Sociedad y derecho

Editores

Andrea Johana Aguilar-Barreto
Valmore Bermúdez-Pirela
Yurley Karime Hernández Peña

UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA | VIGILADA MINEDUCACIÓN

DE ALTA CALIDAD
Res. 23095, del MEN

Sociedad y derecho

Editores
Andrea Johana Aguilar-Barreto
Valmore Bermúdez-Pirela
Yurley Karime Hernández Peña

Sociedad y derecho

UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA

UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA

Editores
Andrea Johana Aguilar-Barreto
Valmore Bermúdez-Pirela
Yurley Karime Hernández Peña

Autores
Andrea Johana Aguilar-Barreto
Yurley Karime Hernández Peña
Carlos Efrén Largo Leal
Carlos Fernando Hernández Morantes
Clara Paola Aguilar Barreto
Claudia Eufemia Parra Meaury
Deisy Marcela Caballero Flórez
Diego Alexander Jaimes Monsalve
Edison Giovanni Medina Ramírez
Elizabeth Pérez García
Erika Nathalia Ordóñez Mahecha
Ever Santafé Prada
Gladys Shirley Ramírez Villamizar
Javier Antonio Alba Niño
José Iván Silva Rincón
Karol Stephanie Cabrera Poveda
LeidyYasmin Quintero Ortega
Leonardo Yotuhel Díaz Guecha
Linda Katherine Murcia Sanabria
Martha Isabel Jáuregui Hernández
Michael Javier Guerrero González
Nereyda Johana Quintero Bayona
Oscar Leonardo Medina González
Paola Sánchez Jiménez
Peter Jesús Niño Villegas
Reynaldo Guarín Roa
Samuel Leonardo López Vargas
Sandra Bonnie Flórez Hernández
Viviana Andrea Botello Pradilla
Yonatan Alejandro Aguilar Bautista

EL MINISTERIO DE EDUCACIÓN NACIONAL ACREDITA
INSTITUCIONALMENTE A LA UNIVERSIDAD SIMÓN BOLÍVAR
Resolución 23095, del 15 de diciembre de 2016

Sociedad y derecho

Editores
©Andrea Johana Aguilar-Barreto
©Valmore Bermúdez-Pirela
©Yurley Karime Hernández Peña

Autores
©Andrea Johana Aguilar-Barreto
©Yurley Karime Hernández Peña
©Carlos Efrén Largo Leal
©Carlos Fernando Hernández Morantes
©Clara Paola Aguilar-Barreto
©Claudia Eufemia Parra Meaury
©Deisy Marcela Caballero Flórez
©Diego Alexander Jaimes Monsalve
©Edison Giovanni Medina Ramírez
©Elizabeth Pérez García
©Erika Nathalia Ordóñez Mahecha
©Ever Santafé Prada
©Gladys Shirley Ramírez Villamizar
©Javier Antonio Alba Niño
©José Iván Silva Rincón
©Karol Stephanie Cabrera Poveda
©Leidy Yasmin Quintero Ortega
©Leonardo Yotuhel Díaz Guecha
©Linda Katherine Murcia Sanabria
©Martha Isabel Jáuregui Hernández
©Michael Javier Guerrero González
©Nereyda Johana Quintero Bayona
©Oscar Leonardo Medina González
©Paola Sánchez Jiménez
©Peter Jesús Niño Villegas
©Reynaldo Guarín Roa
©Samuel Leonardo López Vargas
©Sandra Bonnie Flórez Hernández
©Viviana Andrea Botello Pradilla
©Yonatan Alejandro Aguilar-Bautista

Sociedad y derecho / editores Andrea Johana Aguilar-Barreto, Valmore Bermúdez-Pirela, Yurley Karime Hernández Peña; Carlos Efrén Largo Leal [y otros 29] -- Barranquilla: Ediciones Universidad Simón Bolívar, 2018.

206 páginas; ilustraciones, tablas.
ISBN: 978-958-5533-36-3(Versión electrónica)

1. Responsabilidad médica2. Arbitraje y laudo 3. Arbitraje Internacional4. Emigración e inmigración -- Aspectos socio-jurídicos 5. Derechos Humanos 6. Derecho ambiental -- Análisis jurisprudencial 7. Acuerdos de Paz -- Análisis histórico -- Colombia 7. Delitos informáticos -- Análisis jurídico -- Colombia I. Aguilar-Barreto, Andrea Johana, editor II. Bermúdez-Pirela, Valmore, editor III.Hernández Peña, Yurley Karime, editor IV. Largo Leal, Carlos Efrén V. Hernández Morantes, Carlos Fernando VI. Aguilar Barreto, Clara Paola VII. Parra Meaury, Claudia Eufemia VIII. Caballero Flórez, Deisy Marcela IX. Jaimes Monsalve, Diego Alexander X. Medina Ramírez, Edison Giovenni XI. Pérez García, Elizabeth XII. Ordoñez Mahecha, Erika Nathalia XIII. Santafé Prada, Ever XIV. Ramírez Villamizar, Gladys Shirley XV. Alba Niño, Javier Antonio XVI. Silva Rincón, José Iván XVII. Cabrera Poveda, Karol Stephanie XVIII. Quintero Ortega, Leidy Yasmin XIX. Díaz Guecha, Leonardo Yotuhel XX. Murcia Sanabria, Linda Katherine XXI. Jáuregui Hernández, Martha Isabel XXII. Guerrero González, Michael Javier XXIII. Quintero Bayona, Nereyda Johana XXIV. Medina González, Oscar Leonardo XXV. Sánchez Jiménez, Paola XXVI. Niño Villegas, Peter Jesús XXVII. Guarín Roa, Reynaldo XXVIII. López Vargas, Samuel Leonardo XIX. Flórez Hernández, Sandra Bonnie XXX. Botello Pradilla, Viviana Andrea XXXI. Aguilar Bautista, Yonatan Alejandro XXXII. Tít.

340 S678 2018 Sistema de Clasificación Decimal Dewey 21ª edición

Universidad Simón Bolívar – Sistema de Bibliotecas

Grupos de investigación
Altos Estudios de Frontera (ALEF), Universidad Simón Bolívar, Colombia
Rina Mazuera Arias

ISBN: 978-958-5533-36-3

Impreso en Barranquilla, Colombia. Depósito legal según el Decreto 460 de 1995. El Fondo Editorial Ediciones Universidad Simón Bolívar se adhiere a la filosofía del acceso abierto y permite libremente la consulta, descarga, reproducción o enlace para uso de sus contenidos, bajo una licencia Creative Commons Atribución 4.0 Internacional. https://creativecommons.org/licenses/by/4.0/

Carrera 54 No. 59-102
http://publicaciones.unisimonbolivar.edu.co/edicionesUSB/dptopublicaciones@unisimonbolivar.edu.co
Barranquilla y Cúcuta

Producción Editorial
Conocimiento Digital Accesible. Mary Barroso, Lisa Escobar
Urb. San Benito vereda 19 casa 5. Municipio Santa Rita del Estado Zulia- Venezuela. Apartado postal 4020. Teléfono: +582645589485, +584246361167. Correo electrónico:marybarroso27@gmail.com, conocimiento.digital.a@gmail.com

Diciembre del 2018

Barranquilla

Made in Colombia

Como citar este libro

Aguilar-Barreto. A.J., Bermúdez-Pirela. V. y Hernández Peña, Y.K. (Eds.) (2018). Sociedad y derecho. Cúcuta, Colombia: Ediciones Universidad Simón Bolívar

DOI:

9 FALENCIAS EN EL SISTEMA LEGISLATIVO EN LA UNIFICACIÓN DE LAS INFRACCIONES INFORMÁTICAS EN COLOMBIA

Edison Giovanni Medina Ramírez
Abogado en formación, Universidad Simón Bolívar

Nereyda Johana Quintero Bayona
Abogado en formación, Universidad Simón Bolívar

José Iván Silva Rincón
Abogado en formación, Universidad Simón Bolívar

Clara Paola Aguilar-Barreto
Abogada, Universidad Libre. Especialista en Derecho Contencioso Administrativa, Externado de Colombia. Maestrante en derecho Púbico, Externado de Colombia. Docente Investigador Universidad Simón Bolívar, Colombia. Orcid: ***https://orcid.org/0000-0003-1185-5154***

Yurley Karime Hernández Peña
Doctorando en Ciencias de la Educación de la Universidad Simón Bolívar, Magister docencia de la Química de la Universidad Pedagógica Nacional, Licencia en Biología y Química de la Universidad Francisco de Paula Santander, Docente Investigadora adscrita al grupo de investigación Educación y Ciencias Sociales de Universidad Simón Bolívar, Cúcuta, Colombia. Orcid: https://orcid.org/0000-0002-0798-5178. E-mail: hyurley05@unisimonbolivar.edu.co

Resumen

La globalización y el progreso de la tecnología han desencadenado fenómenos que actualmente mueven masas, al punto de ser indispensables en la cotidianidad del ciudadano promedio, se trata de la internet, en especial los portales brindados por todos los sistemas digitales y las redes sociales; ya que ha generado importantes avances creando una proyección y un desarrollo en toda la población moderna. Con este desarrollo se busca traspasar las barreras que existían frente a la necesidad de comunicación, pues antes eran necesarios utilizar el

traslado de los hombres o manejar medios de información como las cartas a través del correo, que generalmente demoraban semanas y meses para llegar a su destino; por tal razón la innovación y la evolución de estos medios trae grandes beneficios en optimización de tiempo y otros elementos, también comporta serios riesgos como lo es la presencia de delitos informáticos; el presente artículo aborda los delitos y el cómo el mundo, ha tenido que avanzar en la normatividad jurídica para hacer frente a esos *ciber* delitos. Además, se buscó analizar la evolución de estos sistemas de comunicación pero enfocándose en el marco conceptual y jurídico necesario para incluir las infracciones informáticas, teniendo en cuenta los planteamientos y estudios realizados por diferentes juristas nacionales e internacionales quienes han establecido la base jurídica y normas sobre este tema en Colombia, por tal razón se planteó y creó la ley 1273 de 2009, con la cual se buscó que el país se equipare con las normativas internacionales sobre la *ciber* criminalidad que ha venido infringiendo las distintas áreas de sectores tan esenciales e importantes como el de las comunicaciones personales, las empresariales e incluso institucionales. Cada día aumenta la tendencia a presentar denuncias ante la rama judicial pues con esta modalidad de delitos no sólo se transgrede el campo tecnológico sino también con este modus operandi los delincuentes han encontrado la manera de acceder a otros campos como el económico, social e incluso político; de acuerdo con algunos autores como Ojeda J., Rincón F., Flórez, M. y Daza L. (2010) el delito "*debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática*"

Palabras clave: Delito informático, *ciber* delincuencia, derecho penal, globalización, tutela judicial efectiva.

Failures in the legislative system in the unification of computer infractions in Colombia

Abstract

Globalization and the progress of technology have triggered phenomena that currently move masses, to the point of being indispensable in the daily life of the average citizen, it is about the Internet especially the portals offered by all digital systems and through social networks ; what has generated important advances creating a projection and a development in the whole modern population. This development seeks to overcome the barriers that existed in the face of the need for communication, since previously it was necessary to use the movement of people or to use means of communication such as letters through the mail, which generally took weeks and months to reach their destination; for this reason the innovation and evolution of these media brings great benefits in optimization of time and other elements, also involves serious risks such as the presence of computer crimes; This article deals with crimes and how the world has had to advance legal regulations to deal with these cybercrimes. In addition, it sought to analyze the evolution of these communication systems but focusing on the conceptual and legal framework necessary

to frame computer crimes, taking into account the approaches and studies carried out by different national and international jurists who have established the legal basis and rules on this issue in Colombia, which is why Law 1273 of 2009 was designed and implemented, which sought to make our country equate with international regulations on cyber-crime that has been violating the different areas of such essential and important sectors such as personal, business and even institutional communications. Every day there is an increasing tendency to lodge complaints with the judicial branch, since this type of crime not only transgresses the technological field but also with this modus operandi, criminals have found a way to access other fields with economic, social and even political; according to some authors such as Ojeda J., Rincon F., Flórez, M. and Daza, L. (2010) this crime "must be known, evaluated and confronted, for which the analysis of the norm, its contribution and scope can give other elements of judgment to understand the reality of our organizations and visualize their policies and strategies, in light of the same norm and of the global standards on computer security"

Keywords: cybercrime, Criminal Law, globalization, effective judicial protection.

Introducción

Los cambios acaecidos por la globalización han creado un fenómeno que ha permeado varias áreas del derecho, presentando retos ante la formulación de garantías que concuerden con las metas que ha traído consigo la globalización y la disposición del transporte de información por las redes en especial la internet; gracias a la acogida que ha tenido en las poblaciones actuales ya que cada día se vuelve más accesible, lo cual a su vez ha ofrecido una forma para manejar mejor el tiempo y por ende el dinero, mediante las soluciones rápidas que proporciona esta novedad y demostrando el desarrollo en el área tecnológica e informática, así lo detallan Aguilar-Barreto y Ibañez (2017). La internet, facilita cada día que este desarrollo se vea reflejado en otros elementos de comunicación como lo son los teléfonos celulares ya que en general la comunicación satelital se encuentra en pleno auge; esto hace que estos elementos sean indispensables al agregarles múltiples beneficios, pero también es necesario tener claro que dicha facilidad para su acceso a hecho surgir una gran variedad de delitos con los cuales se viola un derecho constitucional y es protegido por el derecho penal.

Por esto, Colombia ha obtenido gran reconocimiento debido a los avances legislativos de gran importancia logrados en la legislación

nacional y colocándonos como uno de los países pioneros en América latina en seguridad informática, al afrontar de este modo los nuevos retos que aparecen en esta era informática y los cuales se logra al tipificar estos tipos de delitos y crear una categoría para estos como delitos informáticos como lo explican desde el desarrollo tecnológico Aguilar-Barreto e Ibañez (2017). Sin embargo, Mc Luhany Fiore (2009) habla sobre:

"los desarrollos informáticos y el uso del internet se encuentra en su índice máximo, y afirma que estos son un exponente en materia de comunicaciones, trayendo múltiples beneficios y consigo resultados adversos para los derechos de los usuarios".

Adquiriendo estadísticamente, esto genera una serie de impedimentos que deben tener en cuenta y encomendar cada día más del resguardo de la intimidad personal; en un segmento tan impreciso como el *ciber* espacio, estos delitos terminan afectando directamente a los cibernautas quienes ven vulnerados muchos derechos esenciales como el bien jurídico para salvaguardar la información y los datos. En el presente artículo se visualiza el panorama de la *ciber* delincuencia, evidenciando que los delincuentes sacan provecho de las equivocaciones que cometen los ordenamientos jurídicos nacionales, ya que es tan restrictivo el tema de la territorialidad que tiene como consecuencia la imposibilidad de la identificación real o precisa de quien realiza el delito y entre otros aspectos; así mismo se abordarán temáticas atadas a la alteración de documentos profundizando en las leyes que rigen estos delitos en Colombia.

Metodología

En el presente artículo se plantea el paradigma interpretativo o método cualitativo en donde se utiliza el diseño hermenéutico, y la decisión de los lineamientos existentes del Derecho Penal, para los casos en donde se presentan delitos informáticos y se hace necesaria la defensa del bien legal de la información y los datos personales.

Este método también se puede caracterizar como método documental, ya que para ello se debe realizar una revisión documental

tanto de la norma como del análisis relacionados con el tema propuesto, donde se tiene en cuenta algunas categorías como la *ciber* delincuencia, analizada desde un punto de vista que se ha definido como fenómeno actual de afectación de derechos, en ese sentido se pretende analizar las falencias en portales digitales para la aplicación o amparo de los derechos con lo ofrecido en el ordenamiento penal actual.

Resultados y discusión

Para Rodríguez (2002): "La ciber delincuencia son aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, sin perjuicio de que además puedan suponer una puesta en peligro o lesión de bienes jurídicos distintos".

Por lo anterior, se pude diferir que el *ciber*delito se puede entender como la ejecución de una operación que reuniendo las particularidades que definen el concepto de delito, se lleva a cabo utilizando un dispositivo informático, o quebrantando los derechos del titular de un aparato informático ya sea hardware o software. Para que un delito sea configurado dentro de los ciber delito es estrictamente necesario que en su realización o en alguna de sus partes sea utilizado algún mecanismo electrónico, para que esta conducta sea considera punible y como resultado dicha acción es traducida o entendida como la violación a un método informático. Los tipos de delitos más frecuentes son la creación y utilización indebida de información que se halla recopilada en operaciones informáticas, y se presenta en otros como la transformación y destrucción de estos en sistemas informáticos.

De acuerdo a lo anteriormente expuesto, el bien jurídico que se protege se encarga de tipificar y puntualizar las amenazas informáticas para que la ley que lo reglamenta lo considere como un bien jurídico nuevo, con una característica esencialmente virtual pero orientada hacia la protección de la información sensible y la confiabilidad de datos personales recopilados en los sistemas de información virtual. Dentro de la delincuencia cibernética el fraude informático es considerado como

estafa y establece que: "*esta consiste en la transmisión no consentida de activos a través de la manipulación o alteración de datos informáticos*". Rodríguez (2002).

Por consiguiente, según los criterios doctrinales se está ante un comportamiento simultáneo a una conducta enmarcada como estafa, en donde el actuar del sujeto activo se encuentra guiado hacia un fin lucrativo y se dirige al usufructo patrimonial, donde el fraude es un desafío mediante engaño lo cual no se debe a un error de la víctima sino a la estafa que se hace mediante un sistema informático. Además, se encuadra dentro de los *ciber*delitos, la clonación de las tarjetas de débito, crédito o de cualquier sistema de pago similar con tarjetas magnéticas o con chips, ya que esta acción en años posteriores ha tenido un aumento progresivo en la frecuencia con la que denuncia o detecta estas actividades, por lo cual se revelan la existencia de organizaciones criminales especializadas en el encargo hacia este tipo de delitos; por tal motivo los establecimientos bancarios se han visto abocados a realizar las correspondientes previsiones en sus sistema informáticos de manejo financiero, para bloquear y restringir al máximo el acceso a estos datos.

Desde una perspectiva más enfocada a la legislación penal actual, las conductas conocidas como el *phishing* y *pharming* se encuentran tipificadas en la nueva modalidad de estafa a través de medios informáticos; las jurisprudencias buscan principalmente definir que todas estas acciones son destinadas a duplicar páginas web con la conclusión de atraer de esta manera la información financiera de los usuarios para con ésta hacer transferencias, compras o avances en efectivo, lo cual hace una disminución patrimonial no autorizada y de este modo están perjudicando a un tercero, produciendo un engaño en el titular de la cuenta mediante el envío de mensajes falsos que les termina generando pérdidas económicas.

La forma más usada por los delincuentes en estos casos es la elaboración de un sitio web falso o la réplica de un ciberespacio, pero cuya finalidad es engañar al usuario y es por esta razón que esta labor se

considera como delito de falsedad documental, y a su vez es tipificado como delito de recepción de información íntima y personal de datos en medios informáticos y esto pretende precisamente la creación de toda una estructura criminal que generalmente la mayor parte de los casos se propagan internacionalmente, lo cual incrementa la pena para quien realiza este tipo de actos fraudulentos de acuerdo a lo establecido en cada normatividad territorial actual, en Colombia, la ley 1581 de 2012 que recientemente ha entrado en vigor y con la cual a través de ésta se protegen los datos sensibles. Al estar en ella bien especificado y tipificando los delitos y con esto volviéndolos punibles y sancionándolos con multas económicas e incluso de acuerdo al daño causado con prisión (Aguilar-Barreto y otros, 2018).

En Colombia, se viene presentando un preocupante aumento en la denuncias por falsificación de documentos digitales, que son usados como instrumentos de pago electrónicos debido a esto ha tenido que ser determinado como un delito del ciberespacio, provocando que este sea considerado dentro de las conductas delictivas de tipo penal y entendido como uno de los nuevos delitos adoptados por las cortes como delitos punibles y juzgables. En general, todo documento donde se incluyan características electrónicas podría incluirse dentro de los *ciber* delitos o delitos informáticos; y con la sentencia T-277/15 la Legislación Colombiana contempla sustancialmente salvaguardar el derecho a la intimidad personal y familiar, donde se vea afectado su imagen, la dignidad y el pleno ejercicio de sus derechos.

Asimismo, para darle aplicación al ejercicio del derecho colombiano, el habeas data es una vía de acceso al reajuste y rectificación de la información dentro del proceso del método dado en medios electrónicos, ya sea con un carácter público o solamente privado que tiene todo ciudadano en Colombia, no sólo las personas naturales se ven directamente afectadas por los delitos informáticos, también las empresas se convierten en víctimas diariamente y lamentablemente la preparación para contrarrestar estos delitos o ataques es mínima, llevando consigo que los datos de millones de usuarios sean vulnerados, pero el gobierno busca

crear en este momento dentro de los organismos judiciales unidades especializadas, las cuales hacen énfasis sobre la seguridad actuando en la prevención, corrección, detección efectiva en los casos o violaciones a la intimidad a través de su información, como lo aborda Díaz, Aguilar-Barreto y Bonilla (2018).

El criminólogo Edwin Sutherland, (1943) fue "el primero en manejar el término delitos de cuello blanco además presentó dos puntos exactos para incluir al autor del delito: primero que el sujeto activo del delito debe ser un individuo de cierto estatus social y económico; segundo que el cometido nunca podrá justificarse en la falta de medios económicos, carencia en la educación, poco conocimiento al contrario son individuos con una gran especialidad en informática que conocen muy bien las particularidades de la programación de sistemas computados, de esta manera es como logran un manejo técnico de las herramientas necesarias para quebrantar la seguridad de un sistema automatizado".

Por otro lado, en los niveles corporativos la confidencialidad opera de manera que dependiendo del usuario y el rol dentro de la organización se le otorgan diversos permisos, por ejemplo, en un banco se denotaría diferentes niveles de acceso que se le otorgan a cada usuario, dependiendo de la labor que ejerza dentro del banco ya que la información financiera tiene un tratamiento confidencial. Para el caso específico de las corporaciones financieras, esto depende del rol que tiene el autor del delito dentro de esa organización ya que se les otorgan diversas claves, accesos o permisos, a cada usuario dependiendo de la labor que desempeñe dentro del banco ya que como es bien sabido la información financiera tiene un tratamiento muy confidencial.

Por consiguiente para lograr este propósito, estas corporaciones financieras hacen uso de diversas herramientas de seguridad informática, como las aplicaciones y programas, los cuales permiten encriptar toda esa información para reducir al máximo la debilidad de los datos confidenciales de los beneficiarios; en estos casos la información es sensible, por tal motivo no todas las personas tienen acceso a la información y

en los procesos de que esta sea extraída por terceros son manejadas con fines delictivos. Por esta razón el Estado colombiano vio la necesidad de derogar ciertos artículos de la ley 1273 de 2009, para proteger derechos y con la elaboración de la ley 1581 de 2012 permitió salvaguardar los datos íntimos y reglamentar los derechos que tienen los Colombianos al habeas data y la importancia que se tiene del mismo.

De igual manera, mediante la sentencia 748 de 2011 se establecieron controles Constitucionales a la ley 1581, buscando que todos los antecedentes asentados en cualquier base de datos sean protegidos y permitan efectuar operaciones, recolección, acaparamiento, circulación, uso o supresión por parte de entidades de carácter privado y público. Es por esto que la Corte Constitucional anunció el habeas data como garantía del derecho fundamental a la intimidad, y por ello la defensa de los datos hace referencia a la vida familiar y personal, lo cual se considera específicamente impenetrables, pues son entendidos como fundamentales para efectuar su proyecto de vida y ningún otro particular puede interferir o apoderarse de éstos, ya que se evita el desarrollo normal de los ciudadanos colombianos e incluso extranjeros dentro del propio territorio.

En la actualidad, el habeas data es un derecho independiente, combinado por la independencia económica e independencia informática; este derecho es considerado fundamental y debe ser eficaz al momento de la protección se deben generar los mecanismos que la garanticen, los cuales no sólo deben ser reafirmados solo por jueces, sino también por parte de una institución administrativa, que además de controlar y vigilar a todos los sujetos aplicando tanto el derecho público como al privado, obedeciendo que cada caso en particular desempeñe su función de una manera efectiva, buscando siempre el resguardo de datos en razón de su carácter técnico, y que éstas tengan la capacidad de instaurar políticas públicas encaminadas a este factor, pero sin el preámbulo del carácter político para el acatamiento de estas disposiciones.

Así mismo, la Ley obliga a todas las entidades ya sean públicas o

privadas a revisar y mantener mecanismos de seguridad sobre el uso y manejo dado a toda la información de carácter personal contenidos en sus bases de datos, para con ello cumplir lo expuesto por Rodríguez (2015). "Al promover un sistemas de información en donde está, no presente fugas que puedan fortalecerse de manera puntual utilizando herramientas dadas por la ley haciendo que estas entidades, definan la forma y la manera que pueden darse los tratamientos y cuáles son los fines y medios esenciales para el tratamiento de éstos, solicitando a los usuarios o titulares quienes deben fungir como responsable y qué tipo de datos pueden transferirse a otras entidades respondiendo así a los principios de la administración de datos y a los derechos a la intimidad y el hábeas data del titular del dato personal".

Según otro autor: "*existe una clasificación de delitos informáticos, la cual está dada por el Convenio de Ciberdelincuencia del Consejo de Europa firmado en noviembre de 2001 en Budapest".* (Pabón 2013). Por dicha clasificación se puede deducir que los delitos informáticos, se dividen en cuatro grandes grupos: acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de delitos; se debe tener claro que esta clasificación se encuentra fundamentada en tres pilares muy necesarios para la seguridad informática que son: la confiabilidad, la integridad y la disponibilidad de los datos en sistemas informáticos, al respecto, también estos pilares solo pueden ser alterados por expertos con un alto conocimiento sobre el tema de programación y seguridad informática los llamados hackers, pero incluso estos también tiene una clasificación definida ya que hay algunos hackers de cuello blanco que son expertos programadores orientados a violar la información de un sistema informático con libertad, con el único fin de evidenciar las fisuras de una determinada red ya que la mayoría de veces son en realidad trabajadores de los sistemas de una entidad que deben estar velando por la seguridad informática.

Además, se encuentra otra categoría de *Hackers* de sombrero negro, los cuales descargan y violan los sistemas sin autorización con pedido

legal o formal ya sea que este le pertenezca a una empresa o entidad del gobierno, pero estos lo hacen es con otros fines encaminados más a la monetización, esta se da cuando el hacker debe realizar ataques a la red del banco con el fin de obtener información clasificada, como por ejemplo cuentas bancarias y números de tarjeta (atenta contra la confidencialidad) o tumbar páginas para que no puedan ser visitadas o redirecciónando al usuario (atenta contra la disponibilidad) esto se lo realizan no solo a las personas naturales sino también a las jurídicas para realizarle desfalcos; pero también se da por el solo hecho de alcanzar algún nivel de popularidad mediante el reconocimiento mediático como incluso como activista enfocado o defensor de sus ideales mediante el campo digital llamado *hacktivismo*.

Por todo lo anterior, estos ataques se están dando con mayor frecuencia, debido a la forma acelerada con la que se maneja demasiada información en estas bases de datos o sistemas digitales de registro financiero, lo cual a su vez ha provocado que mucha de esta información recorra el mundo moviéndose a una velocidad impresionante y haciendo que muchas veces no sea posible la protección total de esta, en especial los datos de carácter más personal; como lo manifiesta Según informe de la Comisión de Regulación de las comunicaciones (2016) "la instrucción de los derechos en los titulares de la información, deben entender que el manejo de la información, se puede disponer del anuncio como tal, a partir de un tiempo prudencial (a los cinco días siguientes de la comunicación), a partir de ahí el titular, puede hacer llegar una carta, en donde comunique a la Superintendencia de Industria y Comercio, sobre las causales de la queja. Seguidamente, debe anexar el formato de autorización diligenciado para poder recolectar los datos y así determinar el canal electrónico y físico para recibir las autorizaciones".

Otros juristas explican el delito informático en forma típica y atípica, entendiendo como típica las conductas antijurídicas y culpables que se realizan en las computadoras como herramienta para la comisión del delito, actitudes ilícitas, y la capacidad o conocimiento que tiene quien comete el delito a través de la computadora o sistemas informáticos; así

mismo la responsabilidad del acceso a esos datos recae en los que fueron autorizados para manejar este tipo de información y son ellos quienes deben definir las finalidades y los métodos que se utilizarán con cada grupo de acuerdo al interés o sensibilidad la información, pues para esto se debe mostrar la política de tratamiento ajustada a la normatividad creada para este propósito ya que por ellos cuentan con esa autorización.

En Colombia los que pueden manejar la información digital de personas tanto naturales como jurídicas deben ser asentados en sistemas bien protegidos, pues que sobre ellas recae la disposición de la base de datos que de ser accedida sin autorización genera unas sanciones para quienes hayan sido responsables del cuidado y tratamiento de información personal ya sean personas naturales o jurídicas, dichas sanciones son impuestas por la superintendencia de industria y comercio y comprenden multas de carácter institucional o personal hasta por dos mil S.M.L.M.V., además se pueden suspender la autorización que tenía para hacer las actividades ligadas a esta información hasta por seis meses y puede llevarse a cabo un cierre inmediato y definitivo de la actividad que esté ligada a estos datos.

En pocas palabras, las empresas, corporaciones o entidades bancarias, son la únicas responsables de la información que acorde con el principio de la buena fe depositan en ellos los clientes, y los convierte en únicos responsables de los daños o robos virtuales de que lleguen a ser víctimas sus clientes, es por ello que se ha querido dejar claro cuáles son las leyes que las regulan y generan obligaciones sobre estas entidades, entonces es bueno pasar a establecer cuál es la ruta jurídica que debe seguir quien sea víctima de cualquier conducta punible y sancionable por el ordenamiento penal colombiano; lo primero que se debe hacer al enterarse que está siendo o fue víctima de algún robo, suplantación o estafa a través de medios electrónicos es utilizar este mismo medio a su favor y notificar a la entidad, corporación o banco de lo que está sucediendo para que este de forma inmediata suspenda, apague, bloqueé la tarjeta o evite la realización de más descuentos de la cuenta ya sea crédito o débito. Segundo, cuando la estafa o el robo es por un valor que

se encuentre entre 10 y 150 S.M.L.M.V. ($7´377.170 y $110´657.550) deben demostrar una querella ante la Fiscalía en cualquiera de sus oficinas más cercanas en todo el territorio nacional por parte del titular de la cuenta.

Si la estafa es mayor a 150 S.M.L.M.V., no solo puede denunciar la víctima sino cualquier persona que tenga conocimiento del caso, se pueden presentar en forma verbal o por escrito y sin la necesidad de un abogado, ya sea en los diferentes centros de atención dispuesto para este propósito como las salas de atención al usuario (S.A.U.), la unidad de reacción inmediata (U.R.I.) los centros de atención a víctimas y las casas de justicia. Ya cuando este caso se presenta en un municipio o corregimiento donde no existen ninguna oficina lo puede hacer ante la policía nacional; debe presentar la cédula de ciudadanía y la mayor cantidad de material probatorio posible, que permita la demostración de la estafa o del engaño ya sean: unas facturas, algunos folletos de la empresa o entidad que le pidió sus datos, material fotográfico en físico o en un dispositivo, testimonios, comprobantes de pago o facturas, entre otros.

Asimismo, la Fiscalía hará la indagación de los hechos y los presentará ante un juzgado penal para establecer el autor material del delito, teniendo en cuenta que las entidades bancarias son responsables pero hasta cierto monto y este varía de acuerdo a las políticas propias del banco. El siguiente segmento que se quiere analizar está relacionado a algo muy común y actual que es la información, ya sea que esta esté en texto o en imágenes que puede almacenar un dispositivo móvil en su memoria interna o externa y se trata de los computadores portátiles, las memoria U.S.B, una Tablet o un celular, ya que como lo han demostrado diferentes estudios se está en la época en que se han hecho videos y tomado más fotografías que en todo el tiempo trascurrido desde la aparición de estos dispositivos en la humanidad, lo otro que se demostró es que esto como es apenas lógico, se ha debido a la accesibilidad que se tiene para adquirir y disfrutar estos aparatos, como dichos dispositivos tiene un uso privado los textos e imágenes también almacenadas en ellos terminan siendo sensibles para su propietario, ya que pueden contener contenidos muy íntimos o comprometedores.

Además, es allí donde la legislación colombiana promulgó la ley 1273 del 2009 y creó otros bienes protegidos por el Estado, para velar por el buen nombre o Habeas Data del artículo 15 de la Constitución Colombiana el cual en estos casos es el bien intangible que puede verse afectado por el uso o manejo prohibido de la información personal almacenada en equipos móviles; esto también puede convertirse a su vez en un concurso de hechos punibles al presentarse extorsiones, abusos sexuales, todo lo que se puede presentar por el solo hecho que la víctima no quiere que se rebele o se dé a conocer algunas imágenes o información que tiene en su poder el victimario. Lo complicado de eso es que muchas personas no tienen conocimiento de que las autoridades cuentan con muchas herramientas para colaborar con estas personas en la solución pronta y efectiva para esta situación, y es entonces cuando por querer evitarse un escándalo público terminan convirtiéndose ellos mismos en los creadores del mismo.

Así mismo es muy importante tener claro las formas como la información es obtenida por el victimario, porque si ésta se dio por confianza en él y ella se le entregó de forma voluntaria, pero este ya sea por represalia, venganza o buscando beneficio económico decide publicarla, eso no exime de responsabilidad al culpable o en los casos en que cometiendo un delito este conlleva a otro, como puede ser el hurto de un teléfono móvil o celular que al lograr ser desbloqueado por el victimario descubre una imágenes de un contenido sexual explícito y valiéndose de artimañas pretende extorsionar o acceder sexualmente a la propietaria para no publicar en la WEB esa información. En estos dos casos hipotéticos pero muy comunes se está ante el delito de *sexting* pero para que se configure este se debe presentar el material probatorio como: fotos, videos y mensajes de contenido sexual que son enviados a través de sistemas electrónicos ya sean dispositivos móviles o computadoras; y hacer la respectiva denuncia ante la unidad de delitos sexuales de la Fiscalía en donde narre los hechos que fundan el delito.

También podrá dirigirse a realizar la denuncia ante el cuadrante de la Policía Nacional o la Comisaria de Familia más cercana a su residencia,

donde será enviada a la autoridad competente, durante el transcurso del proceso la Fiscalía deberá solicitar al Ministerio de las Tecnologías de Información y de las Comunicaciones y por medio del proveedor de servicios de internet, bloqueé la página web donde aparecen las imágenes del menor para darle un manejo adecuado a las pruebas para que puedan ser válidas y tenidas en cuenta en un futuro proceso penal.

Por otro lado, la Asociación Internacional de Derecho Penal (1992) adoptó "diversas recomendaciones respecto a los delitos informáticos, estas contemplaban que en la medida en que el derecho penal tradicional no sea suficiente deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad)".

Por consiguiente, los delitos informáticos son difícilmente manifiestos ya que estos delincuentes actúan discretamente y poseen equipos capaces de borrar todo rastro de infracción y fabricación del delito, y desafortunadamente el país no cuenta con personal altamente calificado para indagar dichos hechos ya que al momento de ser denunciados son tipificados como otros bienes jurídicos constituidos en el código penal colombiano; además se debe tener en cuenta que la ley penal de cada Estado solo es aplicable dentro de su territorio, lo que genera un escenario donde mayormente se configura este delito llamado ciberespacio ya que en éste no existen fronteras territoriales. (Laudon y Guercio, (2009); Loja Flórez (2013); Martínez (2006) y McClure, Scambray y Kurtz (2000))

En conclusión, los infractores que cometen esta clase de delitos se mantienen en anonimato como forma de evitar su responsabilidad, ya que no emplean sus propios equipos electrónicos para que no puedan ser detectados, utilizando múltiples virus o en ocasiones se pueden valer de un tercero para *hackear* la información de usuarios que no tienen las medidas de seguridad adecuadas, convirtiéndose en presa fácil de estos criminales que cometen toda clase de trasgresiones vulnerando la intimidad y la privacidad de sus datos.

Conclusiones

En la actualidad, la sociedad post moderna busca crear una comunicación rápida acortando las distancias; en ese sentido el internet ha contribuido al avance acelerado de las Tecnologías de la información y la comunicación permitiendo con la misma premura los delitos informáticos; por ello desde la apertura de la era tecnológica también los gobiernos vieron la necesidad de tipificar y sancionar la apropiación ilícita de la información íntima de quienes utilizan las redes sociales, y esta debe ser considerada para precautelar la integridad y la intimidad personal, que en muchas circunstancias las transgresiones a la seguridad informática no solo afectan la intimidad de una persona sino que pueden afectar a un colectivo en general.

En Colombia, aún existen vacíos legales para la tipificación del delito informático como la apropiación de la información y la privacidad en la red social y debe considerarse un acto antijurídico, además debe ser causa de sanción debido a que lesiona los derechos constitucionales y de pertenencia; siendo las redes sociales un medio de interacción entre personas, que pueden o no compartir los mismos gustos, estas plataformas permiten una comunicación asertiva entre los usuarios pero también es un medio para cometer delito y la poca idea que se tiene del contenido que se propaga en las tecnologías de la información y comunicación es la principal causa que impide salvaguardar los derechos, pues es allí donde los futuros abogados deben reformar la legislación en materia penal, para fortalecer algunos elementos más contundentes en caso de llevarlos ante los jueces del gobierno.

En este orden de ideas, existe la posibilidad que también puedan verse afectados los sistemas de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, entre otros; por el uso indebido que se le dan a los medios electrónicos ya que pueden ser manipulados, permitiendo la comisión de conductas delictivas de distintas características, lo que hace necesario que la Corte en cumplimiento de su deber constitucional y legal adopte medidas para

garantizarle a la sociedad una efectiva protección de aquellos datos que son suministrados por los usuarios para la integra prestación de sus servicios y no lleguen a ser alterados o difundidos de forma irregular donde se vulnere la dignidad humana.

Al Estado se les imposible en muchas ocasiones conocer la verdadera magnitud de los delitos informáticos, ya sea por la falta de denuncias o las falencias que presenta el sistema al investigar y aplicar el procedimiento jurídico adecuado a esta problemática; y en otras ocasiones existe el temor de las entidades de denunciar estos ilícitos por el descrédito que esto les puede ocasionar y las consecuentes pérdidas económicas que les genera, lo que hace que este tipo de conductas se mantenga bajo la llamada cifra oculta o cifra negra quedando en la impunidad y permitiendo que se acrecenté cada día las diferentes infracciones que se cometen desde un sistema informático, dispositivo móvil o cualquier avance tecnológico que requiera de internet para su continuo funcionamiento y pueda acceder a información de bases de datos que al no tener las respectivas formas de seguridad puedan ser manipulados vulnerando la privacidad e información confidencial.

Como citar el capítulo

Medina Ramírez, E., Quintero Bayona, N., Silva Rincón, J., Aguilar-Barreto, C., Hernández Peña, Y. (2018). Falencias en el sistema legislativo en la unificación de las infracciones informáticas en Colombia. En A. Aguilar-Barreto.,V. Bermúdez Pirela., y Y. Hernández Peña. (ed.), *Sociedad y derecho.* (pp. 169-187). Cúcuta, Colombia: Ediciones Universidad Simón Bolívar.

DOI:

Referencias bibliográficas

Aguilar-Barreto, AJ. &Ibañez, E. (2017) Escenarios virtuales: Bases de nuevas formas de comunicación que inciden en la acción educativa. En:Graterol-Rivas, M., Mendoza- Bernal, M., Graterol-Silva, R., Contreras-Velásquez, J., y Espinosa-Castro, J. (Ed.),*Las Tecnologías de Información y Comunicación y La Gestión Empresarial* (pp.175-191). Maracaibo, estado Zulia, República Bolivariana de Venezuela. Publicaciones Universidad del Zulia. Recuperado en: http://bonga.

unisimon.edu.co/bitstream/handle/123456789/2105/TIC%20y%20Gesti%C3%B3n%20E.pdf?sequence=1&isAllowed=y

Aguilar-Barreto, A.J., Mendoza, M., Villamizar, E., Aguilar-Bautista, Y.A. (2018). Propiedad Intelectual y Derechos de Autor: Su protección en Colombia. En Aguilar-Barreto, A.J. & Hernández, Y. (Ed.),*La Investigación Jurídica: Un análisis de la incidencia de los aspectos sociales para el Derecho*. Barranquilla, Colombia: Ediciones Simón Bolívar. Recuperado en: http://bonga.unisimon.edu.co/bitstream/handle/123456789/2289/Lainvestijureconoaccionorm.pdf?sequence=1&isAllowed=y

Alemania. Asociación Internacional de Derecho Penal (1992) Coloquio de Wurzburgo.

Colombia. Ley 1581 de (2012). Disposiciones generales para la protección de datos personales, recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Colombia. Sentencia T-277/15 (2013). Derecho a la intimidad y al debido proceso. Recuperado de: http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm.

Comisión de Regulación de las comunicaciones (2016) Nuevo Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, Respuestas a los comentarios realizados a la propuesta regulatoria, Bogotá. Recuperado en: https://www.crcom.gov.co/recursos_user/2016/Actividades_regulatorias/NuevoRPU/DOCUMENTO_RESPUESTA_COMENTARIOS_FINAL_RPU.pdf

Díaz, Y., Aguilar-Barreto, A.J., Bonilla, J. (2018). Protección a Derechos de Autor desde el Derecho Comparado. En Aguilar-Barreto, A.J. & Hernández, Y. (Ed.), *La Investigación Jurídica: Un análisis de la incidencia de los aspectos sociales para el Derecho*. Barranquilla, Colombia: Ediciones Simón Bolívar. Recuperado en: http://bonga.unisimon.edu.co/bitstream/handle/123456789/2289/Lainvestijureconoaccionorm.pdf?sequence=1&isAllowed=y

Laudon, C. y Guercio, C. (2009), Delitos informáticos y entorno jurídico vigente en Colombia. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3643404 .

Loja Flórez, C. (2013): Universidad Técnica Particular de Loja, tipos de

hackers, Revista de información, tecnología y sociedad No. 18.

Martínez, B. (2006). La filosofía hacking & cracking http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/32 .

Martínez, R. (2006). Hackers blancos y negros, mismo trabajo, distinto objetivo. Recuperado de: http://ntrzacatecas.com/2016/04/24/hackers-blancos-y-negros-mismo-trabajo-distinto-objetivo/

McClure, S., Scambray, J., Kurtz, G. (2000).Hackers: secretos y soluciones para la seguridad de redes.

McLuhan, Marshall; Fiore, Quentin (2009) El medio es el masaje. Un inventario de efectos. Barcelona: Paidós.

Ojeda-Pérez, J., Rincón-Rodríguez, F., Arias-Flórez, M., & Daza-Martínez, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos De Contabilidad*, *11*(28). Recuperado a partir de https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

Pabón, P. (2013). *Manual de Derecho Penal*. Tomo II Ediciones Doctrina y Ley.

Rodríguez, G. (2002). Derecho penal e Internet, y CREMADES, J. Régimen jurídico de Internet, La Ley, Madrid, pág. 261.

Rodríguez, J. (2015), Revista Derecho Penal, año III N° 7, análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación, facultad de derecho, Universidad Javeriana, Bogotá.

El Derecho como disciplina humanística que tiene por objeto el estudio la interpretación, integración y sistematización de un ordenamiento jurídico para su justa aplicación; que atendiendo a este propósito desde el ejercicio investigativo como un campo laboral no explorado, los procesos de investigación formativa que se adelanta en la Universidad Simón Bolívar tienden al análisis teórico, analítico y crítico de distintas situaciones que alteran el orden justo, y por ende la dinámica de la sociedad; así este libro presenta resultados de estudios que permiten comprender la relación entre "Sociedad y Derecho". Cada uno de sus capitulo muestra los resultados desde la reflexión investigativa de un grupo de excelentes profesionales, que apoyando a los abogados en formación y experiencia ofrecen nuevas perspectivas del Derecho, desde su trascendencia frente a las diferentes problemáticas sociales. Así, esta obra se muestra un conjunto de saberes que evidencian intereses comunes e investigativos, los cuales han sido revisados por especialistas en el área, dando origen a los diferentes capítulos, donde se encuentran problemáticas de gran impacto en la actualidad, como lo son cáncer gástrico, migración, derecho ambiental, arreglos de paz, infracciones informáticas en Colombia, derechos fundamentales y laudos de arbitraje internacional.

EDICIONES
UNIVERSIDAD
SIMÓN BOLÍVAR

9 789585 533363