¿QUÉ DIFERENCIAS EN CIBERDELITOS EXISTEN ENTRE COLOMBIA Y ESPAÑA?

Presentado por:
JUAN PABLO AYALA MARTINEZ
DANIEL ALEJANDRO DUQUE MARTINEZ

Fecha de entrega:
13 de mayo de 2022

Profesor:
DANIEL GÓMEZ GÓMEZ

UNIVERSIDAD CES

FACULTAD DE DERECHO
DERECHO
MEDELLIN, COLOMBIA
2022

Tabla de Contenido

Resumen

Este trabajo está enfocado en abstraer los elementos principales entre algunos delitos informáticos que se encuentran en común entre España y Colombia. Se centra en analizar conductas diferentes entre ambas legislaciones. Comparara lo que caracteriza los principales delitos que se encuentran en Colombia y España.

PALABRAS CLAVES: CIBERDELITOS, DELITOS INFORMATICOS, CONVENIO DE BUDAPEST

Abstract

This work is focused on abstracting the main elements among some computer crimes that are in common between Spain and Colombia. It focuses on analyzing different behaviors between both legislations. Compare what characterizes the main crimes found in Colombia and Spain.

KEYWORDS: CYBERCRIME, COMPUTER CRIMES, BUDAPEST CONVENTION

Pregunta de investigación

¿Qué diferencias en ciberdelitos existen entre Colombia y España?

Objetivo general

Identificar las diferencias en ciberdelitos existentes entre Colombia y España.

Objetivos específicos

Examinar el convenio de Budapest como norma pionera.

Comparar elementos esenciales en algunos ciberdelitos entre Colombia y España.

Diferenciar elementos esenciales de delitos que solo se encuentran en España como el sexting y el grooming.

Caracterizar elementos esenciales de ciberdelitos propios de Colombia.

Introducción

Desde hace unas décadas en los países avanzados se ha despertado un interés en construir normatividad que regule las conductas desarrolladas desde los medios informáticos, naciendo así un movimiento legislativo que busca tipificar en la mayoría de los países en el mundo conductas conocidas como ciberdelitos, las cuales con el pasar del tiempo crecieron, dejando relegado a los legisladores.

El tratado de Budapest ha sido la norma guía para que los países tomen de base para acogerse o legislar sobre las conductas contenidas en este, para llegar a armonizar los ordenamientos jurídicos.(Acurio, 2016,página 47) “La Convención se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. Es decir, contar a nivel de Latinoamérica con una herramienta común tanto sustantiva como adjetiva para procesar este tipo de manifestaciones delictivas, procurando con este elemento comunitario en la parte sustantiva el mejoramiento de la cooperación internacional de los países miembros, ya que solamente existiría en esta materia, la aplicación de una ley común de carácter supranacional que permita a los gobiernos intercambiar información y pruebas.”

Algunos doctrinantes citan que Colombia ha sido uno de estos países que se han quedado atrás con esta regulación. “La ausencia de tipos penales para castigar los cibercrímenes era generalizada en Colombia (un verdadero paraíso informático) no es posible afirmar que las previsiones delictivas de la ley 1273 de 2009 hayan subsanado los errores previos o hayan completado las posibles lagunas que existen en esta materia)” (Posada, 2017), con esto confirma

que esta ley subsano un vacío existente para ese momento, pero con la constante evolución de la tecnología, el derecho penal queda atrasado y desbordado por unas nuevas conductas, haciendo que con el pasar del tiempo quede atrasada esta actualización.

Además, la gran relevancia en este tema es que la web se ha convertido en una de las formas como los seres humanos cubrimos las necesidades básicas, las cuales son lo mínimo necesario para una persona pueda vivir y por ende necesitan una gran protección por parte del estado, ya que una grave amenaza hacia esta, causaría un grave peligro para el ser humano.

En el siglo XXl las comunicaciones y la información se han convertido un pilar para el crecimiento de la sociedad, haciendo que esta fuera consolidándose con el pasar de los años como valores sociales importantes para la comunidad.

¿Qué diferencias en ciberdelitos existen entre Colombia y España?

Convenio de Budapest

Desde hace mucho tiempo los países europeos vienen en su lucha contra la delincuencia informática, pero debido a que el ciberespacio era un campo para muy pocas personas, no era necesario regularlo, esto se puede evidenciar con el año de nacimiento del primer ordenador, denominado con el nombre Z1, y el cual fue creado en Alemania en los años 1938 (Bejarano, 2018), siendo esta la primera computadora debido a que necesitaba una programación para funcionar; en los años 1940 Alan Turing creo la maquina bombe (La vanguardia, 2018) la cual fue fundamental en la segunda guerra mundial para descifrar el código alemán de comunicación, llamado enigma. Apenas hasta el año 1962 se empezó con la investigación del internet, el cual fue un proyecto desarrollado por el ministerio de defensa de Estados Unidos y dirigido por John Licklider, un científico del instituto tecnológico de Massachusetts y culminando el proyecto en el año 1972. En los años 1992 empezó la expansión del internet con 50 páginas y triplicando esta cifra para los años 1993 con 150 páginas.(Facultat d'Informàtica de Barcelona)

Con todo esto se puede evidenciar que los ordenadores y el internet no es algo nuevo, al contrario su rápida expansión, se debió a que cuando salió de la esfera de los gobiernos al público, se multiplicaron los usuarios, tanto de ordenadores como de internet, haciendo que estas máquinas se repartieran por todo el mundo, trayendo múltiples beneficios como simplificación de procesos o comunicación, pero además de esto también trajo un nuevo campo para la delincuencia, debido a que las personas empezaron a confiar en las máquinas para realizar

muchos procesos, como es el caso de las empresas que iniciaron a guardar la información en discos duros.

Por todo esto, los países avanzados han despertado un interés en construir normatividad que regule las conductas punibles desarrolladas desde los medios informáticos, naciendo así un movimiento legislativo que busca tipificar en la mayoría de los países del mundo conductas conocidas como “ciberdelitos”, las cuales tienen un carácter expansivo, ya que con el crecimiento del ciberespacio y la sobre utilización del internet, estas se volvieron fundamentales para el cumplimiento de las necesidades básicas.

La Unión Europa ha sido promotora en dar importancia a la ciberdelincuencia, ya que creo el convenio de Budapest para regular los cibercrímenes, que es construido para luchar contra la ciberdelincuencia, debido a que entre el año 1992 y 2000 existió un aumento en el uso de ordenadores y de igual manera de comportamientos dentro de estos mismos que vulneraban personas, esto sobrepasando a los estados europeos, por la inexistencia de normatividades o la existencia, pero el poco desarrollo legislativas de estas. Por lo tanto, Regular el surgimiento de nuevas conductas informáticas o la readaptación de las tradicionales cometidas a través del uso de nuevas tecnologías fue la intención de este tratado(Union Europea, 2001), debido a que la Unión Europea hizo un análisis en sus países miembros, detectando falencias en algunos países como España, donde esta antes del convenio no contenía regulación precisa frente a delitos como el acceso ilícito, o lo que sucedía en otros estados, que existía regulación, pero era una regulación muy desactualizada frente a las nuevas tecnologías.

Todas estas nuevas tecnologías han servido para ser el punto de partida para crear nuevos delitos, que pueden ser clasificados en dos, los primeros (como la estafa o el hurto) los que

están dentro de un código penal, pero han ido evolucionando con el tiempo para ser cometidos con nuevas modalidades ; por otro lado, se encuentran otros delitos que se pueden denominar delitos nuevos, ya que son innovaciones de algunos países posterior a un autoanálisis, debido a la transformación de la sociedad con nuevos comportamientos, los cuales deben ser regulados, ya que esas nuevas conductas vulneran valores sociales que necesitan ser sancionados desde el ámbito penal.

En el mismo sentido el tratado de Budapest cumplió objetivos que la Unión Europea planteo. Entre ellos se encuentra la armonización de la normatividad penal en la unión europea y posteriormente con la mayor cantidad de países que suscribieron el tratado, trayendo una nueva actualización normativa en los países que tenían alguna regulación, complementando sus anteriores normas y realizando una armonización normativa entre la mayoría de los países, debido a que este es uno de los delitos transnacionales con mayor dificultad por su posible comisión multinacional.

La Unión Europea(Anguíta, 2018) identificó que la simple adhesión de sus estados miembros no era suficiente, ya que el obstáculo internacional en la comisión de estas conductas interponía la barrera más grande para sancionar este tipo de delitos, para ilustrar un poco mejor nuestra idea se desarrollara el siguiente ejemplo ilustrativo:

Un cibercriminal pretende ingresar al servidor de una universidad para alterar las notas de su amigo que está haciendo un postgrado en una universidad en España , aquel con su alto grado de conocimiento sobre el hacking (persona que a través de un servidor accede ilícitamente a un servidor violentando una medida de seguridad), sabe que puede ingresar desde su casa en la ciudad de La Paz Bolivia, a un servidor que está ubicado en El Salvador y modificar las notas de

su amigo , sin que tenga una consecuencia jurídica, debido a que no existe ni regulación , ni la armonización burocrática entre España, Bolivia y El Salvador .

Se puede evidenciar, la imposibilidad que un país, sin cooperación internacional pueda ganar la batalla contra los delitos informáticos, por el hecho de que el internet es uno solo, y que las conductas cometidas en él, se pueden realizar desde cualquier parte del mundo, por todo esto se empezó un movimiento para que la mayoría de naciones ratificaran este convenio, consiguiendo que 60 de estos lo hicieran y que en la mayoría de estados del mundo legislaran sobre delitos informáticos.

La Unión Europea no se quedó solo con la innovación del convenio de Budapest, sino que también ha tratado de prevenir las nuevas conductas que van a afectar en el futuro, esto lo han hecho expidiendo reglamentos, directivas o protocolos adicionales, Cada vez que se evidencia el nacimiento de una nueva conducta que perjudica la sociedad informática.

El convenio de Budapest en su redacción se subdividió entre los artículos 2 y 6, como las conductas contra “la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos”, como son el acceso ilícito, la interceptación ilícita, ataque a la integridad del sistema, ataque a la integridad de los datos y abuso de los dispositivos. Y los articulo 7 y 8, como conductas informáticas, como son la falsificación y el fraude informáticos, siendo esta clasificación importante para diferenciar sustancialmente la diferencia entre ciber delito y delito informático.

Diferenciación entre ciberdelito y delito informático

Los delitos informáticos son un grupo de conductas genéricas, que adquieren importancia por el surgimiento de nuevas tecnologías, las cuales buscan proteger la información de las personas que se pueden vulnerar a través de un medio digital.

Existe un grupo conocidos como delitos informáticos, que son un conjunto de conductas cometidas a través de la red, pero que su resultado no es aplicado directamente en esta, como es el caso de la estafa o la extorsión a través de medios electrónicos, como, por ejemplo: Una extorsión aplicando el uso de Facebook, el cual el medio utilizado es la red social pero el resultado físico es el constreñimiento de la voluntad de la persona.

Estos delitos se caracterizan porque ponen en peligro algunos bienes jurídicos como el patrimonio, la fe pública, la intimidad personal, la libertad y formación sexual, el honor, los derechos morales y patrimoniales de autor. Además de estos existen algunos los cuales su peligro o lesión se ve reflejado subsidiariamente a la lesión de otro bien jurídico, como lo es la seguridad de la información. Se puede observar el caso del hurto por medios informáticos, el cual se identifica por proteger principalmente el patrimonio económico y subsidiariamente la seguridad de los datos.

Los ciberdelitos o delitos informáticos en sentido estricto se entienden como los delitos que son realizados propiamente dentro de la web como nos deja en claro (Posada, 2017, página 103) “Por el contrario, la doctrina especializada ha dicho que los ciber crímenes (o delitos informáticos en sentido estricto o propio) son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación,

daño, falsificación, interceptación, manipulación previa o posterior, ejecución automática de datos o sistemas informáticos, sin el consentimiento o con abuso de este.

Con todo esto se puede definir un ciberdelito como un delito que es propio a el sistema informático en otras palabras, se debe realizar la conducta dentro de un sistema informático y que afecte directamente al sistema o la información del sistema, al contrario del delito informático, que se utilizan los sistemas como un medio para cometer un tipo de conductas que sin estar directamente interconectadas por la red o un sistema de datos, se pueden realizar conductas punibles con sistemas independientes o dependientes al que se está afectando o utilizando, como es el caso ya mencionado la ciber extorción.

Por esto diferenciar entre ciberdelito y delito informático es de gran relevancia, ya que como se puede observar en la ley 1273 del 2009 (que sirvió para la creación de un nuevo bien jurídico en Colombia llamado, ”de la protección de la información y de los datos”) , ayudo a demostrar que es lo que se quiere proteger, como es el caso de Colombia donde se muestra de forma explícita que del artículo 269A al artículo 269G se protege la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, y el 269I y 269J habla de los atentados informáticos y otras infracciones. Se puede evidenciar que se sanciona dos cosas diferentes, en el primer caso los datos y sistemas informáticos, y en el segundo caso son los atentados informáticos y otras inflaciones, demostrando que del artículo 269A al 269G son ciberdelitos porque son delitos que solo se pueden cometer a través de sistemas informáticos y los artículos 269I y 269J son delitos informáticos ya que utilizan los sistemas informáticos como medios para cometer otras infracciones.

Bien jurídico

El bien jurídico es considerado como el pilar fundamental del sistema penal, desde el principio de su creación no se ha podido identificar con claridad que es el bien jurídico, ha sido uno de los dilemas más grandes de los doctrinantes a la hora de llegar a un consenso general sobre su significado y su origen, esto debido a que es un término que ha evolucionado con el tiempo. Uno de los grandes problemas a la hora de determinar el bien jurídico ha sido su búsqueda dentro del derecho, autores como(Bustos, 1989) Birnbaum contradicen la tesis de ser definido como concepto jurídico y lo ubican más allá del derecho, ya que para el son valores dados por la naturaleza y el desarrollo social, por lo tanto, necesitan su protección por parte del estado.

Por otro lado, Binding respalda la tesis inicial de que el bien jurídico se encuentra dentro de la norma jurídica y es intrínseco a ello, ya que se ve al estado como el garante de los valores de la sociedad y por eso se entendería al mismo como el bien fundamental.

Saliéndose de esta discusión el profesor Fernando Velásquez (VELASQUEZ, 1995) sugiere que el bien jurídico se puede observar desde dos esferas distintas, la primera es desde una visión política criminal y definida como “todo lo que merece ser protegido por el derecho penal” y desde una esfera dogmática como “el objeto efectivamente tutelado por las normas vulneradas en concreto o, como dice la ley, “el interés jurídico tutelado””.

En nuestra opinión el concepto más acertado es el de Birnbaum, debido a que el bien jurídico es un concepto no jurídico, ya que estos valores que se protegen por el estado son construcciones sociales importantes para la comunidad, siendo el grupo de personas las que fundamentan la importancia de este valor y teniendo obligación por parte del estado de proteger

estos valores, debido al contrato social de Roseau, donde el ciudadano transfiere unas libertades a cambio de que el estado brinde unas garantías.

Uno de los bienes jurídicos que el estado debe garantizar su protección es el "de la información y de los datos" que, en el caso colombiano, se creó en el año 2009 por la ley 1273, debido a la necesidad de proteger la información y los datos de las personas que por el auge del internet se aumentó paralelamente las conductas que vulneraban este valor social.

El caso de España es diferente debido a que la mayoría de los delitos se encuentran dentro del bien jurídico de la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, todo esto respaldado por el artículo 18 de la Constitución, donde se garantiza la intimidad personal, el derecho a la propia imagen y la inviolabilidad del domicilio. Afirmándose por este articulo y ratificando el convenio de Budapest, donde existe la libertad legislativa a los congresos para adaptar las figuras jurídicas más pertinentes, analizando que para el caso español según su redacción legislativa lo más acertado fue insertar la mayoría de los ciberdelitos dentro de este bien jurídico. Sumado a esto, el legislador repartió los delitos informáticos donde creía que su inserción era la más adecuada, como es el caso de la ciber extorsión ubicada en el bien jurídico de las defraudaciones o el del grooming el cual se encuentra en los abusos sexuales, demostrando que estos tipos de delitos no son estáticos, ya que el legislador encaja el delito según el bien jurídico que más afecte.

Ahora bien, Tanto el legislador colombiano como el español tomaron el convenio de Budapest de diferentes formas, ya que por una parte el legislador colombiano, adapto todas estas conductas en un bien jurídico independiente, frente al legislador español que adapto cada conducta en el bien jurídico que para ellos mejor se adaptaba.

Delitos comunes entre España y Colombia

Entre Colombia y España existe una relación desde que se realizó la conquista de América, desde ese momento nació una relación de un hijo con un padre, debido a que se a trasferido cultura, religión, creencias y muchas cosas más.

Esto no solo a quedado hay, ya que tenemos una relación muy cercana en la creación de algunos delitos, como son los realizados por medios informáticos.

Acceso abusivo a un sistema informático

Para iniciar con nuestro primer delito se analizará la legislación colombiana y española, comparando en su literalidad las dos conductas descritas en el código respectivo de cada país.

Delito de acceso abusivo a un sistema informático	
Legislación española	Legislación colombiana
Código penal español (Ley orgánica 10 de 1995 modificada Ley orgánica 1/2015), artículo 197bis.1	Código penal colombiano (Ley 599 de 2000, modificado por el art. 1° de la Ley 1273 de 2009, que introdujo el art. 269A)
"El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo,	"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en

será castigado con pena de prisión de seis meses a dos años.”	multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.”

España

El acceso abusivo es uno delito más conocidos debido al termino hacker, que es conocido coloquialmente como el sujeto que es capaz de hacer diferentes actos por medio de internet, siendo una explicación más específica la siguiente(Figueiras,2021, página 3) “hacker tiene un doble significado dentro del campo de la informática. Puede ser un programador informático experto que cree software y hardware complejos. Estos piratas informáticos son expertos en el campo de la informática y han alcanzado un cierto estatus de élite dentro de su campo. El otro significado comúnmente conocido de la palabra es alguien que irrumpe en las redes de seguridad informática para su propio propósito.”

Sujeto activo y pasivo

En el primer caso (español) empezaremos con un sujeto activo indeterminado que, de la misma manera, por un medio indeterminado, vulnere una medida de seguridad, la cual se refiere en superar una barrera que puede ser desde otro ordenador, violentando el código de programación o desde el mismo servidor, pero introduciendo la contraseña correcta para ingresar.

El sujeto pasivo o víctima de la conducta es la persona que es la vulnerada directamente por esta, y es la cual está en cabeza la titularidad del sistema informático, como puede ser el

usuario titular de un sistema informático que un tercero ingresa sin autorización o que se mantenga en el sistema informático en contra de la voluntad del titular.

La palabra sin autorización nos adentra dentro del campo del sujeto, (Barrio, s. f.)la cual se refiere a que, si el usuario que está ingresando al sitio cuenta con el aval de entrar y permanecer en él, siendo el caso de una persona que violente una barrera de seguridad, pero sea un usuario autorizado, no estaría cometiendo la conducta.

Verbo rector

Al hablar de acceder o facilitar se está hablando del verbo rector, el cual nos describe dos conductas diferentes, la primera es acceder a un sistema informático, que consta de ingresar sin importar si se da desde el mismo dispositivo o desde otro. Para (Salvadori, 2011) “la conducta de acceso tiene que ser entendida como la posibilidad por parte del sujeto agente de «utilizar» los datos sin que sea necesario que él se entere de su Contenido”. Por otro lado, facilitar se puede definir como posibilitar o brindar una ayuda a un tercero para que este acceda de una manera más cómoda al sistema.

En tercer lugar, encontramos el ultimo verbo rector que contiene esta conducta: mantenerse el cual se puede identificar que allí no se sanciona directamente el acceso, sino siendo lo penalizado mantenerse dentro de un sistema sin la autorización del propietario de este mismo. Para ejemplificar tal consideración nos remitimos a una de las conductas más conocidas, esta es cuando un empleado tiene ingreso al sistema, pero, entra en un horario diferente o realiza una función distinta a la permitida, siendo lo sancionado la permanencia sin la autorización.

Elementos

Seguidamente al referirse al "conjunto o una parte del sistema"(*Circular 3 del 2017*, 2017) se debe de entender si el usuario a la hora del acceso tiene la disponibilidad del todo el sistema de información o tuvo en su disposición solo una parte, siendo entendido disposición como la posibilidad de decidir sobre el contenido o acceso sobre el sistema, teniendo mucho cuidado con la palabra posibilidad, ya que se sanciona el simple ingreso, pero con una posibilidad de lesionar al legítimo dueño, para ser más claros un ejemplo, donde una persona ingresa a una página que se encuentra totalmente vacía y no se posee una forma desde esta página de quitarle el debido ingreso al propietario, siendo este el claro ejemplo de que un ingreso que no puede ser penalizable, debido a que no se poseía la disponibilidad de la página.

Colombia

En primer lugar el artículo 195 del código penal, contenía el acceso abusivo a un sistema informático hasta el año 2009, momento en que se realizó la reforma al código penal, insertando la nueva ley 1273, que creó el bien jurídico de la información y de los datos, y que sustituyo el bien jurídico protegido del acceso abusivo el cual era "de la violación a la intimidad, reserva e interceptación de comunicaciones", evidenciando que antes de esta nueva ley se comprendía que el bien jurídico protegido en este delito era la intimidad, siendo similar al caso español.

Sujeto activo y sujeto pasivo

El segundo caso por tocar es el colombiano, en el cual al principio se habla de un sujeto activo no calificado, idéntico al caso español. Prosiguiendo con el término "sin autorización o por fuera de lo acordado", en el cual el primero (que ya había sido explicado anteriormente en el

caso español) se debe entender que el usuario que intenta ingresar no tiene el aval del propietario del sistema y el segundo termino el cual se puede evidenciar a simple vista que se trata sobre pasar la confianza permitida del propietario del sistema informático. De la misma manera el sujeto pasivo no es calificado y recae la conducta sobre el dueño del sistema.

Resulta claro que más allá del análisis intrínseco del texto deben existir unos elementos más allá de la literalidad del texto entre ellos se encuentran el concepto de insider y outsider, siendo el primero cuando una persona se encuentra autorizada para ingresar a un sistema informático pero, excede su autorización al ingresar a hacer algo distinto a lo autorizado o en un tiempo diferente al permitido, como puede ser el caso de un técnico de sistemas que se adentra en un ordenador a realizar mantenimiento en un momento el cual no es debido hacer su función. Otro caso, es el de la funcionaria de un banco que accede fuera del horario laboral a mirar los estados de cuenta de los clientes, lo que la simple inspección en las cuentas debe ser juzgado como punible.

El tribunal superior de Medellín en su sala penal mediante la sentencia (STSM 0526/16 del 14 de marzo de 2017), en ella se expone el caso de una empleada de un banco que pertenece a su vez a una banda criminal, se aprovecha de sus funciones en el banco y extrae información de los clientes para luego ser hurtarlos por sus cómplices, aquí el tribunal trae de la doctrina el concepto de insider.

Por otro lado, el articulo 269H, el que se refiere a los agravantes, en su inciso 3 dice “Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este” evidenciando su parecido con la figura del insider en el sentido que

en los dos casos se sobre pasan la confianza del titular de la página y siendo estas dos conductas compatibles ya que el insider es un término doctrinal y jurisprudencial.

Por otro lado, el outsider, es el caso de un ingreso realizado desde el exterior que, violando una medida de seguridad informática, accede deliberadamente a un sistema informático que no es de su propiedad. (Posada, 2013)

Elementos

En este orden, continuando con el análisis del texto nos remitimos a la oración "acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad". Para la primera parte "acceda en todo o en parte a un sistema informático" se puede ver que es igual en ambos países, ya que sus bases provienen del convenio de Budapest. La última parte de la oración "protegido o no con una medida de seguridad" difiere al español, debido a que no exige superar una medida de seguridad para poder cometer la conducta; esto se puede evidenciar, en el caso de una persona que se dirige a un café internet, y se encuentra un computador con el correo electrónico de otra persona abierto, este sujeto inescrupulosamente empieza a ojear la información, demostrando este caso de que no siempre se debe violentar una medida de seguridad.

Hurto por medios informáticos y fraude informático

Delito de hurto por medio informático o ciberestafa	
Legislación española	Legislación colombiana

Código penal español (Ley orgánica 10 de 1995 modificada Ley orgánica 1/2015), artículo 248.	Código penal colombiano (Ley 599 de 2000, modificado por el art. 1° de la Ley 1273 de 2009, que introdujo el art. 269i)
2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.	El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 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, incurrirá en las penas señaladas en el artículo 240 de este Código.

La ciberestafa

España

La ciber estafa es una conducta muy conocida, ya que es muy frecuente en algunos países, entre ellos, España como lo demuestran las cifras del periódico ABC España en su nota al coronel Juan Sotomayor, jefe del Departamento de Delitos telemáticos de la Unidad Central Operativa, donde enuncia la cantidad de delitos que se cometen en este país.

"En los últimos cuatro años, los ciberdelitos han crecido en España un 135%, es decir, han pasado de conocerse 92.716 en 2016 a 218.302, en 2019." (El cibercrimen en España, 2020)

Además de mostrar el gran crecimiento desmesurado en este tipo de delitos, el coronel explica que el 80 % de estas conductas se tratan de estafas informáticas. Por supuesto este crecimiento ha aumentado año tras año de una forma muy escalada, catapultándolo al segundo lugar de los delitos más practicados en España, solo siendo superado por el hurto.(López, 2020)

Para definir este delito, nos remitiremos a (Salvadori, 2011) " …. El «fraude informático», se realiza por parte del que obtiene un acto de disposición patrimonial mediante una conducta de tipo «lógico», es decir, a través de una manipulación informática u otro artificio semejante, que ocupa el lugar del engaño que induce a un tercero a error" siendo esto una forma de la estafa, pero realizada por medios informáticos, y esta última palabra interpretada como si el sistema debido a una programación realice la estafa informática. Según Corcoy Bidasolo (Devia, 2017) "al referirse la estafa cometida por medios informáticos, indica que "se diferencia de la estafa común en que no existe alteridad entre sujeto activo sujeto pasivo del engaño, no hay relación interpersonal entre ambos. Eso es lo que hacía que no pudiese estimarse estafa en los casos de engaño una máquina. Agregan mismo autor, "las estafas comunes cometidas en la red, sino las estafas cometidas con manipulaciones informáticas."

Para ilustrar mejor un ejemplo de que no constituye una estafa informática: un usuario de una de las páginas de subasta de productos de internet compra un celular marca iPhone siendo esta entregada a los 3 días. Al recibir el producto se encuentra que recibe un celular con una manzana dibujada, asemejándose a la marca iPhone. Esto no constituye a una estafa informática debido que no existe manipulación informática sino un engaño de un usuario a otro que se contrataron a través de medios informáticos.

El bien jurídico el cual es protegido por esta conducta, es el patrimonio, el cual se puede definir según la real academia española como el "conjunto de bienes pertenecientes a una persona natural o jurídica, o afectados a un fin, susceptibles de estimación económica" siendo esto el objetivo de protección en la estafa informática, debido a que el sujeto activo en esta conducta actúa con un animus especial, siendo en este caso el lucro. Como estas conductas se debe realizar mediante medios informáticos, se debe de entender que el patrimonio es todo aquello que pueda considerarse con valor cambiario en el mundo físico, como es el caso de las acciones, monedas digitales, dinero o otras que se pueda adquirir el dominio.

Sujeto activo y pasivo

Tanto el sujeto activo como el sujeto pasivo son las personas que concurren en la conducta, uno como agresor y el otro como el agredido, el primero es el que comete la acción atacando y vulnerando el bien jurídico, el cual puede ser cualquier persona y no necesita una calidad especial para realizar la conducta, además de esto esta debe tener el ánimo de conseguir un beneficio patrimonial. El sujeto activo puede ser tanto la persona autorizada para acceder al sistema como terceros no autorizados.

En el caso del agredido, es diferentemente ya que el sujeto pasivo es el la persona titular del derecho patrimonial que es directamente afectado por la conducta, que en algunas ocasiones se ve afectado tanto el titular del derecho, como los bancos, siendo estos responsables algunas veces de pagar el dinero al dueño del patrimonio, pero dejando bien claro que ellos en ninguna ocasión pueden ser considerados sujetos pasivos de la conducta debido a que ellos fungen como guardianes del dinero, no titulares de este, por esto no siempre el que se encuentre afectado por la conducta es el titular del bien jurídico.

Elementos

En la manipulación informática la conducta consiste en modificar los elementos que afectan la programación informática, la cual es definida por (González, 2014) como :

"cualquier acción que suponga una intervención en el sistema informático; alterando, modificando u ocultando los datos que deban ser tratados automáticamente, o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial" se resaltar que la definición se refiere a una conducta que se comete frente a un sistema y esto debido a que, como se mencionó con anterioridad, el ordenador es el que debe de manipular a la víctima, haciendo que la labor del sujeto activo sea manipular el sistema para que este induzca al error a las víctimas. Al hablar de artificio semejante el legislador español se refiere a este término como una artimaña, enredo, o truco debido que fue creado para los supuestos donde se pudiera defraudar a una maquina como es el caso de un cajero automático, donde se puede evidenciar que el engaño la produce el sujeto activo frete a la maquina y no a otra persona.

Pero el Tribunal Superior de España específico que:

"El Código penal de 1995 introdujo el párrafo 2º del art. 248 del Código penal una modalidad específica de estafa para tipificar los actos de acechanza a patrimonios ajenos realizados mediante la realización de manipulaciones y artificios que no se dirigen a otros, sino a máquinas en cuya virtud ésta, a consecuencia de una conducta artera, actúa en su automatismo en perjuicio de tercero. Estos supuestos no cabían en la anterior comprensión de la estafa pues el autor no engañaba a otro, sino a una máquina. En el supuesto enjuiciado, la utilización de una tarjeta de crédito aparentando ser su titular no podía ser integrado en el concepto clásico de la

estafa en cuanto el "engaño" era realizado a la máquina que automáticamente efectuaba la disposición patrimonial. El engaño siempre presupone una relación personal que no es posible extenderlo a una máquina.” (STS, 603/2000 del 20 de noviembre de 2001, FJ2.)

Con esta sita y el texto anterior se puede llegar a una confusión debido a que si no se puede engañar una maquina por que el legislador ha creado la figura del “artificio necesario”, pero la respuesta es lógica, debido a que cuando se lleva a un error al sistema, que se hace mediante la utilización de elementos que suplantan al usuario real, no se engaña al sistema, sino que evade las medidas de seguridad del creador del sistema para suplantar un usuario real.

El ánimo de lucro es un elemento el cual el sujeto realiza la conducta con la intención de obtener un veneficio económico de su actuar, haciendo que este tenga relación directa con el patrimonio, debido a que el sujeto activo actúa con la intención de sustraer un bien mueble de la red, el cual contiene un valor cambiario, que es lo que mueve el actuar para agredir.

Hurto por medios informáticos

Colombia

El hurto por medios informáticos en Colombia, lo trajo la ley 1273 del 2009, está inspirada por el artículo 8 del convenio de Budapest, denominado como fraude informático, debido que para esta entidad lo que se debería proteger son las defraudaciones, diferente al caso colombiano, la ley ya mencionada en el artículo 269I se le nombro hurto por medios informáticos, debido a que la norma remite al artículo 239 del hurto, haciendo que los elementos de estese trasfieran al que se realice mediante medios informáticos. Esto lo menciono la corte suprema de justicia en su

sentencia 1245/2015 que trata de un hurto informático a través de clonación de tarjetas de crédito.

"Ciertamente, aunque el legislador fue consciente de la dificultad que comportaba la ubicación del bien jurídico protegido respecto de aquellas acciones antijurídicas reguladas dentro del mentado título, que de manera directa afectaban el patrimonio económico, prefirió atar, de manera antitécnica, como lo aseveró el representante de la Fiscalía, la modalidad de la acción típica prohibida –que es el hurto por medios informáticos- al bien jurídico amparado en el referido título VII bis, que adicionar o modificar las circunstancias modales calificantes del artículo 240 del Código Penal, como hubiera sido lo ideal." (SCSJ, 1245/2015 del 11 de febrero de 2015.)

Aunque lo más conveniente hubiera sido cumplir los lineamientos dados en el convenio de Budapest, debido a que del continente americano solamente Venezuela y Colombia ratificaron la figura como hurto informático(gonzalez, 2017), los demás países como estafa o defraudación, siendo evidente que es una nueva interpretación legislativa a la recomendación del convenio, debido que cada país debe legislar según la necesidad que exista.

Para definir el hurto por medios informáticos nos deberemos redirigir al hurto, que es el apoderamiento cosa mueble ajena, buscando un beneficio económico para si o para otro, dejando esto como base para entender que cuando se lleve este por medios informáticos, se debe de llevar primeramente de manera informática y segundo que, violentando una medida de seguridad.

Con esto se puede concluir que el hurto por medios informáticos es el apoderamiento de cosa mueble ajena a través de medios informáticos, violentando una barrera de seguridad para conseguir un beneficioso económico para si o para otro.

Sujeto activo y pasivo

En este delito no se requiere un sujeto activo calificado, en otras palabras, cualquier persona puede realizar esta conducta ya sea por sí misma o utilizando un tercero como instrumento, dejando en claro que el sujeto activo siempre debe de tener un ánimo de lucro de apoderarse de un bien mueble mediante un sistema informático.

De la misma manera del sujeto activo, el sujeto pasivo tampoco requiere una calificación especial para ser la victima de la conducta, pero el único requisito que este debe de cumplir es que el bien mueble se le sustraiga de su propiedad.

Elementos

La cosa mueble ajena es el objeto en que recae la conducta, ya que este es un delito informático en sentido amplio y esto hace que los sistemas informáticos no sean el objeto directo de protección, al contrario son el medio por el cual la conducta se realiza, vulnerando conductas diferentes, como en este caso, el cual es el patrimonio como lo menciona el tribunal superior de Medellín con la sita del 27 de abril del 2017 la cual trata de un hurto calificado y su diferencia con el hurto por medios informáticos

“si bien el delito se ubica dentro del título que protege la información y los datos, el bien material del delito no puede ser otro que la cosa mueble ajena que sufre un apoderamiento por parte de un extraño. Los datos, la información y su contenido solo son manipulados con el fin de obtener un provecho económico por medio de la sustracción irregular de la cosa mueble ajena que se condensa en el dinero” STSM, 2014-22638/2015 del 27 de abril de 2017.

Con esto se puede identificar que el objeto en el cual recae la conducta es la cosa mueble ajena, haciendo que cuando el sujeto activo sustraiga de la esfera de protección el objeto movible y trasportable se comete esta conducta. Es de aclarar que estamos hablando de delitos informáticos donde se debe de comprender que esta cosa mueble ajena debe ser un objeto que se pueda apoderarse a través de la red y que esta debe contener un valor cambiario, debido a que el sujeto activo debe actuar con un ánimo de lucro.

Verbo rector

Para empezar con el verbo rector, debemos de aclarar que este es de reenvió, debido que hace una remisión al artículo 239 del código penal que se refiere al hurto, y que tiene el verbo rector que habla del apoderamiento,(gonzalez, 2017) en otras palabras, adquirir la propiedad de un bien mueble de maneras ilícitas mediante la utilización de sistemas informáticos. (gonzalez, 2017)

objeto

La superación de una medida de seguridad informática es atravesar el impedimento interpuesto por el usuario dueño del sistema para que no puedan ingresar, estos delitos se pueden llevar acabo de dos maneras distintas, suplantando un usuario o superando una medida de seguridad

La primera es la suplantación de un usuario, que consiste en la superación de una barrera de seguridad, haciéndose pasar por el titular de la cuenta. Para llegar a esto se exige la concurrencia de dos conductas, (Suarez, 2019) la primera ”la suplantación de usuarios ante los

sistemas de autentificación y de autorización establecidos y 2) el apoderamiento de cosa mueble ajena”

El cual el primero se divide en dos, los sistemas de autentificación son los que corroboran que la persona que este ingresando cumpla los requisitos establecidos para ingresar a este, como lo es ingresar una contraseña y un usuario. La autorización es la aprobación del sistema del cumplimiento de aquel control. Y el apoderamiento de cosa mueble ajena es como se mencionó anteriormente, la adquisición ilegal de la propiedad de una cosa mueble.

La superación de una medida de seguridad informática, se refiere mediante una manipulación de un sistema informático, traspase su barrera de protección, el cual se puede llevar cumpliendo 3 pasos(Suarez, 2019), ” 1) la superación de medidas de seguridad informática 2) la manipulación de un sistema informático, una red de sistema electrónico, telemático o u otro semejante y 3) el apoderamiento de la cosa mueble ajena”.

La primera se refiere sobre pasar la barrera de seguridad que puede ser contraseñas, huellas digitales, claves de vos, análisis de iris o cualquier otra forma de identificarse como titular.

La segunda se entiende como la alteración no autorizada de sistemas o datos. La tercera como ya la mencionamos en párrafo anterior no la volveremos a discutir

Se puede apreciar la gran diferencia entre estas dos, cuando se analiza que en una existe la alteración no autorizada de sistema o de datos y en otra solo es superar la barrera y el apoderamiento.

Por su relación con el hurto tiene que existir un provecho económico que puede ser para si o para otro como lo dice la sentencia de la corte suprema de justicia que habla sobre un hurto por medios informáticos llevado a través del cambio de tarjetas de crédito.

"también el ingrediente especial subjetivo necesario para su comisión, como lo es, el animas lucrandi o la finalidad o propósito doloso de obtener un provecho o utilidad - propio o en favor de un tercero- de carácter patrimonial." (SCSJ, 14302/2016 del 5 de octubre de 2016.)

Tipos penales españoles, que no se encuentran tipificados en la legislación colombiana

Tanto España como en Colombia coinciden algunas figuras, como es el caso del acceso ilícito o el hurto por medios informáticos, ya previamente mencionados. Pero además existen otras que solo se encuentran en la legislación española, como es el sexting y el grooming. Siendo un punto para determinar, si existe la necesidad de agregar estos delitos al ordenamiento jurídico colombiano debido al crecimiento de estas nuevas conductas. Por todo esto se debe analizar en estos capítulos que es y que se entiende en España, cuáles son los elementos y cuáles son sus diferencias entre sexting y grooming y la importancia que estos pueden llegar a tener.

Grooming

El grooming es uno de los delitos contenidos en el código penal español y el cual es legislado en el artículo 183TER del código penal español y agregado por la ley orgánica 1/2015.

Empezaremos explicando el grooming en España, que consiste en contactar a un menor de 16 años a través de sistemas informáticos con el fin de cometer una de las conductas

descritas por los artículos 183 y 189, este contacto debe de estar relacionado con actos encaminados al acercamiento, envió de pornografía o mostrar imágenes pornográficas.

Por consiguiente, los delitos contenidos en el artículo 183 se refieren a conductas sexuales con menores de 16 años, y los del 189 regulan los relacionados con la pornografía infantil.

El Instituto Nacional de Tecnologías de la Comunicación de España (INTECO)(Cuenca, 2014) define el grooming como “las acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor”.

Sujeto activo y sujeto pasivo

Lo primero que hay que decir es que este delito (Palazzi, 2016)no exige un sujeto activo calificado,, haciendo alusión a que no necesita ser alguien en especial, pero siendo necesario que el autor actúe mediante cualquier tecnología de la comunicación e información, siendo estos los medios por los cuales se realiza la conducta.

En el sujeto pasivo se requiere que sea calificado, debido que la victima de esta conducta tiene que ser un menor de 16 años, el cual debe tener la capacidad para manejar un artefacto electrónico y poderse comunicar a través de él o por medio de una red social como titular de esta.

Verbo rector

Uno de los elementos más importantes en este artículo es el concepto “contactar”, ya que este se puede entender como dirigirse o establecer una comunicación con un menor de edad.

Pero aclarando que no se debe de sancionar el simple contacto, sino que el menor conteste el mensaje. Como lo explica (Cuenca, 2014,pag 36) "… se requiere un contacto con un menor de trece años a través de una TIC. Parte de la doctrina se inclina por entender que no es suficiente con que haya un intento de contacto, sino que además es necesario que el menor conteste a esta petición de contacto, aunque también hay autores que entienden que es suficiente con que haya conocimiento por parte del menor".

El simple contacto no es sancionado debido a que se debe cumplir otros elementos, como(Ministerio de Justicia, 2015) los requisitos mencionados acerca de que la conducta sea dirigida a cometer delitos contenidos en los artículos 183 y 189 y que se busque concertar un encuentro.

Elementos

En el concertar un encuentro existen muchos puntos a desarrollar. El primero es que se deben hacer actos materiales encaminados al acercamiento, siendo esto que(Díaz, 2011) el sujeto activo realice ciertas acciones para materializar el encuentro con el menor, como lo pueden ser mensajes, llamadas, videollamadas, obsequios, cartas y otras.

Otro punto por expandir es si existe la necesidad de que el menor acepte el encuentro, el cual no debería ser necesario para la consumación del acto, debido a que el simple contacto encaminado a concertar un encuentro con la intención de cometer una de las conductas de los artículos anteriormente mencionados, debe ser considerado como punible ya que los dos requisitos no se refieren a un efectivo encuentro o una comisión de los delitos mencionados. Se puede evidenciar mejor con un ejemplo: un niño con 10 años se dispone a revisar su bandeja de mensajes de la red social de Facebook, donde encuentra un mensaje de una niña de su edad ofreciéndole un encuentro, al cual debería de asistir solo a un lugar solitario, viendo este

que el mensaje no era común, decide ignorarlo. Se puede evidenciar que aunque el menor no responde el mensaje, se están cumpliendo los elementos del tipo, debido a que se propone una invitación a concretar un encuentro y con intención de cometer uno de los delitos mencionados.

Sumado a esto, en su apartado final el artículo se refiere a las medidas de mayor punibilidad en la conducta, cuando esta se realice con coacción, intimidación o engaño. La primera consiste en que el sujeto activo utilizando la fuerza, se imponga con violencia física o psíquica sobre la víctima, siendo esta solo de manera psíquica debido a que la imposición de obligatoriedad del encuentro solo se puede llevar a través de sistemas informáticos. La intimidación consiste en que el sujeto activo ejerza una fuerza moral sobre el sujeto pasivo, haciendo que este acceda a aceptar el encuentro. Y el engaño consiste en tergiversar la realidad para llevar a la víctima al encuentro mediante artimañas, el ejemplo más claro es cuando un menor de edad accede a un encuentro con una persona que dice tener su edad, pero realmente resulta ser una persona mayor y con una intención diferente por la que se pactó el encuentro.

Segundo inciso del grooming

Continuando con el estudio del inciso segundo de este artículo, el cual fue agregado por la Ley orgánica número 1/2015 como una nueva parte del grooming, ya que lo que sanciona es el contacto con un menor de edad, pero en este caso no debe ser dirigida a realizar las conductas de los artículos 183 y 189, ni hacer actos dirigidos a realizar un encuentro, por el contrario lo que sanciona es buscar embaucar a un menor para que este envié material pornográfico o imágenes en las que aparezca o se represente un menor . Esta conducta es tipificada como grooming, con elementos del sexting (que será desarrollado más adelante), debido a la exigencia de realizar actos que conllevan a embaucar, para que la víctima facilite

videos o imágenes pornográficas en las que se represente o aparezca un menor, demostrando que esta conducta sanciona el envío de este material.

Sexting

La figura del sexting tiene diferencias con el grooming entre ellas el bien jurídico, debido a que en el sexting se protege “la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”; Siendo muy diferente al grooming, en el sentido de que protege directamente a los menores de edad y no a todas las personas.

Autores como (PALOP, 2017) define el sexting como “envío a través de internet por ordenador, móvil, Tablet o cualquier otro dispositivo conectado a la red mediante grabaciones o imágenes íntimas obtenidas con el consentimiento del emisor”.

También se puede definir como la falta de confidencialidad difundiendo, revelando o cediendo imágenes o grabaciones sin la pertinente autorización del afectado a través de medios informáticos menoscabando la intimidad de la víctima, siendo preferentemente videos, imágenes o fotografías de carácter privado.

Sujeto activo y pasivo

El elemento del sujeto activo trata de la persona que realiza la conducta, donde el propio delito describe si se exige un carácter o denominación especial, o, por el contrario, cualquier persona puede realizar la conducta. Como es este caso en el que cualquier persona puede cometer el delito; sin embargo, esta conducta es diferente,(Diaz, 2017) ya que una de las exigencias es que el contenido privado provenga de la víctima o haya dado su autorización a la hora de gravar o fotografiar, haciendo que si el contenido no se obtiene con la debida autorización de la víctima, no se podría encajar como sujeto activo de la conducta, y por el

contrario estaría violentando un delito diferente porque podría ser un acceso ilícito, debido a la forma de conseguir la información.

Ahora bien, el sujeto pasivo o víctima es la persona que envió o autorizó (fotografías o videos) a un tercero. (Fernandez, s. f.)Aquí lo más importante es que la víctima puede ser cualquier persona, debido a que el ámbito de protección del bien jurídico es la intimidad, la cual cubre tanto adultos como niños.

Verbo rector

Para empezar a abordar este artículo, iniciaremos con los verbos rectores los cuales son: difundir, revelar o ceder. Ceder puede ser definida como la transferencia a un tercero de una imagen o videograbación que debe de contener un elemento que violente la privacidad de la víctima; una de las características de ceder es que se puede interpretar que la víctima le envió la foto en primera instancia y este se encargó de renviarla a otro. En la palabra revelar se puede interpretar que debe existir algo secreto u oculto que no debe salir a la luz, pero en esta ocasión el sujeto activo hace caso omiso a su prohibición y deslumbra el secreto a un tercero, pero en este caso contrario al anterior, la víctima no envía el material gráfico o fílmico, sino que el victimario participa en la grabación o realización del video o imagen, siendo este el que posee las imagines, porque este fue el que las capto con el consentimiento de la víctima. Finalmente, la palabra difundir consiste en el envío del material de una forma masiva a la mayor cantidad de personas posibles de maneras diferentes, a través de redes sociales, páginas web o mensajes masivos. Esta conducta es diferente a las anteriormente mencionadas debido a que esta exige un carácter de masificación de la

información, al contrario de las anteriormente descritas que se pueden entregar solo a un tercero.

Elementos

Continuando con el análisis, la frase “obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros”, en la que (Navarro, 2020,pag 23)se refiere a la obtención con anuencia: “En conclusión, la interpretación correcta será la de considerar incluido en el tipo penal tanto el material captado y elaborado directamente por el autor con el consentimiento de la víctima, como el elaborado exclusivamente por la víctima y enviado con posterioridad al sujeto activo. Ya que, se debe interpretar que la obtención de las imágenes o vídeo puede ser llevada a cabo directamente por el autor, u obtenerla posteriormente el autor de la víctima cuando sea ésta quien se lo proporcione.”

La palabra anuencia(Ministerio de Justicia, 2015) quiere decir con el consentimiento de la víctima. Frente a la parte del texto que dice “en un domicilio”, se puede evidenciar que se refiere a una vivienda o lugar de carácter privado. La expresión “cualquier otro lugar fuera de alcance de terceros”, habla de un sitio publico donde no todas las personas pueden ingresar como es el caso de un baño o un vestidor.

En la última parte de este artículo se habla del requisito de menoscabar la intimidad, el cual se entiende que debe ser una violación grave a la privacidad, siendo el término intimidad muy amplio debido que se puede entender como todo lo que guardemos para nosotros o nuestro núcleo cercano como confidencial, siendo esto no solo conductas sexuales, sino también pensamientos políticos, cultos religiosos, fetiches, etc.… cabe mencionar que este delito se ubica dentro del bien jurídico de la intimidad porque no solamente pretende proteger la sexualidad.

Asimismo, como en el grooming, este delito tiene una medida de mayor punibilidad, cuando la conducta se produce de una de estas formas: por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa. Con esto se puede evidenciar, que la conducta se puede considerar más grave si es cometida contra un menor de edad o de una persona con discapacidad, también en los casos en que la pareja sea el sujeto activo del delito o en que la persona comete la conducta con finalidad de generar ingresos financieros.

Delitos no contenidos en España

A diferencia de España, Colombia ha calificado como conducta punible en la ley 1273 del 2009, el delito de suplantación de sitio web para capturar datos personales, el cual no se puede encontrar en España.

Esto es debido que para España este delito se encuentra contenido dentro de la estafa por medios informáticos, ya que se comprende que se utiliza manipulación informática o un artificio semejante.

Suplantación de sitio web para capturar datos personales

Colombia al igual que con demás delitos informáticos ha tenido un aumento exponencial de la conducta de suplantación de sitio web para capturar datos personales, siendo esto mencionado por el periódico el tiempo (Tecnóesfera, 2021) “La suplantación de sitios web se convirtió en el 2020 en el ciberdelito con mayor crecimiento en el país, con más de 303 por

ciento más casos que en el año anterior" convirtiéndose en una de las prácticas delictivas informáticas con mayor crecimiento.

Para comenzar con el análisis de este tipo penal hay que adentrarnos primeramente en la estructura de este delito, ya que es un delito poco desarrollado por legislaciones extranjeras, debido a que estas tienen en su ordenamiento jurídico el delito de estafa por medios informáticos, como es el caso de España, el cual menciona en su artículo 248.2 que para cometer esta conducta se debe de realizar mediante una manipulación informática o artificio semejante, que para la doctrina española esto cubre tanto el phishing o pharming como lo explica (Rico, 2012) "Desde la óptica del derecho penal español, las conductas constitutivas de phishing y pharming se encuadran en el delito previsto en el artículo 248.2 del CP, donde se tipifica la estafa informática."

Para explicar que es phishing nos remitiremos a (Rodríguez, 2015, página 1): "El término phishing proviene de la unión de los siguientes vocablos en inglés password, harvesting y fishing, con lo que se viene a hacer alusión a "cosecha y pesca de contraseñas". A la persona que pone en práctica este delito se le conoce como phisher……. este delito data de la década de los noventa, y su operativa se centraba en el envío masivo de correos electrónicos fraudulentos a los clientes de entidades financieras …. con la finalidad de obtener de éstos los datos y las claves de usuario que les permitirán acceder fraudulentamente a la cuenta de la víctima"

Siendo este un término adecuado para saber que es el phishing e identificar a su hermano el pharming, el cual tiene verdadera importancia para este tema, debido a que es el inciso 2 de la suplantación por sitio web y es definido como (Gudin, 2018)"la explotación de una

vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otro ordenador diferente". O dicho con otras palabras esto es confundir a un usuario simulando una página real, la cual debe de tener una reputación, debido a que las personas creen que ingresaran al verdadero servidor, pero en realidad es una página web fraudulenta.

Por todo esto mencionado hay que preguntarse si el pharming en Colombia es considerado un hurto por medios informáticos, debido a sus similitudes con la estafa en España, pero esto no es así, ya que en Colombia se decidió que era más pertinente tener un delito independiente, como los es la suplantación de sitio web para la captura de datos personales, ya que en este delito se encuentran más de una conducta.

Verbo rector

Para iniciar con el estudio especifico de este delito se debe de analizar primero la conducta, debido a que la diferencia más grande se puede advertir en la comparación de los verbos rectores descritos en el párrafo 1 y 2, en la que el primero se refiere a diseñar, desarrollar, traficar, vender, ejecutar, programar o enviar unos elementos determinados, los cuales trataremos con posterioridad en el objeto.

La primera conducta es diseñar, la cual es definida por (Suarez, 2019, página 53) como "hacer el diseño o proyecto de la página electrónica, el enlace o la ventana emergente, con el propósito de ser enviada por el mismo sujeto o por otro a los usuarios, a fin de invitarlos a conectarse utilizando el denominado vinculo de hipertexto para que realicen actividades orientadas a obtener la información codiciada."

La palabra desarrollar tiene similitudes con la ya descrita, por lo tanto nos basaremos en el mismo autor para definir esta (Suarez, 2019, página 53), como " …llevar a la practica la creación de los elementos que constituyen el objeto material del delito, para que se dé el envío de estos y la emisión de información o datos informáticos por parte de los usuarios inducidos a error"

Estas dos primeras se diferencian en que la primera es la planificación y la segunda una manera de llevar a la practica el diseño.

Con el verbo traficar se puede evidenciar que tiene una connotación comercial, debido a que se debe de entender cómo el poner en el comercio una página web en mercados ilícitos.

Por su parte, el verbo vender está relacionado con la transferencia patrimonial de la propiedad de una página a otro por un precio antes convenido .

El verbo ejecutar es definido por (Posada, 2017, página 314) como "poner en funcionamiento una página web, un enlace o una ventana emergente. También se usa para expresar el conjunto de ordenes informáticas dirigidas a la puesta en ejecución de programas de ordenador dentro de un sistema informático o red informática, que busca la realización de determinadas tareas o la realización de procedimientos específicos para el tratamiento de datos personales"

Con el verbo Programar se debe entender como codificar un determinado ordenador para que realice una función específica en un instante determinado.

Para finalizar estas definiciones, enviar se puede definir como transferir una página web, una ventana emergente o un enlace por un medio que tenga comunicación con otros usuarios.

Como se puede observar el legislador pensó en darle orden a cada verbo según los actos previstos desde su creación hasta la parte final de la conducta que sería el envío.

En el párrafo 2 se refiere a un verbo rector diferente, el cual es modificar un elemento especifico, como cambiar el dominio o IP de la página original para intentar llevar al error al usuario como lo explica (Suarez, 2019, página 54) ” La conducta se rige por el verbo modificar, que aplicado al caso significa trasformar o cambiar el sistema de nomenclatura jerárquica de computadores, servicios o recursos conectados a internet o una red privada, el cual tiene como función principal localizar y direccionar los equipos conectados a la red en el mundo” todo esto con la finalidad que el usuario ingrese a un dominio diferente creyendo que es el original.

Sujeto activo y sujeto pasivo

Continuando con la subdivisión presentada en los párrafos anteriores, el sujeto activo del inciso primero es un sujeto activo no calificado, debido a que cualquier persona puede realizar la conducta, pero la complicidad en esta es imposible de imputar, ya que los verbos rectores describen una a una las conductas realizadas, por lo tanto cualquier tipo de colaboración, se estaría cometiendo la conducta con coautoría, debido a que existe una distribución de trabajo criminal con una misma importancia de aporte.

En el segundo verbo, el cual es modificar, es igual que en los anteriores descritos en el punto de que no exigen un sujeto activo calificado, pero con referencia a la complicidad perfectamente se podría aplicar en este inciso, porque la descripción típica solo habla de solo un verbo.

El sujeto pasivo de esta conducta al igual que el anterior se tiene que dividir, debido a los dos incisos diferentes, el primer sujeto pasivo es la sociedad, así que se está vulnerando a todos con solo cumplir con un verbo rector, además de esto en algunos casos se estarían violentando los derechos morales y patrimoniales de autor, dado que las páginas webs, los enlaces o las ventanas emergentes sean imitaciones de las ya existentes.

En el segundo inciso que se describe la clonación de IP, existen dos sujetos pasivos de la conducta, ya que tanto la persona que es engañada para revelar sus datos personales, como el propietario de la página clonada que le están vulnerados sus derechos morales y patrimoniales de autor, son las víctimas de esta conducta.

objeto

El primer objeto a analizar es el del inciso primero, el cual se refiere a páginas electrónicas, enlaces o ventanas emergentes que son los objetos que protegen las conductas, siendo definido el primero como (Posada, 2017) " documentos con capacidad de contener información electrónica de texto, voz, video o imágenes, que puede ser accedida mediante un software de navegación."

Enlaces se refiere a una conexión existente entre una página y una dirección de hipertexto, haciendo que la persona que posee esta dirección pueda ingresar directamente a una página web solo oprimiendo este enlace.

Ventana emergente se puede definir como (Suarez, 2019, página 55) "una ventana del navegador de internet que aparece de manera automática en la panta del computador, sin ser solicitada, y que usualmente tiene como finalidad desplegar publicidad, dirigir tráfico de internet a ciertas páginas, recopilar direcciones de correo electrónico, etc."

Evidenciándose que los objetos protegidos en esta conducta son virtuales y relacionados directamente con el ciberespacio o el internet, puesto que son elementos que están hechos para la diversificación a todo público y por esto se debe de proteger desde su creación hasta la finalización del proceso criminal.

En el segundo inciso es un objeto indeterminado, debido a que puede ser tanto una IP (internet protocol), como los datos y códigos personales de las personas que ingresan sus datos en las páginas simuladas. Todo esto se debe a que las IP son un código numérico único de cada ordenador, que es simulado por otro, haciendo un código IP idéntico, vulnerado directamente al titular de la página.

Conclusiones

El convenio de Budapest es la base de los ciberdelitos y delitos informáticos en gran parte del mundo, pero como se evidencio en el texto su gran acogida en muchos países, no significa que todos o la mayoría lo hayan hecho, siendo esto un gran problema para los países que lo suscribieron, puesto que el problema de la transnacionalidad delictual no se ha superado, haciendo vulnerables a todos los países del mundo frente a estos delitos, y más que esto, la cifra de impunidad ha aumentado, ya que existen países que son paraísos para esta clase de delincuentes.

Otro punto complicado sobre este convenio es la desactualización normativa de muchos países que suscribieron este tratado, debido a que después de muchos años desde su creación han sido ratificado en sus ordenamientos jurídicos, reflejando un atraso normativo frente los nuevos peligros representados en las nuevas tecnologías, debido al gran crecimiento que han tenido los sistemas informáticos y la aparición de nuevas conductas.

El acceso ilícito tanto en España como Colombia son muy similares debido a que vienen de una fuente común, pero con una redacción legislativa diferente entre Colombia y España. Esto hace que esta cercanía creada por su origen desaparezca debido a que en Colombia se entiende que este delito protege el bien jurídico de la información y los datos, frente a el caso español, el cual protege la intimidad, derecho a la propia imagen y la inviolabilidad del domicilio. Siendo lo más acertado entenderlo como lo hacen en España, considerando que el eje central de los datos y la información es la privacidad; en Colombia este bien jurídico existe en el código penal con el

nombre de violación a la intimidad, reserva e interceptación de comunicaciones, y el cual contenía anteriormente el delito de acceso abusivo a sistema informático que estaba contenido en el artículo 195 y el cual fue desplazado al de la información y los datos por la ley 1273 del 2009. Esto demuestra que este cambio o la creación del bien jurídico de la información y los datos es mero capricho del legislador, puesto que todos los delitos contenidos en este se podían ubicar en bienes jurídicos ya existentes.

Similar a este caso, el bien jurídico de hurto por medios informáticos y la ciberestafa están ubicados en bienes jurídicos diferentes, ya que a que en España se encuentra en el patrimonio y el orden socioeconómico, por ende se entiende que esta conducta es una de las modalidades de la estafa, y por eso se debe de comprender que la verdadera vulneración en estos casos no es la información y los datos, sino el patrimonio, contrario al caso colombiano donde se considera que la verdadera vulneración en estos delitos es la información y los datos, siendo algo que ya se ha demostrado que el hurto por medios informáticos exige el ánimo de lucro como elemento esencial para realizar la conducta, y además de esto el delito depende directamente del tipo penal de hurto, ello se debe a que el tipo penal de hurto por medios informáticos reenvía al hurto para sustraer sus elementos. Y no solo esto, existe dos conductas muy similares la cual es el hurto por medios informáticos y el hurto calificado en su inciso 4, el cual habla de “Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes” siendo muy similares, tanto que los fiscales pueden escoger cuál de las dos conductas aplicar, esto es redundancia legislativa, la cual no debería de existir.

Ahora frente la diferencia entre porque España tiene un delito de estafa y Colombia el hurto, se debe remitirse al convenio de Budapest donde se habla del fraude informático, siendo

este muy similar al caso de España y el mundo, donde acoge el nombre de ciberestafa o defraudación informática. No existe un motivo evidente de porque Colombia no introdujo el concepto de ciberestafa o defraudación informática.

El delito del grooming es totalmente distinto a los anteriores mencionados debido a que este no se encuentra en Colombia, pero si en España y es un bien jurídico totalmente ajeno a la intimidad, y este es "la libertad e indemnidad sexual", debido a que lo que se quiere proteger es la sexualidad de un menor de edad, ya que en este no existe un desarrollo psicológico o social. Colombia no es ajena a este problema y en el 2017, formulo un proyecto de ley que pretendía proteger a los menores de edad de las redes sociales, esto debido al gran aumento de conductas que estaban afectando a los menores, como los son el grooming, el sexting, la sextorsión o el ciberbullying, pero lamentablemente este proyecto no fue aprobado, perdiéndose la iniciativa legislativa para regular esta conducta. Con esto quedó demostrado la necesidad de que Colombia regule estas conductas lesivas con rapidez, debido a que están afectando a los menores a través de medios informáticos

Como se mencionó anteriormente, no se pudo aprobar el proyecto de ley que venía con la iniciativa de regular estos tipos de delitos, dejando al descubierto la necesidad de una norma que proteja la figura del sexting, (Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes; se modifica el código penal y se dictan otras disposiciones., 2017)(colombia, 2017) debido a que en la explicación de este proyecto, la policía nacional denuncia que de 2015 a 2016 subieron de 20, a 87 casos por año, viéndose un crecimiento exponencial, demostrando que la justicia necesita una solución a casos que resplandecen por su

impunidad, debido a que esta conducta no se encuentra regulada. Otro dato que demuestra que los casos son muchos más de los que se reportan, es el informe del ministerio de las tecnologías dado por RCN radio, que nos dice que “el 72 % de los colombianos no están familiarizados con términos como ciberacoso, grooming o sexting”, demostrando que las personas en Colombia no son capaces de distinguir cuando se les comete este tipo de conductas.

La suplantación de sitio web es un delito que es poco común en las legislaciones extranjeras debido a que, en la mayoría de los países, el denominado pharming se encuentra dentro de la estafa informática, ello se debe a que entienden que se está haciendo una manipulación informática o medios semejante. Colombia innovo en este delito, el cual se ha adaptado muy bien a la realidad del país, ya que como se demostró en su capítulo este articulo trae dos supuestos, siendo el primero el que trae todos los verbos desde su fabricación hasta su final, que sería el envío. El segundo inciso trae la modificación de una dirección IP para engañar al usuario y vulnerar los derechos patrimoniales y morales de autor. Todo esto para demostrar que en Colombia se hizo bien al crear este delito independiente, ya que sanciona todo lo que se pretenda hacer con una intención ilícita con un sitio web, enlace o ventana emergente, y además de esto también toda clonación de dirección IP para suplantar una página real. Haciendo con todo esto un delito muy completo y necesario para combatir la cibercriminalidad en Colombia.

Lista de Referencias

Acurio, S. (2016). *Delitos informaticos: Generalidades*.

Anguíta, jose. (2018). *Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. 4*, 9. http://dx.doi.org/10.18847/1

Barrio, M. (s. f.). *La ciberdelincuencia en el DERECHO ESPAÑOL*. 14.

Bejarano, P. (2018). *Z1, la historia de la primera electrocomputadora programable*.

Bustos, R. (1989). *Manual de derecho penal, parte general* (3 sera edicion). Ariel.

Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes; se modifica el código penal y se dictan otras disposiciones., Penal (2017).

Cuenca, A. (2014). *El nuevo delito de grooming del articulo 183 bis del codigo penal*.

Devia, E. (2017). *DELITO INFORMÁTICO: ESTAFA INFORMÁTICA DEL ARTÍCULO 248.2 DEL CÓDIGO PENAL*. 468.

Díaz, L. (2011). *El denominado «child grooming» del articulo 183 bis del codigo penal: Una aproximacion a su estudio .* 22.

Diaz, P. (2017). *Tratamiento penal del sexting.* 12.

El cibercrimen en España: Un delito con «casi el cien por cien» de impunidad. (2020, noviembre 3). abc. https://www.abc.es/espana/abci-cibercrimen-espana-delito-casi-cien-cien-impunidad-202011040036_noticia.html

Facultat d'Informàtica de Barcelona. (s. f.). *Historia de internet*.

Fernandez, I. (s. f.). *Elsexting y otros delitos cometidos mediante telefonos moviles.* 7.

Figueiras, S. (2021, diciembre 13). *¿QUÉ ES EL HACKING?* https://www.ceupe.mx/blog/que-es-el-hacking.html

Circular 3 del 2017, (2017) (testimony of Fiscalia General del Estado).

gonzalez, D. (2017). *La protección de información y los datos en el marco de la Ley 1273 de 2009: Un estudio del dato y la información como objeto material en el tipo penal hurto por medios informáticos.*

Gonzalez, M. (2014). *Fraude en internet y estafa informatica*. Univercidad de oviedo.

Gudin, F. (2018). *NUEVOS DELITOS INFORMÁTICOS: PHISING, PHARMING, HACKING Y CRACKING*. 15.

La vanguardia. (2018, junio 27). *¿Qué aportó a la ciencia Alan Turing?* https://www.lavanguardia.com/historiayvida/historia-contemporanea/20180611/47312986353/que-aporto-a-la-ciencia-alan-turing.html

Lopez, O. (2020, junio 7). *Los ciberdelitos son ya el 10% de las infracciones penales conocidas*. https://elpais.com/espana/2020-06-07/los-ciberdelitos-son-ya-el-10-de-las-infracciones-penales-conocidas.html

Ministerio de Justicia. (2015). *ANÁLISIS DE DERECHO COMPARADO SOBRE CIBERDELINCUENCIA, CIBERTERRORISMO Y CIBERAMENAZAS AL MENOR.* (p. 191).

Navarro, N. (2020). *EL SEXTING: INTERVENCIÓN PENAL*. Univercitat Jaume.

Palazzi, P. (2016). *Los delitos informaticos en el codigo penal.*

PALOP, M. (2017). *PROTEC CIÓN JURÍDICA DE MENORES VÍCTIMAS DE VIOLENCIA DE GÉNERO A TRAVÉS DE INTERNET*. Univercitat Jaume.

Posada, R. (2013, junio 9). *El delito de acceso abusivo a sistema informático: A propósito del art. 269A del CP de 2000*.

Posada, R. (2017). *Los ciber crimenes: Un nuevo paradigma de criminalidad*.

Rico, M. (2012, septiembre 12). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos*.

Rodriguez, M. V. (2015, octubre 30). *Estafa informática. El denominado phishing y la conducta del "mulero bancario": Categorización y doctrina de la Sala Segunda del Tribunal Supremo*.

Salvadori, I. (2011a). *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado*. 32.

Salvadori, I. (2011b, junio). *LOS DELITOS CONTRA LA CONFIDENCIALIDAD, LA DISPONIBILIDAD Y LA INTEGRIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS*.

Suarez, A. (2019). *Lecciones de derecho penal, parte especial* (Vol. 2).

Tecnóesfera. (2021, febrero 22). *Estas son las prácticas más usadas de suplantación de sitios web*.

Union Europea, C. (2001). *Informe explicativo, convenio sobre la ciberdelincuencia.* (p. 2) [Explicativo]. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802fa403

VELASQUEZ, F. (1995). *DERECHO PENAL, PARTE GENERAL.* (segunda edición). Temis.

STSM 0526/16 del 14 de marzo de 2017.

STS, 603/2000 del 20 de noviembre de 2001, FJ2.

SCSJ, 1245/2015 del 11 de febrero de 2015.

SCSJ, 14302/2016 del 5 de octubre de 2016.