El CIBERDELITO EN EL DERECHO PENAL COLOMBIANO.

CYBERCRIME IN COLOMBIAN CRIMINAL LAW.

Jean Harold Bujato Venencia

C.C. 72.000.571

Código estudiantil: 200121571

Correo institucional: Jbujato@unisimon.edu.co

Andrés Alvarado Pertuz

C.C. 1.004.356.954

Código estudiantil: 201421655308

Correo institucional: aalvarado7@unisimon.edu.co

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de

Especialista en Derecho Penal

Tutor

Dr. Jairo Enamorado Estrada

RESUMEN

La investigación se encuentra enfocada en analizar los vacíos que se encuentran en la legislación penal colombiana con respecto a los delitos informáticos, que conlleva a que no se de total cumplimiento a la aplicación de la pena en este tipo de delitos, todo esto teniendo en cuenta que los ciberdelitos o delitos informáticos, se pueden realizar desde cualquier lugar, no siendo necesaria la presencia de la persona para cometer el acto delictivo, hecho que como es evidente no permite que se le de cumplimiento a las penas promulgadas en la ley 1273 de 2009, en los diversos tipos de delitos informáticos.

Es de vital importancia definir el ciberdelito aquellos actos delictivos que se cometen a través de las redes informáticas, realizando acciones que reúne las características que delimitan el concepto de ser un delito antijurídico, pero que tiene la característica esencial de utilizar un elemento informático, llegando a vulnerar los derechos del afectado.

En la actualidad todas las actividades que realiza una persona requieren del servicio de internet, servicios tales como los recaudos de servicios públicos, compra de acciones en la bolsa, pagos interbancarios, entre otros, lo que permite que los ciudadanos tengan que emitir mucha información personal en las diversas

páginas, convirtiéndose en presa fácil para quienes se dedican al ciberdelito, razón por la cual el estado colombiano se ha visto en la necesidad de crear la normatividad para regular este tipo de delitos, la problemática radica en la imposibilidad de dar cumplimiento a estas leyes, ya que en muchos casos estos delitos se causan de forma virtual, por lo cual no se le da el cabal cumplimiento a lo emitido en la norma.

En Colombia se promulgó la Ley 1273 de 2009, referente a todos los delitos que se relacionen con la tecnología, el ciberdelito, y las diversas modalidades de este tipo de delitos, otorgando una sanción o pena dependiendo de la modalidad del delito cometido, sanciones que pueden ser monetaria o privativas de la libertad por un tiempo determinado.

Es de vital importancia mencionar que la inseguridad cibernética se ha convertido en un flagelo no solo en Colombia, sino en todos los países del mundo, problema bastante complejo que requiere de la intervención de los gobiernos, situación que se ha vuelto dramática perjudicando a muchas personas que han sido víctimas de este tipo de delitos.

Es importante mencionar que el nacimiento de las redes informáticas conllevaron a la proliferación de esta forma de delinquir, por lo cual es imprescindible analizar y profundizar acerca de los motivos por los que se han proliferado este tipo de delitos, donde el las redes de la información han

contribuido mucho a la proliferación de los mismos. (Van Eekelen, M.C.J.D & Vrankend, H.P.E., 2012). Es de anotar que el internet ha pasado por diversas etapas, y de acuerdo a su evolución y desarrollo esto ha permitido que aparezcan las nuevas formas de delinquir relacionadas con la sistematización.

Las redes informáticas a través del tiempo ha venido evolucionando, hecho que ha permitido las conductas delictivas, se han dado cuatro etapas entre las cuales se encuentran: a) el denominado período militar, que se registra durante los años setenta, por otro lado, se encuentra el ciclo comprendido entre los años 80 y 90; y por último, se encuentra la fase comercial, que se vivió durante los años noventa; para llegar a la última etapa que es la del actual siglo XXI. (Nogales Flores, 2012).

Cabe mencionar que a nivel mundial se han producido grandes delitos a través de las redes tecnológicas, como sucedió en el Banco de Suecia, en el gran robo de más de un millón de dólares, hecho que se produjo por medio de las redes informáticas, utilizando un procedimiento diversos, burlando todo tipo de límites de seguridad, utilizando diversas técnicas, tales como la implantación de virus entre estos el denominado Troyano, en el cual se lograba intervenir a todos los clientes del banco, cuando estos intentaban acceder a la página del banco, el programa se activaba, siendo estos dirigidos a una página del banco que no era la

original, accediendo a las diversas claves y usuarios de todos los clientes del banco, todos los clientes que ingresaban a la página original del banco eran inmediatamente dirigidos a la página falsa, con el argumento de que se estaban presentando diverso tipo de problemas técnicos, en donde los delincuentes utilizaban los datos que habían obtenidos de los clientes del Banco, a través de lo datos ya suministrados, y poder sacar todo el dinero existente en la verdadera página del banco.

Generalmente la cibercriminalidad se considera como una forma de delinquir segura, ya que quienes cometen estos delitos, engañan a los clientes de las entidades comerciales o bancarias, sin enfrentarlos directamente, solo se hacen dueños de sus claves con el propósito de llevar a cabo sus delitos. (Periódico El Tiempo. 2009).

De igual manera el también se considera un delito seguro, ya que se realiza a través de la distancia por los diversos medios, tales como el correo electrónico, el cual se puede ejecutar desde cualquier sitio y a cualquier hora, sin tener la carga de que los van a atrapar…

Es importante señalar que los delitos informáticos inciden negativamente tanto en las organizaciones, como en las organizaciones, en el que el gobierno debe dar cumplimiento a lo preceptuado en la Ley 1273 de 2009 con el propósito de brindar seguridad a la ciudadanía, al respecto, no solo debe existir un esfuerzo

privado por adaptar sistemas de seguridad, debe ser respaldado por las herramientas que la ley les otorga a los jueces, con las cuales puedan desarrollar eficazmente su función, razón por la cual se hace urgente y necesario que en Colombia se apliquen las normas jurídicas correctivas, con el cumplimiento de las pernas estipuladas en la Ley 1273 de 2009, con el fin de brindar seguridad a los ciudadanos, y evitar que se sigan proliferando los delitos informáticos, para así de esta forma, el Estado pueda brindar seguridad a los ciudadanos protegiendo su información financiera, y cuidado de su patrimonio.

ABSTRACT

The investigation is focused on analyzing the gaps found in Colombian criminal legislation regarding computer crimes, which leads to a lack of full compliance with the application of the penalty in this type of crime, all this taking into account that cybercrimes or computer crimes can be carried out from anywhere, the presence of the person not being necessary to commit the criminal act, a fact that, as is evident, does not allow compliance with the penalties enacted in Law 1273 of 2009 , in the various types of computer crimes.

It is of vital importance to define cybercrime those criminal acts that are committed through computer networks, carrying out actions that meet the characteristics that define the concept of being an unlawful crime, but that have the

essential characteristic of using a computer element, reaching violate the rights of the affected party.

At present, all the activities carried out by a person require internet service, services such as collections of public services, purchase of shares on the stock market, interbank payments, among others, which allows citizens to have to issue a lot of personal information. in the various pages, becoming easy prey for those who are dedicated to cybercrime, which is why the Colombian state has seen the need to create regulations to regulate this type of crime, the problem lies in the impossibility of complying with these laws, since in many cases these crimes are caused virtually, which is why the provisions of the standard are not fully complied with.

In Colombia, Law 1273 of 2009 was enacted, referring to all crimes related to technology, cybercrime, and the various modalities of this type of crime, granting a sanction or penalty depending on the modality of the crime committed, sanctions that They can be monetary or deprived of liberty for a certain time.

It is vitally important to mention that cyber insecurity has become a scourge not only in Colombia, but in every country in the world, a fairly complex problem that requires government intervention, a situation that has become dramatic, harming many people. who have been victims of this type of crime.

It is important to mention that the birth of computer networks led to the proliferation of this form of crime, for which it is essential to analyze and delve into the reasons why this type of crime has proliferated, where information networks They have greatly contributed to their proliferation. (Van Eekelen, M.C.J.D & Vrankend, H.P.E., 2012). It should be noted that the Internet has gone through various stages, and according to its evolution and development, this has allowed the appearance of new forms of crime related to systematization.

Computer networks over time have been evolving, a fact that has allowed criminal behavior, there have been four stages among which are: a) the so-called military period, which is recorded during the seventies, on the other hand, is find the cycle between the years 80 and 90; and finally, there is the commercial phase, which was experienced during the nineties; to reach the last stage that is the current 21st century. (Nogales Flores, 2012).

It is worth mentioning that worldwide there have been great crimes through technological networks, as happened in the Bank of Sweden, in the great robbery of more than one million dollars, a fact that occurred through computer networks, using a diverse procedure, circumventing all kinds of security limits, using various techniques, such as the implantation of viruses, among them the so-called Trojan, in which all the bank's clients were able to intervene when they tried to access the bank's page , the program was activated, being directed to a page of the bank that

was not the original, accessing the various passwords and users of all the bank's clients, all the clients who entered the original page of the bank were immediately directed to the false page, arguing that various types of technical problems were occurring, where criminals used the data they had obtained from customers you from the Bank, through the data already supplied, and be able to withdraw all the existing money on the real page of the bank.

Generally, cybercrime is considered as a safe form of crime, since those who commit these crimes deceive the clients of commercial or banking entities, without confronting them directly, they only become owners of their passwords with the purpose of carrying out their crimes. . (Newspaper El Tiempo. 2009).

Referencias Bibliográficas

Castillo Jimenez, María Cinta, Ramallo Romero, Miguel. (1989). El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático..

Congreso de la República. Ley No. 1273 del 5 de enero de 2.009

Gutiérrez, Mariluz. (2009). Crimen Silencioso. No. 010 - Mayo del 1999. (consultado en http://www.alfa-redi.org/rdi-articulo.shtml?x=266, noviembre de 2009).

Jimenez Dan, Ricardo. (2009). Crimen Silencioso. En Revista de Derecho Informático. (Recuperado: http://www.alfa-redi.org/rdi-articulo.shtml?x=266).

Naciones Unidas. (2005). Oficina Contra la droga y el delito. Delitos informáticos.

Nogales Flores, J.T. Tecnologías de Internet. (2012). Naturaleza y evolución de Internet. Recuperado de: https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html

Periódico El Tiempo. Hackers borran contenido de nuevo periódico digital de Barranquilla (Recuperado de: http://www.eltiempo.com/colombia/caribe/hackers-borran-contenido-denuevo-periodico-digital-de-barranquilla_6361227-1, noviembre de 2009).

Pérez Luño, Antonio Enrique. (1996). "Manual de informática y derecho", Editorial Ariel S.A., Barcelona.

Rivera Llano, Abelardo. (1995). Dimensiones de la informática en el derecho. Editorial Jurídica Radar, Santa fe de Bogotá p. 89.

Rodriguez, Ricardo. (2018). Historia de un „cracker" barranquillero. Periódico El Heraldo.

Sneyers, Alfredo. (1990). El fraude y otros delitos informáticos. Ediciones T.G.P. Tecnologías de Gerencia y producción.

Téllez Valdés, Julio. (1999). "Los Delitos informáticos. Situación en México", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida.

Tiedemann, Klaus, (1985). Poder informático y delito, Barcelona, España.

Van Eekelen, M.C.J.D & Vrankend, H.P.E. (2012). The Internet: Historical and

Technical Background, en“Cyber Safety: An Introduccion” (Leukfeldt & Stol, coord). Ed. Eleven International Publishing. La Haya, Holanda. págs 31 - 43.