LAS REDES SOCIALES: CAMPO DE OPERACIONES DEL DELINCUENTE ACTUAL

FREDY ELÍAS LÓPEZ SILVA
LINDA VANESSA PLATA SOTO
MARÍA ISABEL BERNAL V.

Resumen:
La conducta delictiva a partir del acceso, la obtención y el uso fraudulento de datos personales encontrados en diferentes plataformas magnéticas como lo son las redes sociales y las cuentas de correo, tal información depositada voluntariamente por el usuario, pero que al mismo tiempo pone en peligro su patrimonio económico. Es esto una problemática que por su trascendencia exponencial y su relativamente nuevo e inexplorado desarrollo normativo lo convierten en un tema sumamente atractivo para nuestros objetivos investigativos. Se dará un breve recuento histórico para proceder con un análisis sociológico y normativo de esta nueva modalidad de conducta criminal relacionada directamente con la relevancia que han adquirido las distintas plataformas sociales en la red y lo fácil que puede resultarles a estos criminales tener acceso a una infinidad de datos personales suministrados por los mismos usuarios de una forma poco precavida, lo cual los convierte en un blanco fácil para estos delincuentes que actúan a través de la web.

Palabras clave:
Delito informático, patrimonio económico, acceso abusivo, sistema informático, redes sociales, Habeas Data, Plataforma Web.

Abstract:
Criminal behavior from accessing, obtaining and fraudulent use of personal data found in different magnetic platforms such as social networks and email accounts, such information voluntarily provided by the user, but at the same time endangers economic heritage. Is this a problem that by its exponential importance and its relatively new and unexplored policy development makes it an extremely attractive subject for our research objectives. It will give a brief history to proceed with a sociological and legal analysis of this new type of criminal conduct directly related to the relevance they have acquired the various social platforms on the network and how easy it may find these criminals have access to an infinity Personal data supplied by users themselves a little cautious manner, which makes them an easy target for these criminals who operate across the web.

Key words:
Computer Crime, abusive access, computer system, Social network, Habeas Data, Web Platform.

INTRODUCCIÓN

Los delitos informáticos son todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hacen uso indebido de cualquier medio informático, con la finalidad de lograr un beneficio propio o ajeno[53]. Es así como se tipifica la conducta punible relacionada con el uso irregular de las nuevas tecnologías, esto no quiere decir que sea una novedad para nuestra sociedad, sino que por el hecho de encontrarse en el proceso de desarrollo y rápido avance, es deber del legislador actualizar la normatividad con el fin de incluir las nuevas conductas delictivas que generan impacto social.

Los sistemas informáticos han adquirido mayor influencia en la vida de las personas, permitiendo facilidad en las formas de tener una vida más social, cómoda y práctica, intentado mantener un punto de información, ordenado de forma ágil y eficiente. De la misma manera a medida que avanza la sociedad en su desarrollo tecnológico, sugiere para la sociedad estar a la alcance de esa tecnología.

Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación. Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos. Es por lo anterior que en la realización de este artículo pretendemos determinar el desarrollo normativo frente a las nuevas modalidades de delitos a través de redes sociales, determinar el fenómeno social en relación a conductas punibles a través de redes sociales, determinar modelo de aplicación de los delitos objeto de investigación en materia de redes sociales, análisis crítico sobre mecanismo y reglas que ha implementado el Estado para proteger a usuarios de redes sociales en delitos contra el patrimonio económico.

La metodología que se implementa en esta investigación consiste en el método inductivo y científico, así mismo se enmarca un parámetro de la investigación que abarca dos factores: el espacio referido a analizar el avance que ha tenido el legislador en las tipificaciones penales, en Colombia. Otro factor es el tiempo en donde se determinan los antecedentes y las medidas preventivas que se han tomado en cuanto a los delitos informáticos, desde el momento en que se inició el uso tecnológico de una forma más eficaz y constante, en Colombia esto data aproximadamente desde el año 2000, aunque el uso del internet ha estado en furor desde los últimos años.

1. HISTORIA DELITO INFORMATICO

El internet es una web (red) global de redes de computadoras enlazadas de modo que pueden compartir información sin importar el lugar, cuando se solicita información por

[53] Ley 1273 de 2009

medio del internet, esta sale de su red de origen a través de una puerta (por así decirlo) y es dirigida de puerta en puerta hasta llegar a la red local que solicita la información. El internet no tiene un control central; es por esto que se convierte en un arma de doble filo al encontrarse a la intemperie y permitir el uso irregular de sujetos con malas intenciones, referente al uso del internet encontraremos sinfines de conductas delictivas, pero aquí nos dedicaremos a la conducta delictiva a través del internet que afecta el patrimonio económico de los usuarios.

Desde la implementación del internet como una herramienta fundamental para facilitar la comunicación y diversas tareas, se han hallado ventajas y desventajas las cuales son determinadas por el uso de este. En las últimas décadas se han reportado avances para la infiltración de datos personas, como ocurrió en el año de 1980 en la ArpaNet (AdvancedResearchProjects Agency Network) del Departamento de Defensa de Estados Unidos, esto llevo que en el año de 1992 se redefiniera el concepto de delito de la cuales adoptaron recomendaciones frente al tema y para culminar vacíos para una política criminal fuerte y amplia. Allí el delito informático es entendido es *"cualquier comportamiento antijurídico no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.*"[54] Un concepto armónico y acorde a los sistemas informáticos de la época.

La expansión del concepto de delitos informáticos acogió su concepto a mediados de los años 90 durante grana apogeo de la revolución digital y a medida que el hombre avanzado en tecnología haciendo que la era digital se acogiera a su manejo de información los delincuentes iban en su proceso de cometer sus actos criminales. Con la creación del grupo G8 se buscó la creación de políticas criminales para combatir el crimen guía por el internet. El grupo "Lyion" diseño el tratado el delito informático del cual a mediados del año 2000 fue expuesto a la opinión pública aunque no fue redefinido un término delito informático como tal.

En la década de los años noventa han sido múltiples los ataques que se han efectuado a los sistemas informáticos, intentado obtener información útil para desarrollar actos delictivos contra la sociedad, esta modalidad delictual avanza en la medida que la tecnología evoluciona.

La información es un elemento útil es la vida de la sociedad, es por eso que cada día las personas, tienden a ser confiables manejando esa información en bases de datos y sistemas operativos. Es por eso que dicha información se debe mantener en bases de datos contra rígidos sistemas de seguridad, pretendiendo reducir el riesgo de que se extraiga de forma indebida y se vulnere los derechos de las personas.

[54] Alemania, 1992, Coloquio celebrado en wurzburgo.

2. LEGISLACIÓN

Con el fin de proteger el patrimonio económico de usuarios que a través de herramientas tecnológicas manejan cuentas bancarias, se han expedidos diversas leyes que sancionan y a la vez protegen los derechos de los usuarios, así como lo es la Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo como antecedentes jurídicos: primero, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener motivo jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.

Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano: "Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones".

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: "Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Es así como los medios de defensa que el estado ha proporcionado a través de un desarrollo normativo para proteger los derechos de los usuarios de las redes sociales, especialmente lo que se refiere a la intimidad y la seguridad, lo que dentro de los cada vez más frecuentes casos, podemos encontrar injurias, calumnias, extorsiones y repetitivos casos de vulneración a la vida íntima de los usuarios por medio de fotos y videos que según los diversos casos conocidos por la justicia pueden ser reales o falsificados pero que en cualquiera de los casos se emplean para violentar la integridad del usuario en su vida familiar, laboral y en general todo su entorno social, claramente atentando contra los derechos que la constitución y la ley penal protegen.

Para darle un desarrollo más específico a este punto, trabajaremos los delitos de forma segmentada.

2.1. Extorsión (seguridad)

Uno de los delitos más graves a ojos de la ley penal en cuanto a su connotación social, siendo esta una perturbación a la tranquilidad, seguridad e integridad de la persona, el estado ha establecido para este delito una pena de prisión considerablemente larga, lo que deja ver la relevancia que para éste tiene.

Con las facilidades que otorgan las redes sociales para proteger, suplantar o falsificar la identidad en algunos casos, encontramos que el abuso a estas ventajas es cada vez más frecuentemente aprovechado por los delincuentes.

Para el caso concreto de la extorsión la justicia se encuentra con una barrera muy fuerte la cual radica en la individualización del victimario, esto sumado a la falta de capacitación con que cuentan los investigadores de la Dijín para poder perseguir a los delincuentes que suplantan o falsifican su identidad en la red, convierte este medio un idóneo puente para el crimen. En estos casos el acervo probatorio debe ser en principio recogido por la misma víctima, lo referente a la identidad del victimario y sus demandas, como así se ha manifestado, no obstante ante la imposibilidad de hacerlo, el usuario, es decir la persona natural puede de igual forma denunciar, con la complicación de que un proceso penal sin la debida individualización del victimario inmediatamente podría considerarse congelado hasta no recaudar dicha información, lo cual deja al ciudadano con la única posibilidad de solicitar protección policial.

‘’*En el caso de People v. Pierre, el Tribunal Supremo de Nueva York confirmó la convicción del acusado por asesinato en segundo grado. La víctima fue asesinada por no acceder a terminar su embarazo. Por medio de prueba testifical se autenticó un mensaje de voz en el celular de la víctima. El testimonio giró alrededor del reconocimiento de la voz del acusado. Además, se presentó en evidencia unos mensajes instantáneos o instant messages que el acusado le envió a la víctima y fueron autenticados a través del testimonio del cómplice quien, aunque no imprimió los mensajes, testificó que el screen name del acusado era el que aparecía en los mensajes. ’’ (Nueva York, 2007)*

Para estos casos se aplica la norma tipificada en el Artículo 244 del código penal colombiano. El desarrollo normativo en este tema no ha avanzado, y se limita a llevar el debate a un ámbito de recolección probatoria principalmente llevado por el usuario afectado.

En cuanto a la intimidad de la persona como usuario de las redes sociales encontramos un desarrollo más entramado y complejo con respecto de las distintas modalidades.

2.2. Injuria

Las redes sociales han facilitado transmitir ideas, fotografías, videos, audios, entre otras cosas a una inmensa cantidad de personas con un solo movimiento del ratón. Esta facilidad ha dado pie a que algunas personas abusen de este medio para vulnerar la privacidad de

otras y para levantar acusaciones deshonrosas en contra de cualquier persona que les plazca casi sin ninguna consecuencia negativa para el victimario.

En este delito, en la internet, como casi en todos los que se encuentran en esta categoría, el aspecto probatorio es tal vez el más espinoso del asunto, actualmente los funcionarios judiciales han sido progresivamente capacitados para tratar el tema de la autenticación electrónica en las redes sociales y mensajes de texto, como es un tema recientemente abordado por la justicia de nuestro país, y al no haber un desarrollo normativo en este aspecto en Colombia –delitos informáticos en redes sociales- se acude al análisis y adhesión de lo que otros países si han adelantado con respecto a esta cada vez más frecuente problemática.

Estos casos del derecho estadounidense se traen a colación en el estudio de las nuevas modalidades de prueba electrónica que se debe implementar en Colombia, máxime cuando son estos medios los más usados actualmente por la sistematización social.

Casos en los que se suben al ciberespacio fotografías de las víctimas en su mayoría en estado de desnudez o realizando actividades privadas, en los casos cuando se usan material autentico o en otros, en los cuales se falsifican y manipulan los documentos audiovisuales para relacionar a una persona con una conducta o actividad deshonrosa son muy frecuentes y son generalmente motivados por malas relaciones, celos, o represarías frente a una decisión de culminar una relación sentimental o laboral por parte de la víctima.

2.3. Intimidad y protección al menor

Otro caso más en medio de esta categoría es el de los menores de edad y el uso que pueden darle estos a las redes sociales, así como las restricciones que deben tenerse en estos casos por lo vulnerables que resultan los usuarios de estas edades ante victimarios que escogen esta población por ser los mismos más vulnerables ante sus tramas y engaños.

Si bien la red social más amplia, es decir Facebook, establece una edad mínima para la creación y administración de perfiles, estas normas son fácilmente violadas por los menores que en su afán de hacer parte del sistema social cibernético, incursionan en estas redes sin tener la madurez necesaria.

Por otra parte tenemos a padres que crean perfiles de sus menores como es el caso que se presenta en la acción de tutela T-260 de 2012 en la cual un padre de familia crea un perfil en la red social Facebook para su hija, según éste con estrictos niveles de seguridad, y con el fin de mantener contacto con ella por ser éste un padre de familia divorciado y no contar con el tiempo suficiente para compartir con ella, dicha acción fue impetrada por la hija de la menor, aduciendo el riesgo que le suponía a la menor tener datos personales y documentación como fotografías que pudieran ponerla en peligro. La corte determinó su fallo a favor de la actora, aduciendo principalmente que hay riesgo en cuanto al desarrollo personal idóneo de la menor, y concuerda con los riesgos que estas redes representan para los menores.

En los casos de las redes sociales la más significativa de las decisiones es la de prevención a la hora de proteger nuestra información personal y en el caso de los menores es imperativo una regulación más estricta.

3. CONCLUSIONES

Al finalizar este estudio llevado a cabo sobre el desarrollo normativo que tiene el estado colombiano, así como sus instrumentos jurídicos para combatir las modalidades criminales en las redes sociales, encontramos que si bien el ente investigador y acusador, como lo es la Fiscalía, ha encontrado formas de combatir a los criminales que se escudan en el anonimato que la red puede llegar a otorgar, no son estas suficientes ni las idóneas para esta tarea, no solamente hablando de herramientas de índole tecnológico o formativo, sino a lo que las normas atañen, y en gran parte a la ausencia de ellas.

Encontramos entendible que por ser una modalidad relativamente nueva, y por ser considerablemente obsoletos las herramientas que puede usar el órgano investigador, aunado con la insuficiente capacitación con respecto a esto, es difícil crearnos una expectativa satisfactoria con respecto de la lucha contra esta modalidad criminal. No obstante no es la única barrera que debe saltar nuestro sistema judicial, el poco desarrollo normativo en este tema es una bola de cañón más para el grillete que lleva ya desde que se disparó este fenómeno tecnológico y se convirtió en una carrera dispar, una carrera que al parecer siempre parece dar más facilidades al delincuente que a las autoridades.

Por ahora, se combatirá esta modalidad con las herramientas que se poseen, esperando que poco a poco, más pronto que tarde, se llegue a una regulación que cumpla con los mínimos parámetros que exige este nuevo mundo de redes y espectros electromagnéticos. Resulta imperativo concientizar a través de campañas (algo que poco a poco se está desarrollando) a los usuarios de las redes sociales para que protejan su información, sobre todo en los casos especiales de menores de edad que por muchos flancos resultan ser los más vulnerables.

BIBLIOGRAFÍA

Rincón Ríos, Jarvey. Delito electrónico en Colombia: (de Proyecto de Rovira a Ley de la República). Ley 1273 de 2009. Cali. Universidad Santiago de Cali. 2009.

Márquez Escobar, Carlos Pablo. El delito informático: conforme con el nuevo código penal: la información y la comunicación en la esfera penal. Bogotá. Leyer. 2002

http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

http://www.certicamara.com/download/eventos/2013/0113_proteccion_de_datos_personales/Presentacion_German_Realpe-curso_proteccion_datos.pdf

http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

Trend Micro (2008). Los 20 virus informáticos más importantes de la historia, sepa cuáles son.http://www.elcomercio.com.pe/ediciononline/HTML/2009-01-22/los-20-virus-informaticos-mas-importantes-historia-sepa-cuales-son.html.

Colombia, Congreso de la República (2000). Ley 599 de 2000, por la cual se expide el Código Penal. Diario Oficial No. 44.097, 24 de julio de 2000. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html.

Colombia, Congreso de la República (2001). Ley 679 de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial No. 44.509, 4 de agosto de 2001. Disponible en:http://www.cntv.org.co/cntv_bop/basedoc/ley/2001/ley_0679_2001.html.

Cisco, Presentación de información diversas fuentes, 2008.http://www.dinero.com/negocios/telecomunicaciones/colombia-tiene-mejorar-seguridad-informatica_50693.aspx.

Presentación blogger, delitos informáticos, Disponible: http://delitosinformaticoslaschecks.blogspot.com/2011/11/historia-de-los-delitos-informaticos.html

Seguridad informática, Blooger, autor SMEC, Disponible: http://seguridad-informatica-smec.blogspot.mx/2012/01/historia-delitos-informaticos.html