Impacto económico y social que ha generado el delito cibernético sobre el comercio electrónico en Colombia durante el periodo 2019-2021

Claudia Andrea Gil López
Isabel Fresneda Saldarriaga
Norman Molina Grajales
Tecnológico de Antioquia - Institución Universitaria

Resumen

Esta investigación tiene como fin evaluar el alto impacto económico y social que ha tenido el delito cibernético en Colombia, donde su comercio electrónico se encuentra en progreso comparado con el de otros países. En ese sentido, se pretende contextualizar la gravedad del tema, ya que esta herramienta tecnológica es el medio por donde se realiza la mayoría de actividad mercantil. Es importante destacar que contener este fenómeno ha sido dificultoso, teniendo en cuenta que es un país donde sus herramientas tecnológicas y justicia penal son aún limitadas. La investigación se realizará con un enfoque mixto, no experimental, considerando los interrogantes básicos de la problemática que afronta el comercio electrónico por causa del delito cibernético y las consecuencias que tienen para la actividad comercial. En cuanto a las conclusiones del instrumento aplicado, el uso del comercio electrónico se convirtió en una herramienta esencial para cualquier escenario productivo, en muchas ocasiones con impactos negativos por diferentes modalidades de engaño perpetuadas por criminales. Por consiguiente, es crucial analizar las amenazas para contrarrestar los riesgos dentro de una empresa y gestionarlos de una manera eficiente y eficaz para generar confianza en el mundo digital y así acrecentar los múltiples beneficios que le ha aportado a la humanidad.

Palabras clave: delito informático; comercio electrónico; impacto; ciberseguridad; tecnología.

Introducción

Según Protheroe (2023), "El comercio electrónico es un proceso de venta y compra de productos por medios electrónicos, donde se realizan negociaciones a gran escala, sin tiempo limitado, permitiendo relaciones como tratados comerciales entre países y aplicando diferentes tipos de comercio" (párr. 1). Esto influye profundamente en que, así como el comercio electrónico tiene alta incidencia en Colombia y en el mundo, y que por temas de la pandemia se aceleró aún más este proceso virtual; de esa misma forma Alfoncea (2016) plantea que el delito cibernético "son todos aquellos actos o hechos que, estando tipificados como delitos se desarrollan en internet o requieren del uso de medios informáticos para ser realizarlos" (párr. 2).

Por otro lado, según García (2010), en su reseña de la ubicación geográfica del país, "Colombia es el único país de Suramérica que cuenta con costas en el océano Pacífico y el océano Atlántico (Mar Caribe)" (párr. 2). Lo que lo hace contar con una

gran extensión marítima. Esta ubicación beneficia al país en términos comerciales, dado que es importante tener estas vías marítimas para sus relaciones de negocios. Asimismo, como el comercio en Colombia se ve beneficiado con este tema, conviene destacar otros elementos derivados de esta actividad comercial como el uso del comercio electrónico y los problemas que se derivan de esta actividad.

De manera que, el comercio electrónico ya es habitual en cualquier tipo de negociación en Colombia y el uso de internet ya es del diario vivir. A su vez, el delito cibernético es un fenómeno que crece de forma exponencial y "con dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal" (Alfocea, 2016, párr. 7).

Sin embargo, y pese a estas estadísticas, la creciente demanda del uso del comercio electrónico del país ha sido una característica exponencial en los últimos años. Es muy importante destacar que con el crecimiento del comercio electrónico (e-commerce) se ha venido presentando paralelamente un problema de tal magnitud que existe una legislación solamente dedicada a penalizar estos actos que se han de considerar punibles en toda su expresión (Cano, 2013). Entonces, es importante evaluar el alto impacto económico y social que el delito cibernético ha tenido en Colombia y su crecimiento vertiginoso entre el período 2019-2021. Donde apoyados en el informe realizado por la Cámara Colombiana de Comercio Electrónico (CCCE, 2020), quien expone:

> El crecimiento exponencial de los delitos informáticos para 2020, que impulsó la pandemia ocasionada por el COVID-19, es una señal de alerta para blindar los sistemas de información, sitios web, correos electrónicos y en general, los documentos digitales que generan empresas y entidades públicas (párr. 1).

Esto indica que las empresas también vienen sufriendo este acto delictivo, por el cual muchas de ellas ya han implementado diversas estrategias para contrarrestar esta situación que pone a tambalear y a repensar como serán las siguientes operaciones en el mercado digital. Teniendo en cuenta lo anterior expuesto, Cámara Colombiana de Informática y Telecomunicaciones (CCIT, 2019) expone que "en Colombia, el monto promedio de las cifras de pérdidas por ataque puede oscilar entre 300 millones a 5.000 millones de pesos, según el tamaño de la empresa afectada" (p. 10). Es por ello por lo que hoy en el mundo y en Colombia se está trabajando en conjunto con todas las autoridades, los estamentos y las personas que de alguna u otra manera se han visto afectados por un ciberataque, que no solo está representado en pérdida de dinero, sino que también en robo de datos y suplantaciones.

Por otra parte, tal como lo destaca López (2017) los ciberdelincuentes se valen de páginas de internet para extraer información personal, del wifi gratis y plataformas como Netflix, son muy peligrosas y resultan bastante útiles para los delincuentes captar información.

De ello resulta apropiado mencionar algunas de las tendencias delictivas que se operan continuamente en las empresas, con la finalidad de suplantar identidades, falsificar información o desviar dineros, tal como el *ransomware* (una ciberamenaza subestimada en Colombia), minería en criptomonedas, ataque de denegación de servicio (DDOS), malware y el ataque al correo electrónico empresarial (BEC), basado en DeepFake, son algunas de las modalidades utilizadas para extraer información personal y confidencial, que revela el informe investigativo soportado por la Policía Nacional de la República de Colombia (CCIT, 2019).

Debido a esto es importante determinar el alcance negativo que ha tenido el delito cibernético y su impacto histórico. En tal sentido se deben identificar las debilidades del sistema para entender por qué ha sido este fenómeno tan paralelo al comercio electrónico y poder minimizar los riesgos y los peligros con el uso frecuente del internet y sus acciones allí realizadas, usando toda la capacidad intuitiva y siempre actuando de manera preventiva. Es importante destacar que el ciberdelito no conoce fronteras y siempre están los ciberdelincuentes perfeccionando sus formas de atacar y hacer daño. En ese mismo contexto se debe advertir la importancia y el compromiso de todos los que actúan en la red para que unan sus esfuerzos y se pueda combatir este fenómeno tan peligroso.

En síntesis, para el desarrollo del presente trabajo se cuenta con tres secciones. En la primera se desarrolla una revisión bibliográfica de antecedentes, donde se podrán encontrar aspectos relevantes de investigaciones relacionadas con el tema objeto de estudio. En la segunda se realiza la revisión de la literatura donde expondrán los diferentes conceptos básicos del problema, la información documental, informes y artículos que soportarán la investigación y conceptos tomados de entidades vinculadas con el tema principal. Finalmente se encontrará la sección del análisis de los resultados, las conclusiones y posibles recomendaciones que permitan entender el impacto económico y social que ha tenido el delito cibernético sobre el comercio electrónico en el país durante el período 2019-2021.

Metodología

Esta investigación está basada en una metodología mixta, es decir, tanto en la teoría cuantitativa como la cualitativa. Según Hernández y Mendoza (2018), los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos

como cualitativitos, así como su integración y discusión conjunta para realizar inferencias producto de toda la información recabada.

En ese mismo contexto hubo recolección y análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta implementados en secuencia, paralelo o mezclados desde el planteamiento. Las características del método mixto amplían las posibles dimensiones de la investigación y proporcionan riqueza interpretativa a las investigaciones (Hernández y Mendoza, 2018).

Por tanto, en este enfoque que se le dio a la investigación se utilizó la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico (Hernández, 2014). Asimismo, el instrumento para recoger la información requerida en la investigación será la entrevista, Schettini y Cortazo (2016) exponen:

> La entrevista se caracteriza por ser un proceso comunicativo que se da en un encuentro entre sujetos, previamente negociado y planificado. En la actualidad, con los avances tecnológicos en términos de comunicación, esta concepción fue sufriendo algunas variaciones, ya que los nuevos instrumentos comunicativos existentes (videoconferencias, chats, celulares con sistema 4G). (p. 14)

De igual forma, otra de las definiciones expuesta por Morga (2012) manifiesta: "su objetivo es recolectar información pertinente para responder una pregunta de investigación, ya sea en investigación cuantitativa o cualitativa; se conduce en función del paradigma de investigación usado" (p. 14).

Discusión y resultados

Con el propósito de determinar y recopilar opiniones acerca del tema objeto de estudio, se realiza una breve entrevista a dos personas que han desarrollado gran parte de su carrera profesional con temas afines al comercio electrónico, marketing digital, medios digitales, transformación digital y, posteriormente, han abordado e investigado el delito cibernético en gran amplitud. La entrevista se realizó en el mes de septiembre de manera virtual, consecuentemente se asignaron cinco preguntas abiertas a cada entrevistado. Donde se infiere que el comercio electrónico en Colombia tuvo un auge muy importante a raíz de todo el tema de apropiación digital en el que nos tuvimos que ver inmersos debido a la pandemia, aun los niveles de confianza, credibilidad y claridad, por parte del cliente para pasar de sus compras presenciales a las compras virtuales es débil. En el mundo digital se confía primero el tema de la automatización y la sistematización de nuestros datos, aunque existe la ley del Habeas Data la cual nos señala que nadie más puede utilizar nuestros datos, en donde nos veamos envueltos en extorciones, como mensajes de texto, correos electrónicos maliciosos, entre otros.

Asimismo, en relación con el delito cibernético, y de acuerdo con las respuestas obtenidas por el entrevistado, es un fenómeno abrumador que como todo delito parece no tener limite. Genera pánico en las personas, acecha a las empresas, pone en jaque a los gobiernos y debilita los sistemas de seguridad. Su impacto es tan negativo que provoca una serie de daños como reputaciones, demandas altamente costosas y no muy lejano la quiebra total de una empresa que no estaba debidamente preparada para un incidente de tal magnitud, incluso las más grandes empresas de Colombia y del mundo han sufrido este flagelo. Las personas que tienen los datos, la información, la forma de operar y las características de cada persona, ya que están constantemente capturando información, mediante la activación de Cookies y demás herramientas como los likes, la ubicación etc., se les da el poder necesario para que puedan vender publicidad en términos digitales y al tener acceso a esa información los hace tener mucho poder indudablemente.

Conclusiones

Previamente a las respuestas de los entrevistados se infiere que el alcance de los ciberdelincuentes es extraordinario y se valen de toda la información que por ingenuidad o desconocimiento plasman en las redes sociales, páginas y demás herramientas digitales que la tecnología nos ofrece para extraer información que finalmente termina siendo muy útil en el acto delictivo, es por ello que prevalecer la seguridad de la información del usuario haría elevar la confianza digital de las empresas.

La privacidad de la información de los clientes es sin duda una garantía de continuidad y prevalencia de una empresa atreves del tiempo. Para que esto sea posible se debe contar con amplia transformación digital y simultáneamente capacitaciones, teniendo en cuanta que lo primordial son aquellas personas altamente vulnerables a un ataque cibernético, ya sea por su edad o desconocimiento.

> Consecutivamente es responsabilidad empresarial minimizar la oportunidad de fraude en los momentos de intercambio de productos o servicios vía electrónica, para ello será necesario definir los procedimientos correctos, tanto la compra y venta, como por ejemplos rastrear pagos o pedidos no autorizados, y análogamente invertir en mecanismos de protección para detectar de manera oportuna amenazas cibernéticas (antimalware o antivirus).

Por otro lado, incursionado correctamente la tecnología e innovación en las empresas, Colombia dejaría de ser visto globalmente como un país subdesarrollado y a largo plazo se convertiría en un país competitivo dentro de la globalización.

La seguridad informática dentro de cualquier proceso de comercio electrónico se verá perpetrada por la falta de refuerzo en seguridad informática, ligado no solo a los establecimientos de comercio, si no a los comercios asociados, PSE, bancos, entre otros, que finalmente son garantes del proceso.

Referencias

Alfoncea, J. (2016, diciembre 16). Qué son y cuáles son los delitos. Delito Penal. https://delitopenal.com/cuales-los-delitos-ciberneticos/

Cano, J. (2013). I*nseguridad de la información. Una visión estratégica*. Alfaomega.

CCCE. (2020, diciembre 29). Con la *"nueva modalidad", los delitos informáticos se multiplicaron en el país, pero pueden contrarrestarse con inversiones digitales.* https://www.ccce.org.co/noticias/con-la-nueva-normalidad-los-delitos-informaticos-se-multiplicaron-en-el-pais-pero-pueden-contrarrestarse-con-inversiones-en-seguridad-digital/

CCIT. (2019). *Tendencias del Cibercrimen en Colombia 2019-2020.* CCIT. www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

García, A. (2019, febrero 21). *Ubicación geográfica de Colombia.* Toda Colombia. https://www.todacolombia.com/geografia-colombia/ubicacion-geografica.html

Hernández, C., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación* (6ª ed.). McGraw Hill.

Hernández, R. y Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* McGraw Hill.

López, D. (2017, febrero 22). *¿Cómo roban nuestros datos personales en internet?* El Nacional. https://www.elnacional.cat/es/tecnologia/datos-personales-internet_138819_102.html

Morga, L. (2012). *Teoría y técnica de la entrevista. Red Tercer Milenio.* http://www.aliat.org.mx/BibliotecasDigitales/salud/Teoria_y_tecnica_de_la_entrevista.pdf

Protheroe, R. (2023, octubre 31). *¿Qué es el comercio electrónico?* Definición de comercio electrónico para 2021. Ecommerce Platforms. https://ecommerce-platforms.com/es/glossary/ecommerce

Schettini, P. y Cotazzo, I. (Coords). (2016). *Técnicas y estrategias en la investigación cualitativa.* Editorial de la Universidad de La Plata. http://sedici.unlp.edu.ar/bitstream/handle/10915/53686/Documento_completo__.-%20Cortazzo%20CATEDRA%20.pdf-PDFA.pdf?sequence=1