and creates a new legal mechanism, with the objective of sanctioning all illicit behavior against the commission of computer crimes in the country, this law will also be commented on in this article since despite being cataloged as one of the most complete laws regarding computer crimes in the continent, it is not being treated in a correct or efficient way

and it is reaching the courtroom with inaccuracies where terms and concepts are confused, leading in some cases to the violation of norms already established in the legal system and that must be ensured, even more so when the computer crime must be reasoned in a global way bal since there are no limits or borders that interpose and only an electronic device (computer, tablet, cell phone) is enough to enter a totally different virtual world in which computer crimes can be generated that ultimately generate violations and damage to the society.

Keywords:

Computer crimes, technology, Criminal Law, Colombian criminal code. Industrial Revolution 4.0, Cybercrime.

INTRODUCCIÓN

Los progresos disruptivos informáticos avanzan de manera casi que incontrolable y estan sobrepasando limites que dentro de un sistema jurídico no se habían contemplado hace un tiempo atrás, todas las facilidades de conectividad que se tienen desde diferentes dispositivos ubicados en cualquier lugar y desde una infinidad de plataformas, redes y apps y desde las cuales se acumulan, procesan y analizan información de todo tipo con un nivel de seguridad de la información muy bajo, todo esto es lo que está permitiendo dejar en riesgo y a la deriva múltiples datos personales, financieros, económicos, transaccionales, crediticios tanto de empresas, personas jurídicas como de personas naturales.

En Colombia ha sido muy paulatino el proceso de reglamentación jurídica del Derecho Penal en el contexto de las tecnologías de la información; en donde se destaca de manera especial el ejemplo de la aprobación e incorporación del Convenio sobre la ciberdelincuencia de Budapest del 23 de Noviembre de 2001 por medio del cual se propende por el diseño y aplicación de una política criminal común para combatir el preocupante aumento de los delitos cibernéticos derivados de la digitalización y la globalización de las redes de informáticas.

A partir de estos hechos notorios es fundamental la restructuración normativa en general respecto delitos informáticos y sobre todo en cuanto a Derecho Penal se refiere se hace evidente la necesidad de contextualizar estas conductas delictivas dentro de un marco normativo especial para delitos especiales ya que las actuales no son suficientes para proteger los derechos fundamentales de la sociedad y los bienes jurídicos tutelados, es innegable que la tecnología está

contribuyendo al desarrollo sostenible a todo nivel, pero este debe mantenerse vigilado y protegido, buscando que esta transición tecnológica que nos lleva a esferas de temas analógicos, digitales, artificiales, físicos y todos estos interrelacionados en cualquier momento mantengan un control adecuado y sobre todo oportuno por parte del Estado enfocado a la protección de los derechos fundamentales como debe ser en un Estado social de derecho como el nuestro.

En este aspecto el derecho penal juega un papel determinante en la protección de estos derechos, a partir de una correcta contextualización entre los delitos cibernéticos, ciberdelitos, cibercrimen y el sistema judicial, asegurando una tipificación precisa en estos casos que permita el principio de legalidad y por ende la judicialización oportuna; en la actualidad vivimos la ausencia de unos parámetros jurídicos que de manera adecuada se encuentren en contexto con la realidad tecnológica, que eviten la impunidad de estos delitos y la violación a los bienes jurídicos tutelados, actualmente la deslocalización de los cibercriminales, la imposibilidad de judicialización a falta de normas supranacionales, la dificultad probatoria e individualización que se tiene en muchos de estos casos debido al modus operandi deslocalizado o incognito del que trata este delito, hace repensar en cómo se estan tratando, visualizando y judicializando estas acciones delictivas y nos marcan el camino proactivo y urgente que se debe trazar en búsqueda de la actualización y modificaciones normativas en pro de la protección de los derechos fundamentales que la sociedad advierte desesperadamente estan siendo vulnerados e impunes.

Interrogante del Artículo

De acuerdo a lo anterior, se determina realizar el presente artículo bajo el enfoque de la pregunta que a continuación se describe:

¿Cuáles son los desafíos jurídicos frente al cibercrimen en Colombia?

Objetivo:

General:

Analizar si la tipificación actual de los delitos cibernéticos estan en concordancia con los avances tecnológicos en Colombia.

Específicos:

- Clasificar las diferentes modalidades más comunes del cibercrimen.
- Contextualizar la tipificación actual del cibercrimen.
- Identificar los elementos jurídicos de las acciones que en la actualidad se consideran como cibercrimen.

METODOLOGÍA

Este artículo se sirve a través del método cualitativo que permite, mediante la investigación, interpretación y deducción, entender aún mejor la sociedad moderna y su dependencia de la tecnología a través de sistemas cibernéticos, más aun cuando es indiscutible que con la posibilidad de acceso al internet con mayor frecuencia y facilidad se puede navegar en páginas y redes desde cualquier lugar y mediante una variedad de dispositivos (móviles, tabletas, pendrive, PC, portátiles, Smar TV, entre otros) aumentando el volumen de procesamiento de información de toda índole y dejando en riesgo cantidad incalculable de datos con información personal, comercial, financiera la cual está quedando a disposición de ser vulnerada en cualquier momento, es en este aspecto es que empieza a tener relevancia el tratamiento, regulación normativa y penalización del cibercrimen que mediante diferentes modalidades (Phishing, vishing, smishing) se ejecutan afectando patrimonio real de personas, compañías, organizaciones, pequeñas y medianas empresas y en cuanto a las personas naturales la posibilidad de vulnerarse la dignidad, la intimidad, el buen nombre, por lo que a hoy existen retos principales como lo es la identificación del tipo de proceso, entendimiento más holístico de la teoría del delito, la conceptualización de la conducta y las teorías del dominio del hecho entre otros puntos que toman fuerza toda vez que empiezan a variar de cara al cibercrimen y no se puede tratar igual que un delito de la acción común y es en este punto donde se debe buscar asegurar unas garantías legales de acuerdo a estas nuevas modalidades.

La constitución política de Colombia en su artículo 15 establece “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y

hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley".

Indiscutiblemente en Colombia se ha avanzado en el uso de las nuevas Tecnologías digitales de la Información y la Comunicación – NTIC-, el acceso es más fácil por los avances en la masificación del Internet y así mismo muchas actividades y procesos que antes requerían presencialidad, actualmente se realizan virtualmente y mediante formatos cargados en la web y es aún más evidente que estas prácticas llegaron para quedarse a partir de la pandemia (COVID-19) y que ha obligado a múltiples sectores a reinventarse en estos procedimientos, pero que en muchos casos no se está vigilando de la mejor manera el cuidado de la información y la seguridad desde las mismas compañías, ni organizaciones.

Acompañando a estos nuevos avances disruptivos tecnológicos, el Estado debe dar tranquilidad y brindar todas las garantías al momento de hacer uso de estas plataformas, asegurando la no afectación del derecho a la intimidad, amparado constitucionalmente con el fin de no vulnerar la integridad personal de quienes acceden por estos medios tecnológicos; esto endosado a una plena protección de datos de las partes y evitar la publicidad de información

personal, empresarial que, por su naturaleza, no pueden ser objeto de conocimiento público (verbi gratia, seguridad y protección de la información).

Otro reto es asegurar una clasificación idónea de los delitos informáticos y el equilibrio entre estos delitos y la sanción o pena impuesta, pero sobre todo el entendimiento correcto de todas las partes sobre este nuevo campo de delitos y entender que es necesario trabajar con técnicos e ingenieros debido a que muchas de las normas actuales son insuficientes e inadecuadas técnicamente y no responden a la criminalidad ordinaria, ni a las metodologías del cibercrimen que estan empleando los criminales o que no regulan los delitos más comunes, el cibercrimen es **deslocalizado** y se requiere que las legislaciones de cada país guarden una armonización y que regulen los delitos de manera homogénea para que las investigaciones y procesos no fracasen.

Las normas actuales son muy estables, mientras que el cibercrimen está constantemente en cambios y actualizándose a las nuevos modelos de criminen informático, por lo que podríamos decir que el Derecho Penal no está preparado aun en su totalidad para dar alcance a las nuevas modalidades criminales de manera eficaz y precisa, este fenómeno se denomina como “cadencia tecnológica” ya que el Derecho Penal está más anclado en el pasado, toda vez que los delitos comunes no han sufrido mayor transformación en el tiempo, no siendo así el caso en los cibercrimenes que estan cubiertos totalmente de nuevas modalidades que no se logran abarcar en su magnitud con la normativa actual.

La teoría del delito ha evolucionado ya que antes estaba diseñada para delitos con ejecución analógica en el mundo exterior con base en comportamientos y basada en la causalidad, hoy es virtual permitiendo programar acciones sin presencialidad y sin que el sujeto sea consiente y quiera realizar dicha conducta al momento de ejecutarse el delito, por ende la conceptualización

de la conducta, la causalidad, el dolo, las teorías del dominio del hecho empiezan a variar de cara a los cibercrimenes, primero la existencia de una ciberacción que tiene unas características en tiempo espacio distintas a la acción común, en segundo lugar esta el dominio lógico sobre estas acciones, dado que las acciones se generan bajo unas instrucciones programados afectando datos, información, transacciones entre otros, todo desde un lugar deslocalizado, por ende las circunstancias expresas en el tipo de tiempo, modo o lugar deben analizarse de una manera diferente con alcance a este nuevo modelo de crimen deslocalizado que por ende se debe hacer con acuerdos de cooperación entre los diferentes países para que permita actuar de manera ágil contra el cibercrimen, las investigaciones demuestran que actualmente existen más cibercrimen ocultos que delitos en la calle con una tasa de impunidad del 97%, lo que hace de imperiosa necesidad establecer mecanismos de cooperación internacionales adecuados, regulaciones que obliguen a guardar información durante un periodo de tiempo prudente que permitan generar una investigación total y con una decisión final en derecho, permitiendo que estos hechos puedan llegar a las cortes toda vez que en la actualidad no sucede debido a que fracasan las investigaciones por falta de evidencia digital y valoración de las pruebas.

En aras de poder demostrar que en el país sí puede ser posible que exista una seguridad jurídica en cuanto a los delitos tecnológicos, que en últimas es uno de los objetivos del derecho procesal en todas sus ramas y evitando así que existan dilaciones innecesarias, e incluso que se logre minimizar la prescripción o vencimiento de términos y por ende disminuir la impunidad en este tipo de delitos, en este sentido es necesaria la especialización de Jueces, fiscales, defensores, capacitación a los mismos, buscar que las partes entiendan estas acciones con la especialidad que estos delitos requieren y sobre todo asegurando mediante un sistema procesal optimo la cadena

de custodia adecuada de los elementos tecnológicos, peritajes de expertos y no procesos ordinarios de documentación simple.

De igual manera se hace necesario destacar que el Derecho Penal lo que hace es reforzar la ciberseguridad avanzando con leyes especiales para delitos especiales como los que tratamos, buscando siempre la protección de bienes jurídicos especiales con el objetivo de no aunar los delitos tradicionales con delitos especiales que deben ser vistos bajo otra óptica jurídico penal, siendo este un punto de alta importancia en el aparato judicial colombiano en búsqueda de estar en armonía con otros países debido a la deslocalización del cibercrimen.

Al finalizar este artículo se tendrá mayor claridad y mejor entendimiento sobre cuáles son los mayores retos que tiene el sistema colombiano en la judicialización del cibercrimen y sus modalidades más comunes, los avances sobre la tipificación actual y la necesidad de nuevos tipos penales específicos para estos delitos, entendimiento de un mejor enfoque en la teoría del delito informático a la luz de la normativa nacional e internacional, además nos marcará las pautas que nos exige la revolución industrial 4.0 en avanzar con la especialización en materia de cibercrimen bajo programas conjuntos entre ingenieros y técnicos, siendo esta la manera de tener expertos profesionales que puedan defender a las víctimas de estos delitos tecnológicos.

Delitos Informáticos – Cibercrimen

1. ¿Qué es el cibercrimen?

El cibercrimen es una actividad delictiva que implica un ordenador, una red informática o un dispositivo con conexión a la red, planteando una amenaza crítica para empresas y personas naturales toda vez que es una acción criminal que goza del anonimato que en muchas ocasiones las redes otorgan, estas acciones criminales vienen avanzado de una manera muy rápida donde hasta hace unos pocos años el alcance que se tenía era solo de cibervandalismo, siendo lo más común en esta acción que se provocara un daño en un PC o varios PC´s y algunos daños colaterales donde dejaban archivos y equipos fuera de servicio, en ese momento estos ataques se generaban principalmente por llamados virus y gusanos (Códigos informáticos que afectan un sistema operativo), sin embargo este cibervandalismo ha evolucionado con mucha rapidez y pasando las esferas del crimen y crimen organizado en donde tanto **hackers** como **crackers** se reinventan para idear nuevos métodos mediante códigos avanzados tanto para mejorar la seguridad informática en el caso de los **hackers** (regidos por un código ético), como para vulnerar los software de defensa informática y generar daños en los sistemas en el caso de los **crackers,** quienes finalmente vienen siendo los cibercriminales actuando ya sea de manera independiente o grupos organizados mediante técnicas avanzadas, quienes principalmente buscan un fin económico y en menor volumen con fines políticos o personales.

2. El cibercrimen en Colombia y su tendencia.

Según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) 8 de cada 10 colombianos usan actualmente internet, 6 de cada 10 colombianos tienen acceso móvil a Internet y 7 de cada 10 accesos móviles a Internet se logran en tecnología 4G (mintic, 2020), esto lo único que demuestra es que la penetración de Internet va en crecimiento exponencial, pero así mismo como incrementa la utilización de estos medios de interconexión aumenta también los ataques cibernéticos en donde actualmente el 45,5% de denuncias se hacen por canales virtuales y se ha reportado 28.827 incidentes de ciberseguridad empresarial, actualmente los ataques por malware han tenido un crecimiento del 612% ubicando a Colombia en uno de los países que recibió el mayor número de ataques en Latinoamérica por ransonware (Programa de software maliciosos que infecta computadores, mostrando sms que exigen el pago de dinero para restablecer el funcionamiento del sistema), siendo este secuestro de datos "Obstaculización de la información" un tipo de delito que no está configurada expresamente en nuestra legislación, en Colombia el hurto por medios informáticos y similares es el tipo de crimen de mayor frecuencia con un 68%, seguido del acceso abusivo a un sistema informático y violación de datos personales, entendiendo con esto que el foco de los cibercriminales desde y hacia Colombia esta hacia los temas financieros comerciales.

Hay que destacar que ni en el Código Penal Colombiano y tampoco en el alcance dado con la Ley 1273 del 2009 se contempla expresamente el concepto de ciberdelitos, cibercrimen, ni delito informático en ningún capítulo en concreto, sino que se definen las distintas conductas delictivas a partir de una acción relacionada con las nuevas tecnologías de la información y las comunicaciones, lo que aumenta la dificulta punible de estas acciones en lo que se dará alcance más adelante.

3. Retos frente al cibercrimen.

En Colombia el proceso de reglamentación jurídica en Derecho Penal con referencia a las tecnologías de la información avanza de manera progresiva mediante esfuerzos del Estado Colombiano con la expedición de normas de carácter especial que regulan los delitos informáticos como lo es la expedición de la Ley 1273 del 2009 dando surgimiento del bien jurídico "de la protección de la información y de los datos" que pretende dar respuesta al cibercrimen, pero que al revisarse desde la doctrina y el derecho comparado, se podrá vislumbrar la dificultad de la aplicación en el ámbito nacional, dando como resultado un desconocimiento o un mal ejercicio legal (Acuña Gamba & Sotelo Vargas, 2017), también se destaca la aprobación e incorporación de protocolos internacionales como lo es el convenio sobre la ciberdelincuencia de Budapest del 23 de Noviembre de 2001 por medio del cual se propende por el diseño y aplicación de una política criminal común para combatir el aumento de los delitos cibernéticos derivados revolución industrial 4.0 todo con el fin de buscar alternativas de tratamiento judicial a los autores de comisión de estos delitos informáticos, sin embargo las legislaciones en muchas ocasiones estan quedando rezagadas en cuanto a la tipificación de nuevos y sofisticados delitos, si a ello se le suma que muchas veces se cometen desde ámbitos externos a la jurisdicción del país, volviéndose un tema de impunidad por la misma complejidad de su detección y coordinación internacional entre países y es por eso que se debe buscar establecer una política penal común y alineada entre países y esto solo se obtiene tipificando los delitos informáticos de manera uniforme entre los países apoyados en este convenio, ya que en la actualidad es el único instrumento internacional vinculante sobre cibercrimen.

Internacionalmente se ha identificado la necesidad de definir políticas claras de ciberseguridad en concordancia con los avances tecnológicos y las nuevas modalidades de cibercrimen, para ello

varios países ya han definido acciones preventivas, sin embargo en Colombia no se identifica una política de ciberseguridad clara que contenga un sistema organizacional y un marco normativo fuerte para contrarrestar estos delitos cibernéticos, solo hasta el año inmediatamente anterior se ha empezado a plantear tan solo una visión rectora mediante el CONPES 3701/ 2011 "Lineamientos de política para la Ciberseguridad y Ciberdefensa", acción que por el momento está en curso y avanza lentamente acompañado del CONPES 3854/2016 "Política nacional de seguridad digital" el cual comprende 4 principios importantes para la implementación los cuales son:

1. Establecer un marco institucional de seguridad digital.
2. Diseñar la gestión del riesgo en la seguridad digital.
3. Fortalecer la defensa y la seguridad nacional en el entorno digital.
4. Generar mecanismos de cooperación, asistencia y seguridad digital.

Sin embargo la ejecución de estas políticas no van a la misma velocidad que si lo hacen las acciones delictivas reinventándose cada día más y es por eso que se hace necesario que al margen de estas políticas el Derecho Penal brinde todas las garantías al momento de hacer uso de estas plataformas, asegurando la no afectación del derecho a la intimidad en este ámbito tecnológico que tratamos.

Como se refirió anteriormente, la deslocalización es otro de los retos representativos en este tipo de delitos y en este sentido, a efectos procesales, hay que matizar que la conducta delictiva puede tener orígenes deslocalizados (uno o varios países) y los efectos de esos delitos producirse en otro u otros tantos, de hecho puede resultar difícil determinar dónde se ha cometido la acción o por parte de quién debido a las múltiples posibilidades de incognito y/o borrado de trazabilidad de los datos que utilizan los perpetradores, claramente afectando a la competencia jurisdiccional, a la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento,

ya que la regla general tradicional se refiere al lugar de comisión del delito acogiéndose al principio de territorialidad, dadas las dificultades de ubicación geográfica precisa en estos delitos en donde tanto la acción como el resultado de esta se puede presentar en diferentes países tanto la doctrina como la jurisprudencia orientar a apreciar la teoría de la ubicuidad que tiene en cuenta como lugar de comisión del delito en el lugar en el que se ha producido la acción como el resultado dañoso, sin ser esta la solución definitiva toda vez que en este campo ya no solo se habla de un delito nacional, sino que ya trascienden fronteras y por ende dificulta más la investigación y enjuiciamiento de estas conductas, si se pone de presente que en muchas ocasiones la conducta delictiva se puede haber llevado a cabo en un país con una legislación incompleta o permisiva con respecto a conductas nocivas cometidas a través de sistemas informáticos, casos en los que no poseen medios de detección y persecución adecuados, o no han ratificado ningún tratado de extradición, esto sin expresar el cuidado y protección que se tiene de los estados cuando de juzgar a un ciudadano propio en otro país se refiere.

4. Clasificación de las modalidades de cibercrimen.

Actualmente mediante el convenio de ciberdelincuencia firmado en noviembre del 2001 en Budapest y sobre el cual se hizo mención anteriormente se han clasificado los delitos informáticos en grupos:

1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

    1.1 Acceso ilícito a sistemas informáticos

1.2 Interceptación ilícita de datos informáticos

1.3 Interferencia en el funcionamiento de un sistema informático

1.4 Abuso de dispositivos que faciliten la comisión de delitos

Algunos ejemplos de este grupo son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware[2] y de keylogger[3] que permiten acceder a algunas acciones de un sistema operativo sin autorización del usuario.

2) El segundo grupo se encuentra en los delitos de fraude:

2.1 Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

2.2 Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

2.3 Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

Por ejemplo el borrado fraudulento de datos o la corrupción de fieros, carpetas, datos del sistema.

---

[2] El spyware es una forma de malware que se oculta en su dispositivo, controla su actividad y le roba información confidencial como datos bancarios y contraseñas.

[3] Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en una computadora, acceso a los datos del portapapeles y las direcciones del sitio sin la captura de pantalla, todo esto sin el permiso ni el conocimiento del usuario administrador.

3) Existe un tercer grupo definido en:

3.1 Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

3.2 Delitos relacionados con infracciones de la propiedad intelectual y derecho afines (Consejo de Europa, 2008)

El el Consejo de Europa adiciono otros delitos al convenio de ciberdelincuencia el cual se podría definir como un cuarto grupo:

4) Actos de racismos y xenofobia.

4.1 Difusión de material xenófobo o racista

4.2 Insultos o amenazas con motivación racista o xenófobo

4.3 Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Posterior a esta clasificación no cabe duda que estos cambios sociales por medio de la tecnología conllevan a que el Derecho Penal se ocupe de estas conductas lesivas, más aun cuando el cibercrimen en Colombia tiene una motivación económica y colocando al hurto por medios informáticos como uno de los delitos más denunciados y para el cual se tiene en la Ley 1273 del 2009 el articulo 269I. Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Art 269J. Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

Es de esta manera podemos evidenciar que esta ley empieza a buscar la judicialización de delitos informáticos, pero sin ser una ley suficiente para los niveles de criminalidad cibernéticos actuales toda vez que las modalidades de modus operandi son muy variables y no se pueden tipificar y tampoco investigar igual ya que se deben enmarcar muchas otras consideración según el tipo de delito cibernético utilizado como lo es el Phishing[4], Vishing[5], Smishing[6], así pues, se advierte que en materia de responsabilidad penal también se vislumbran nuevos problemas a resolver, ya sea por acciones programadas (Deslocalizadas) o por consecuencia de intervención de crackers en los sistemas operativos y es por ello que hay insistencia a dar un tratamiento específico con razón a lo expuesto durante el desarrollo del artículo.

---

[4] Consiste en el envío de correos electrónicos fraudulentos que dirigen a los clientes a páginas 'web' falsas se solicitan datos de la tarjeta de crédito, DNI, contraseña de banca y luego acceden a las cuentas.

[5] Amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet haciendo referencia al phishing.

[6] Son los mensajes de texto o mensajes por WhatsApp donde el emisor solicita contacto vía telefónico a un número de teléfono falso al recibir la devolución de llamada se procede con la estafa mediante el Vishing.

5. Tipificación actual del cibercrimen.

Antes de entrar a detallar la tipificación del cibercrimen es loable anotar que es a partir de una correcta tipificación de los delitos informáticos que se podrá disminuir el alto porcentaje de impunidad, como también la misma criminalidad en este entorno, pero para poder llegar a una correcta estructuración de la tipificación es necesario identificar las conductas que afectan ese bien jurídico en cuanto a la protección de los datos y la información, contar con funcionarios, profesionales e investigadores expertos en la protección de los datos e información y claro está la necesidad de actualizar e ir a la vanguardia en cuanto a normativa del Derecho Penal corresponde.

Si se tiene presente que el cibercrimen son delitos con características especiales con respecto a la acción, el sujeto, el resultado y su imputación, siendo estas características que exponen que la teoría del delito debe ser perfeccionada sino replanteada en algunos de sus aspectos de estos delitos para poder explicar y aplicar a estas particularidades propias de los delitos digitales que ocurren usualmente en realidades virtuales y deslocalizadas, en las cuales se advierte cada vez más una intervención menos directa del ser humano debido a la oportunidad de programación a futuro de la acción delictiva.

Teniendo en cuenta que para que una conducta sea objeto de la legislación penal, debe considerar los tres elementos fundamentales para ser punible como lo es la tipicidad, la antijuridicidad y la culpabilidad, dicho lo anterior tenemos que en el campo de los delitos informáticos en Colombia no se contemplaba ningún capitulo especifico que trate el tema como bien jurídico tutelado y tutelable y por ende a la luz de la ley 599 del 2000 solo era posible

enmarcar algunos tipos penales encuadrados en otros bienes tutelados diferentes a los informáticos, por ejemplo en el caso de hurtos por medios informáticos no existía norma alguna y el funcionario de justicia solo se podía regir por artículos ya definidos para el hurto cotidiano y no el tecnológico, lo que generaba dificultades en llevar a buen término el proceso por falta de información o material probatorio debido a una modalidad muy diferente a la conocida, por casos como este y otros se hacía necesario y urgente regular y penalizar según corresponda estos delitos bajo una normativa acorde al actuar, a partir de ese momento es que posterior revisión de varios proyectos de ley se crea el bien jurídico tutelable denominado De la Protección de la información y de los datos cuya ley tipifica los siguientes siendo un importante avance pero que finalmente no cubre la totalidad de los delitos y sus modalidades.

I. Acceso abusivo a un sistema informático
II. Obstaculización ilegítima de sistema informático o red de telecomunicación
III. Interceptación de datos informáticos
IV. Daño informático
V. Uso de software malicioso
VI. Violación de datos personales
VII. Suplantación de sitios web

Se entiende entonces que el cibercrimen con referencia a las leyes colombianas y específicamente al código penal es fragmentado en una clasificación más detallada que permite definir como se realiza la conducta y su tipificación en el código penal y es de esta manera que al considerarlos desde diferentes ámbitos delictivos como lo es los ciberataques entendido desde el acceso físico y afectación en sistemas informáticos, la interceptación de las comunicaciones,

denegación de accesibilidad y los delitos informáticos que son los que corresponden a los delitos contra la confidencialidad y los atentados informáticos buscando así garantizar una seguridad jurídica en este ámbito delictivo.

6. Elementos jurídicos del cibercrimen

Actualmente en el sistema jurídico Colombiano y principalmente en nuestra constitución se destaca el artículo 15, siendo este el postulado de mayor proyección en cuanto a delitos informáticos se refiere, toda vez que guarda correlación y se fundamenta en la protección de los datos y la información siendo este el bien jurídico que se afecta en este tipo de delitos informáticos, posterior a la constitución se destacan varias leyes que buscan la protección de una manera u otra de los derechos en cuanto a delitos informáticos se refiere, pero cabe resaltar que estas se han ido presentando en algunos casos de manera desestructurada; la Ley 1915 de 2018 en su articulo12 que busca la protección de derechos de autor, Ley 527 de 1999 en su artículo 2, literal - a – haciendo alusión a la normatividad aplicable para el acceso y uso de los mensajes de datos y el cual busca brindar protección a la información, Ley 1266 de 2008 en donde se da protección al habeas data financiero pero esto sin haberse reglamentado con antelación la ley estatutaria que para el efecto se debería instituir con prelación para el desarrollo de los parámetros jurídicos relativos a la protección de los datos personales por lo que se identificó una nueva necesidad reglamentaria y contextualización al respecto y se expide la Ley estatutaria 1581 de 2012 y claro está la ley 1273 del 2009 que es la ley que más abarca la protección de derechos y judicialización por delitos mediante sistemas tecnológicos resaltando el articulo 269 y

subsiguientes en el código penal los cuales a partir del Título VII BIS refiere la protección de la información y de los datos y la más reciente ley 1928 del 2018 en concordancia y retomando el "Convenio sobre la Ciberdelincuencia" adoptado el 23 de noviembre de 2001 en Budapest y de esta manera tratando de aplicar todas las herramientas jurídicas para evitar su avance.

A estas leyes acompañan los siguientes instrumentos internacionales que ayuda a combatir el cibercrimen y orientan a tener unas políticas homogéneas entre naciones que permitan la correcta investigación y judicialicen de estos delitos dada su alta capacidad de deslocalización territorial, los cuales se refieren a continuación:

El convenio referido en varias oportunidades que es el Convenio sobre la ciberdelincuencia de Budapest del 23 de Noviembre de 2001.

Seguido de la Resolución AG/RES 2004 de la Asamblea General de la Organización de los Estados Americanos el cual orienta a que los Estados miembros examinen y actualicen la estructura y la labor de entidades u organismos internos encargados de hacer cumplir las leyes a modo de adaptarse a los constantes cambios y características de los delitos cibernéticos.

Decisión marco 222/2005 la cual refiere sobre los ataques a los sistemas de información y busca fortalecer los sistemas judiciales mediante la consolidación de un Derecho Penal globalizado que evite este tipo de delitos tanto nacional como internacionalmente.

Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo el cual se refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, esto con el fin de fortalecer la cooperación internacional en la consolidación de un contexto digital con ciertas libertades pero que siempre de seguridad y exista justicia en el tratamiento inadecuado de los datos de las personas tanto naturales como jurídicas.

En este contexto entonces corresponde al legislador determinar las conductas por las que se estarían vulnerando los bienes jurídicos tutelados y a los jueces les cabe la ardua tarea de la adecuación típica mediante la interpretación y aplicación de la norma penal idónea en cumplimiento de los fines esenciales de un Estado Social de derecho, siendo relevante en este punto evitar simplismos jurídicos y asegurar enmarcar las conductas determinadas con exactitud como delito a partir de la argumentación jurídica y el supuesto de hecho, por ello es necesario identificar los contextos *penal* e *informático* para definir de una manera idónea este tipo de delitos.

Aunado a lo anterior y como se hizo referencia en el punto 3 sobre los retos frente al cibercrimen existe un elemento que señala la inaplicabilidad de los preceptos del Derecho Penal con referencia al cibercrimen y delitos cibernéticos y es la dificultad de establecer los parámetros de aplicación de territorialidad, dado que en el contexto cibernético la deslocalización se presenta con facilidad, lo que no permite identificar el autor y en casos donde se identifica, no es posible que sea sancionado y judicializado por el delito cometido, debido a que se ejecutaron estas acciones fuera de las fronteras nacionales, por lo que en el derecho penal colombiano se señala en el artículo 14 de la Ley 599 del 2000 sobre la "Territorialidad. La ley penal colombiana se aplicará a toda persona que la infrinja en el territorio nacional, salvo las excepciones consagradas en el derecho internacional.

La conducta punible se considera realizada:

1. En el lugar donde se desarrolló total o parcialmente la acción.

2. En el lugar donde debió realizarse la acción omitida.

3. En el lugar donde se produjo o debió producirse el resultado.

Con eso tenemos que se previó la posibilidad de cometer delitos por fuera de las fronteras colombianas pero estos criterios que se han definido continúan direccionando al lugar de comisión de los hechos dificultando así la aplicabilidad de la ley penal en cuanto a delitos informáticos, la ley es clara en resaltar que el principio de territorialidad para hacer aplicable una pena es que la acción se cometa dentro del territorio, situación que claramente ha cambiado en la actualidad debido a la cantidad de delitos cometidos en el ciberespacio quedando por fuera de contexto la territorialidad lo que lleva a replantear esa necesidad inminente en la que el Derecho Penal se debe ajustar a las novedades del delito informático, actuando de una manera proactiva y no reactiva como se observa actualmente, si dejamos lo anterior solo en el contexto teórico y de aplicabilidad de este principio de manera precisa en estos delitos cibernéticos y nos trasladamos a la dificultad que representa la capacidad probatoria que se tiene en estos procesos dada la deslocalización y la imposibilidad de individualizar al sujeto activo de la acción delictiva o en otros casos de no poderlo hacer así se identifique, esto debido al mismo principio de territorialidad, llevando a la impunidad de muchos cibercriminales, así pues se decanta claramente la actualidad que vive el sistema judicial colombiano en una necesidad de generar una restructuración bajo un modelo vanguardista y acorde a los retos de la Revolución Industrial 4.0[7], es evidente la necesidad de un Derecho Penal supranacional, colaborativo entre los estados y sobre todo homogenizado en cuanto a delitos informáticos, marcando un símil referente al tratamiento que se da con los Derechos Humanos , considerando que esta es la manera más idónea

[7] se refiere a una nueva fase en la revolución industrial que se enfoca en gran medida en la interconectividad, la automatización, el aprendizaje automatizado y los datos en tiempo real.

de minimizar la impunidad a nivel internacional y dando una respuesta oportuna a la sociedad para que sus derechos afectados y bienes jurídicamente tutelados se vean protegidos.

CONCLUSIONES

Se resalta los avances que ha tenido Colombia en cuanto delitos informáticos se refiere y que son de vital importancia para este contexto del que tratamos, El estado se apoya principalmente en la ley 1273 de 2009 por medio de la cual modifican el código penal colombiano a la luz de reglamentar de mejor manera los delitos informáticos y también en el convenio de Budapest del 2001 siendo estos los pilares más relevantes para la judicialización de estos delitos, pero que finalmente resultar ser insuficientes como se ha referenciado en este artículo al compararlo con los avances que se estan observando en el creciente mundo de las tecnologías, también el desconocimiento y el bajo nivel de cultura informática que se tiene en la sociedad hace que sea cada vez más fácil para los cibercriminales ejecutar sus acciones delictivas, con el agravante que lo pueden hacer incógnitamente, dificultando el actuar judicial y su penalización, las normas penales estan mas orientadas a los delitos físicos y no a los cibernéticos por ende la tipificación y contextualización de estos delitos debe ir madurando de manera vertiginosa para prevenir que los delitos cibernéticos mantengan esa impunidad y puedan ser controlados de manera exitosa.

Es imperativo entonces restructurar y fortalecer de una manera loable y ágil la normativo sobre delitos informáticos, ya que en la actualidad sobre la ley 1273 del 2009 solo contamos con 9 conductas punibles y 8 circunstancias de agravación, pero en donde desafortunadamente los avances en esta materia las han desactualizado parcial o totalmente en un abrir y cerrar de ojos, haciendo reflexionar al poder legislativo sobre cómo se debe actuar en teste tipo de delitos y adelantarnos de una mejor manera en decisiones legislativas que aseguren judicializar en tiempo y forma el actuar delictivo de los cibercriminales sin impunidad, sobre este entendido se debe

valorar que no es un trabajo cargado únicamente a nivel normativo en nuestro sistema judicial, sino que este debe estar acompañado de unas políticas claras de ciberseguridad que modele la protección de la información y los datos de una manera obligatoria para personas jurídicas y naturales buscando así ir un paso delante de los delitos cibernéticos y que estas normativas del Derecho Penal se trabajen interdisciplinariamente con las normas de ciberseguridad y sobre todo con otras ciencias especialistas en mecanismos de seguridad tecnológica, ya que hasta el momento existen grandes vacíos jurídicos en la materia sin vislumbrar propuestas legislativas que se adecuen a los lineamientos sustantivos del Derecho Penal y que rompan los paradigmas actuales en materia de criminalidad cibernética debido al desconocimiento profundo y especialista correlacionado con tecnología-derecho, siendo esta la manera más plausible de atacar esta disrupción tecnológica avanzada.

Finalmente considerando los diferentes retos y oportunidades en materia de seguridad informática, en la normativa adaptada a estos delitos, la velocidad frenética en la que avanza esa materia en contrario con los avances normativos, la deslocalización e identificación adecuada como punto neurálgico de la impunidad y otros tantos conceptos mencionados, se hace necesaria una regulación de manera expedita, pero consecuente con todo lo concerniente al cibercrimen, a fin de llenar esos vacíos legales que represente una afectación para la sociedad, sin perder nunca el concepto clásico de delito, siendo la conducta típica, antijurídica y culpable que castigan las leyes penales pero abarcando ya la correcta identificación, tipificación, deslocalización (Homogenización de las nomas supranacionales en temas de cibercrimen), y de esta manera cerrar la fisuras y vacíos jurídicos entre el cibercrimen y la real judicialización de estos delitos con penas adecuadas a estas acciones en constante crecimiento.

REFERENCIAS BIBLIOGRÁFICAS

24 horas. (14 de 02 de 2017). *Conoce los tipos de hackers y su forma de operar*. Obtenido de https://www.24horas.cl/tendencias/ciencia-tecnologia/conoce-los-tipos-de-hackers-y-su-forma-de-operar--2299770

Acuña Gamba, E. J., & Sotelo Vargas, D. A. (2017). Ley 1273 de 2009: ¿Los jueces del cibercrimen? *Iter Ad Veritatem*.

ANARTE BORRALLO, E. (s.f.). INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL SISTEMA PENAL.

Castillo, C. (s.f.). *'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas?* Obtenido de BBVA: https://www.bbva.com/es/receta-de-joan-roca-de-carrillera-de-cerdo-al-vino-tinto-con-apionabo/

Congreso de la república. (2009). *Ley 1273 de 2009 "Ley de delitos informáticos en Colombia"*.

CONVENIO SOBRE LA CIBERDELINCUENCIA, Sentencia C-224/19 (La Sala Plena de la Corte Constitucional 22 de 05 de 2019).

Jorge Eliécer Ojeda Pérez, F. R. (s.f.). Delitos informáticos y entorno jurídico vigente en Colombia. *Scielo*. Obtenido de http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a03.pdf

kaspersky. (2020). Consejos para protegerse contra el cibercrimen. *kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime

mintic. (29 de 09 de 2020). Colombia siguió mejorando las cifras de conectividad en el primer trimestre del año. *mintic*, 1. Obtenido de https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/151386:Colombia-siguio-mejorando-las-cifras-de-conectividad-en-el-primer-trimestre-del-ano#:~:text=Colombia%20cerr%C3%B3%20el%20primer%20trimestre,registrados%20al%20final%20de%202019.

Parlamento Europeo. (16 de 02 de 2017). *Parlamento Europeo*. Obtenido de https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html?redirect

RAYÓN BALLESTEROS , M. C. (s.f.). Cibercrimen: particularidades en su investigación y enjuiciamiento. *DIALNET*.

TicTac. (2019). Tendecnias del Cibercimen en Colombia 2019 - 2020. *CCIT*. Obtenido de https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

UNIR REVISTA. (2020). Ciberdelincuencia: ¿qué es y cuáles son los ciberdelitos más comunes? *UNIR*. Obtenido de https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/

Acuña Gamba, E. J., & Sotelo Vargas, D. A. (2017). Ley 1273 de 2009: ¿Los jueces del cibercrimen? *Iter Ad Veritatem*.