UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE SUFICIENCIA PROFESIONAL

INFLUENCIA DE LOS DELITOS INFORMATICOS EN EL CONTEXTO DE EMERGENCIA SANITARIA EN LIMA METROPOLITANA, AÑO 2021

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTOR:

GUEVARA GABRIEL AMADO

CÓDIGO ORCID: 0000-0002-7156-5549

ASESOR:

PANTIGOZO LOAYZA MARCO HERNAN

CÓDIGO ORCID: 0000-0001-6616-0689

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

FEBRERO, 2022

Resumen

De conformidad con el contexto social que venimos experimentando y de acuerdo a diferentes consultas bibliográficas, obtenemos como resultado que los delitos informáticos muestran un elevado avance en nuestro país y el resto del mundo; En razón a ello, destacamos la pertinencia del presente trabajo de investigación.

El presente trabajo busca analizar la influencia de los delitos informáticos en el contexto de emergencia sanitaria que viene atravesando nuestra sociedad actual y especialmente en el ámbito de Lima Metropolitana en el año 2021. A través de un análisis jurídico y de técnica legislativa, el trabajo resalta los principales aciertos y desaciertos de la ley 30096, proponiendo cambios que consideren una armonización entre el contexto social y el derecho positivo, fomentando de este modo el respeto integral y oportuno de los derechos fundamentales que nuestra Constitución establece.

Nuestra investigación está directamente orientada a brindar un aporte a labor que desarrollan los docentes en las aulas universitarias en materia de derecho y para todos los operadores de la justicia en nuestro país, incluyendo a nuestro legisladores, desarrollen actividades académicas, deliberativas y de análisis respecto a la normatividad relacionada con los delitos informáticos y de este modo se actualice y contribuya a la solución de los problemas sociales que hoy afecta a nuestra sociedad.

Palabras clave: Derecho informático, Delitos informáticos, Ciberseguridad, TIC

Abstract

In accordance with the social context that we have been experiencing and according to different bibliographical consultations, we obtain as a result that computer crimes show a high advance in our country and the rest of the world; For this reason, we highlight the relevance of this research work.

The present work seeks to analyze the influence of computer crimes in the context of the health emergency that our current society is going through and especially in the area of Metropolitan Lima in the year 2021. Through a legal analysis and legislative technique, the work highlights the main successes and failures of Law 30096, proposing changes that consider a harmonization between the social context and positive law, thus promoting comprehensive and timely respect for the fundamental rights established by our Constitution.

Our research is directly oriented to provide a contribution to the work carried out by teachers in university classrooms in the field of law and for all justice operators in our country, including our legislators, to develop academic, deliberative and analytical activities regarding the regulations related to computer crimes and thus update and contribute to the solution of social problems that affect our society today.

Keywords: Computer Law, Computer Crimes, Cybersecurity, ICT

Tabla de Contenidos

Introducción

Auscultando nuestra realidad en los últimos tiempos verificamos que, la globalización ha traído consigo el proceso de transversalización cultural, social y económica a nivel mundial trayendo consigo un gran desarrollo de las tecnologías de la información y comunicación (TIC), y la gran difusión de la misma resulta jugando un papel imprescindible en el desarrollo cultural de la sociedad.

La gama de nuevas posibilidades que ofrecen las TIC y ponen al servicio del hombre se relaciona con el procesamiento, almacenamiento, transmisión y digitalización de la información, así como un conjunto de procesos y productos que simplifican y nos facilitan la comunicación, haciendo más viables la interacción entre las personas.

Uno de los principales inventos tecnológicos que ha traído la globalización es el internet con todos sus accesorios tales como: Messenger, correo electrónico, Facebook, twitter, web, WhatsApp, Instagram, etc. Este avance tecnológico revolucionó nuestra visión de tiempo-espacio en las relaciones humanas, por lo que la comunicación se puede dar en tiempo real sin importar la distancia ni fronteras, como podemos experimentar con mayor énfasis en estos tiempos de pandemia con el desarrollo de las plataformas de video conferencias que se ha convertido en una acción y necesidad cotidiana.

Por su parte, las herramientas que ofrecen las TIC a partir de internet, se consideran ejes fundamentales para el desarrollo de nuestra sociedad, dado que auspician un canal eficaz para el desencadenamiento de una vasta gama de servicios básicos en los lugares más recónditos de nuestro planeta, abarcando todos los ámbitos que se desarrolla nuestra sociedad.

No obstante, conforme avanza la tecnología a velocidades impresionantes, se incrementa al mismo tiempo los riesgos relacionados en cuanto al uso adecuado de las tecnologías de la información y de comunicación. Hoy más que nunca de contexto de emergencia sanitaria en el que estamos atravesando, el desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen como principal herramienta el uso de los sistemas informáticos e internet.

En esta perspectiva, vislumbramos algunos aspectos vulnerables más significativos que traen consigo las TIC: a) La escasez de filtros adecuados en la red, que nos permitan establecer algún sistema de control, por lo que es casi imposible saber qué información se transporta en el espacio digital. b) El incremento del número de personas que tienen acceso y hacen uso de los medios tecnológicos sin ninguna dificultad c) La facilidad que ofrece la tecnología para que los delincuentes oculten su identidad y dificulte la imputación de los delitos que cometen d) La libertad que existe para acceder a la información y poder manipular o alterar datos, siendo posible hasta destruir sistemas informáticos por más confidenciales que estos sean.

1. ANTECEDENTES

1.1 Antecedentes Internacionales

Es importante recoger el aporte desarrollado por Velástegui (2019) en su artículo titulado "*Los Delitos Informáticos y su incidencia en la provincia de Pastaza"*, en el cual afirma que la tecnología actualmente es muy amigable con la población y es de fácil acceso, por tanto, también se presta para la comisión de ilícitos penales por parte de los delincuentes. En ese sentido afirma que:

> "La tecnología es más amigable con la población, pero también la pone en riesgo a sufrir más hechos ilícitos por medio del uso de esta tecnología, que se vuelve parte de uno cada día que avanza. En su metodología realizada tuvo un enfoque mixto, es decir, cualitativa y cuantitativa, tuvo como población a la provincia de Pastaza en el país de Ecuador y la muestra fue representativa para conocer su opinión y valoración. Se verificó que para la recolección de datos se utilizaron entrevistas y encuestas que permitieron al investigador recoger información muy relevante sobre el problema ya investigado" (Velástegui, 2019).

Dentro de sus principales conclusiones, afirma el autor que los delitos informáticos más comunes en su ámbito son la difamación, la calumnia y los de orden económico.

> "Los delitos informáticos se presentan con mayor continuidad en la difamación y calumnias, son muy comunes en las redes sociales teniendo un daño directo al honor y a la honra de personas naturales y jurídicas, la afectación de estos delitos al orden económico es incalculable, por motivo que estos hechos se dan con el desconocimiento de las personas, teniendo que implementar mejores controles y políticas de seguridad" (Velástegui, 2019).

Por otro lado, Narváez y Recalde (2018) señalan en una de sus revistas digitales que "la legislación penal americana debe adecuarse a los delitos que se presentan en la actualidad", especialmente lo concerniente a los delitos informáticos, por lo que proponen que debe tipificar las conductas penales para que exista un mayor control de estos hechos delictivos.

> "En los resultados de esta investigación se comentó que los delitos informáticos afectan directamente a la intimidad y el honor de una persona; por otro lado, se examinó sobre el uso de identidad de manera ilícita, así como muchas variedades de delitos que se van innovando de forma permanente. Se concluye por tanto que, todo este tipo de variedad de delitos es un fenómeno social que afecta a miles de personas en todo el mundo; por lo que propone, se debe tipificar estas conductas como figuras penales para controlar y minimizar este tipo de hecho delictivos" (Narváez y Recalde, 2018).

Así también, en la investigación desarrollada por Ruiz (2017) titulada "*Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos"*, en la cual el autor señala que, el desconocimiento del manejo de las herramientas digitales, tanto por parte de los operadores de3 la justicia como por gran parte de la población, favorece a los delincuentes para seguir cometiendo delitos de carácter informático y mientras no se tomen cartas en el asunto, la problemática seguirá latente.

> "Los delitos informáticos no solo afectan el patrimonio de muchas personas, sino también puede llegar afectar la privacidad de una persona o una colectividad. De la investigación se infiere que, la falta de conocimiento de las tecnologías de información y la comunicación por parte de los operadores de justicia desencadena en la omisión de ciertos procedimientos para determinar la responsabilidad de los autores de estos hechos ilícitos" (Ruiz, 2017).

Por su parte, Maldonado (2014) en su investigación titulada "*Los delitos informáticos y el derecho constitucional a la seguridad jurídica"* afirma que, la población más vulnerable de es este tipo de delitos cibernéticos son los civiles y con escasos conocimientos en tecnologías de la información y comunicación. Los delincuentes se aprovechas de estas carencias que sufre la población para cometer sus actos delictuosos.

> **"Los delitos informáticos representan hoy en día un acto ilícito que afecta en mayor medida a aquellas personas que no poseen suficiente preparación o conocimientos informáticos, siendo vulnerables sino logran capacitarse oportunamente. Asimismo, se demanda la regulación efectiva a través de un marco normativo que contemple la protección de datos e integridad personal en razón del ejercicio y goce de sus derechos respaldados por la Constitución" (Maldonado, 2014).**

Echevarría (2015) en su investigación titulada "*Los Delitos Informáticos y El Derecho Constitucional a la Seguridad Pública"*, afirma que la tecnología se ha convertido en un fenómeno amigable para la mayoría de la población, ya que el acceso es cada vez cercano y posible. Sin embargo, los mecanismos de investigación de los delitos informáticos siguen siendo aún incipientes y poco eficaces, por lo que se requiere una mejora en los mecanismos legales para obtener mejores resultados.

> **"La tecnología se ha vuelto un factor muy amigable para el uso de todas las personas, enfocados en los delitos con la seguridad pública según los casos presentados en la Fiscalía General del Estado en el periodo 2015. Así la metodología fue de tipo cualitativa y cuantitativa, teniendo una población de 152 personas entre fiscales, agentes investigadores, abogados en libre ejercicio, personas afectadas, con una muestra de 109 ciudadanos lo cual ayuda para el análisis respectivo. La técnica aplicada fue la encuesta, con la utilización de los instrumentos como cuestionarios de encuesta. En esta investigación que, el país de Ecuador está en constante cambios sobre las investigaciones de los delitos informáticos, sin embargo, se tiene que mejorar el mecanismo que nos permite que todas las investigaciones frente a estos delitos tengan una dirección adecuada, dentro de un marco legal adecuado para realizar una eficiente acción frente a tales fenómenos" (Echevarría, 2015).**

1.2 Antecedentes Nacionales

Por su parte, en la investigación de Chilcon (2019) titulada "*El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional"*, señala que en nuestro país los delitos informáticos vienen

causando graves daños a la población en general y de modo particular a la Seguridad Nacional, por lo que es inminente que los operadores de la justicia implementen nuevas estrategias para afrontar con mayor eficacia y prontitud esta problemática que viene lacerando a nuestra sociedad.

> **"En la presente investigación se menciona que el *ciberdelito* ha alcanzado en el Perú un nivel elevado del número de víctimas por el uso de tecnología que por la ola de aplicaciones y de redes sociales, ello hace que cada día aumente la población de posibles víctimas de estos hechos ilícitos. Como conclusión presenta el autor que, el *cibercrimen* es un delito que se encuentra en crecida y lo preocupante es que no se está adoptando medidas de control y con el avance de la tecnología y el desarrollo de las capacidades. En efecto, estos hechos ilícitos sí afectan a la seguridad nacional, por lo que se recomienda implementar estrategias a largo plazo para el correcto abordaje de estos nuevos delitos" (Chilcon, 2019).**

Zorrilla (2018) en su investigación titulada "*Inconsistencias y ambigüedades en la ley de delitos informáticos Ley Nº 30096 y su modificatoria Ley Nº 30171, que imposibilitan su eficaz cumplimiento"*, manifiesta que en el Perú se adolece de una legislación que pueda definir adecuadamente la tipificación de los delitos informáticos, razón por la cual los operadores de la justicia se encuentran con barreras jurídicas insalvables que no permiten accionar eficientemente ante esta realidad.

> **"Entre los resultados de las encuestas se manifiesta que sí hay inconsistencias normativas para abordar este delito y que fue muy necesario que la ley de delitos informáticos tuviera su modificatoria. Concluyendo el autor que, hay varios artículos que presentan imprecisiones en su redacción originando confusión en sus operadores; afirma, finalmente que, en el Perú no hay una ley que defina correctamente los delitos que se presentan con mayor frecuencia en las redes sociales" (Zorrilla, 2018).**

En cuanto a la investigación presentada por Chávez (2018) denominada "*El delito contra datos y sistemas de informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de Lima Norte, 2018"*, manifiesta que los delitos informáticos en nuestro país están causando graves daños a la población y el avance es incalculable. También refiere que son los derechos fundamentales y la intimidad personal que más se vienen vulnerando.

> **“El delito contra datos y sistemas informáticos y su afectación directa a los derechos fundamentales y a la intimidad personal en la Corte Superior de Justicia de Lima Norte durante el año 2018. La metodología utilizada fue el enfoque cuantitativo, alcance explicativo, diseño no experimental, de corte transversal y de carácter correlacional – causal. La población fue de 510 abogados y la muestra de 220 de ellos; la técnica utilizada fue la encuesta y como instrumento un cuestionario por cada variable. En consecuencia, se concluye que se debe capacitar al personal y a todos los operadores que hacen lucha frontal a estos delitos, para que de esta forma no se vulneren todo tipo de medios de prueba que pueden servir como material idóneo para contrarrestar este tipo de delitos” (Chávez, 2018).**

Así también podemos ver en la investigación de Sequeiros (2016) titulada “*Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano – 2016”*, en la cual postula que ante la problemática de los delitos informáticos que se viene incrementando, es necesario y fundamental que continúe implementando y dando el soporte necesario a la estrategia del gobierno digital ya establecido en nuestro país.

> **“Dado que este fenómeno se va innovando, también se requiere realizar modificaciones en las leyes. Se concluye afirmando que, los delitos informáticos no deben limitar a la población de hacer uso de la tecnología ya que es un medio del cual nos simplifica procesos; por lo el contario, se necesita más presencia del Estado para dar el soporte de seguridad a través de un gobierno digital adecuado en donde los ciudadanos puedan hacer sus funciones, desde el punto donde se encuentren y lograr la integridad de información en la organización” (Sequeiros, 2016).**

2. BASES TEÓRICAS DEL TEMA

2.1 Delitos informáticos.

Según refiere Fayos (2016) en cuanto a las definiciones respecto a los delitos informáticos menciona tres significados a saber: “Es cualquier acción ilegal en la que el ordenador sea el instrumento o el objeto del delito y, más concretamente, cualquier delito ligado al tratamiento automático concretamente de datos; Cualquier acto criminoso relacionado con la tecnología informática, por el cual una víctima ha sufrido una pérdida y un autor ha obtenido intencionalmente una ganancia. Cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos”.

2.2 Los autores de los delitos informáticos (El sujeto Activo)

En cuanto al sujeto activo podemos decir con Maldonado (2014) afirma que: "Adolescentes con un coeficiente intelectual alto, y ausentes de toda consciencia de estar obrando mal (síndrome de Robín Hood). Mito ya que una gran cantidad de casos, son cometidos por sujetos que trabajan en el mundo de la informática, de edad superior y no necesariamente muy inteligentes. Empleados de confianza por la actividad que realizan o por el tiempo que llevan en la empresa. Además, existen los delincuentes a distancia".

Así también Narváez (2018) refiere que, "se ha venido realizando una caracterización casi mítica respecto del perfil del delincuente informático, basándose en los primeros casos de estudiantes americanos que fueron dados a conocer, en que se trataba de adolescentes con un coeficiente intelectual alto ausentes de toda consciencia de estar obrando mal".

Señala el mismo autor que "las características de delincuentes informáticos descritos por la mayoría de los autores, señalan al sujeto activo de estos delitos como jóvenes cuyas edades fluctuaban entre los 18 y los 30 años de edad, en su mayoría varones solteros sin antecedentes penales, inteligentes motivados por su profesión y por el desafío técnico".

Chilcón (2020) refiere que, "las conductas informáticas delictivas se llevan a cabo por personas vinculadas de algún modo a las empresas, como empleados de confianza, técnicos especialistas en programación y en general, todo tipo de personas con acceso material a las instalaciones de procesamiento de datos. Normalmente, suelen ser empleados de confianza por el tiempo que llevan en la empresa o por el tipo de trabajo que desempeñan en ella, y conocen debilidades del sistema. Sin perjuicio de lo anterior, Internet permite que hoy concurran como sujetos activos de los delitos informáticos, los delincuentes a distancia, quienes desde cualquier país del mundo pueden atentar contra un sistema de tratamiento de información".

Posso (2014) refiere que “los criminales informáticos en su generalidad son de sexo masculino de 18 a 30 años de edad, con características de ser un empleado de confianza en la empresa en la que normalmente desarrolla sus funciones, posee necesariamente conocimientos técnicos de computación e informática. Estos agentes responden a motivaciones dispares generalmente el “*animus delicti*” es motivado por razones de carácter lucrativo. Por la popularidad que representa este actuar en la sociedad moderna o por simple diversión *“hackers”* o por intención de que su actuar puede responder al deseo de destruir o dañar un sistema informático, lo que varía es la intencionalidad en su comisión”.

2.3 Las víctimas de los delitos informáticos (El Sujeto Pasivo)

Rendon (2012) refiere “que las características de las víctimas de los delitos son frecuentemente: Personas Jurídicas, Bancos, Compañías de Seguros Empresas públicas y privadas. Asimismo, no denuncian los delitos por temor a pérdida de imagen corporativa (Seriedad, solvencia y seguridad) buscan solucionar mediante medidas internas (despidos o aumentos de medidas de seguridad). Esta situación favorece a delincuentes porque, generalmente, no se denuncian los delitos, llegándose a un acuerdo con el delincuente”.

Es importante saber, continúa nuestro autor aseverando que, “las víctimas de estos delitos son generalmente personas jurídicas, como pueden ser, usualmente bancos compañías de seguros, empresas públicas y privadas, sin importar si cuentan o no con medidas técnicas de protección. Una vez que estas asociaciones detectan las conductas ilícitas de las cuales que han sido objeto, suelen no denunciar los delitos por temor a sufrir una pérdida de su imagen corporativa. No están dispuestas a perder la imagen de seriedad, solvencia y seguridad y antes de ver sus debilidades expuestas, prefieren solucionar sus problemas mediante la aplicación de medidas internas, como despidos o aumentos de seguridad”. Por lo tanto, esta actitud solo favorece a los delincuentes,

quienes no cesarán en seguir cometiendo delitos, sin que nadie pueda imputarles o recibir los remedios merecidos.

2.4 El bien jurídico tutelado

Como podemos ver, según la dogmática jurídica, sobre estos temas existe poca bibliografía que pudiera satisfacer las expectativas de una población que se siente desprotegida de las leyes y de sus autoridades. Como afirma Rendon (2012):

> **"Si bien existe consenso en aceptar a la categoría de los delitos informáticos como el reflejo de una nueva forma de criminalidad, que se relaciona directamente con el uso o la intermediación de un elemento o dato informatizado, existen dos distintos caminos para encarar el citado fenómeno desde un punto de vista propiamente penal: Uno de estos, que se acerca a la posición asumida por el legislador del Código Penal de 1991, así como las posteriores reformas, niega que el avance tecnológico y los problemas presentados por el uso generalizado de los sistemas informáticos configuren un nuevo interés digno de protección, de manera que, en realidad, subyacería una nueva forma de criminalidad aun carente de adecuada tutela, pero que versaría sobre bienes jurídicos ya conocidos por todos" (Rendon, 2012).**

2.5 El Estado frente a los delitos Informáticos

El Ministerio Publico, es la entidad estatal competente, para afrontar esta lacra social que atraviesa nuestro país, pero según informan fuentes oficiales, en Distrito Judicial de Lima existen sólo 47 Fiscales provinciales en materia penal. Los defensores de la legalidad se enfrentan a la compleja y apremiante realidad de la lucha los delitos informáticos con desabastecido equipamiento profesional y material.

2.6 Las tecnologías de la información y la comunicación

Conforme al planteamiento de Sequeiros (2016) quien afirma que, "en las dos últimas décadas han surgido distintos fenómenos (sociales, tecnológicos, etc.) que, pese a no originarse en el entorno criminal, han sido aprovechados por este para la realización de comportamientos prohibidos. Por lo cual, el principal cambio mundial, sin lugar a dudas, es el fenómeno de la

globalización y el portentoso desarrollo y generalización de su principal instrumento: las tecnologías de la información y de la comunicación (TIC)".

De acuerdo con la tesis que plantea Narváez (2018), podemos afirmar que, "es preferible optar por una perspectiva amplia, que incluya tanto a las tecnologías de la comunicación (principalmente la radio, la televisión y la telefonía en todas sus formas) como a las tecnologías de la información, vinculadas principalmente con la informática, los ordenadores y las redes que permiten el rápido flujo de esa información, principalmente, la Internet; por lo que, resultaría más acertado utilizar la expresión TIC para referirse a ellas". Está claro que, desde el punto de vista tecnológico y jurídico, el termino más adecuado y que engloba a toda esta problemática, es Tecnología de la Información y Comunicación.

Finalmente, de acuerdo con los postulados de Sequeiros (2016) compartimos el argumento que, "en nuestro ordenamiento jurídico, la Ley N.° 30096 no se ha decantado por una u otra alternativa, posibilitando así que se le atribuya unos alcances muy amplios (la telefonía fija, el móvil, la radio y la televisión, la informática y los ordenadores, la videoconferencia, los SMS, la Internet, entre otros); por lo que ,consideramos que hubiese sido preferible que la mencionada Ley ofrezca algunos alcances sobre lo que ha de entenderse por tecnologías de la información o de la comunicación", pero lamentablemente aún no se ha dado ese paso jurídico tan esperado.

Conclusiones

Como hemos podido advertir en todo el desarrollo del presente trabajo de investigación que, tanto la dogmática como la jurisprudencia nos señalan que el fin de la Ley Nº 30096, Ley de Delitos Informáticos, es la prevención y la sanción de actos no lícitos que atentan contra la base de datos y la información secreta de personas naturales y jurídicas.

Por otro lado, conforme afirma Chávez (2018), "la figura penal de acceso ilícito, regulada en el artículo 2 de la referida Ley, se clasifica como un delito de mera actividad, porque en este ilícito el delito queda consumado en el mismo acto de vulnerar las medidas de seguridad de un sistema informático". Es decir, que nuestra legislación peruana tiene una agenda pendiente, respecto a la configuración de los delitos informáticos.

Asimismo, continúa nuestro autor señalando que, "la figura penal de atentado contra la integridad de datos informáticos, regulada en el artículo 3, se clasifica como un delito de mera actividad, porque en este ilícito el delito queda consumado en el mismo acto de introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible los datos informáticos". Esto hace suponer que aún existen vacíos legales urgentes por subsanar.

Ciertamente, es preocupante la alarmante desprotección que se vislumbra cuando nos encontramos ante este ilícito penal que atenta contra nuestros niños y adolescentes. Ante esta realidad, subyace una laxitud imperante de la ley y un clamor desesperado por la tutela de nuestros derechos fundamentales.

Finalmente, como es de conocimiento público, lo más común y lo que más se ha incrementado en estos dos años de pandemia, según las estadísticas, son los delitos de fraude informático. Sin

embargo, los hechos ilícitos están latentes pero las normas actuales no favorecen para hacerles frente. Concluyendo sin lugar a dudas que, existen vacíos legales que respondan a la coyuntura actual que viene atravesando nuestra sociedad peruana y especialmente en el ámbito de nuestra capital de Lima Metropolitana.

Aporte de la Investigación

Efectivamente, después de todo lo expresado, estamos seguros en afirmar que nuestro trabajo de investigación tiene el fin de contribuir e incentivar a un estudio mucho más profundo desde la dogmática jurídica y la jurisprudencia para encontrar caminos muchos más claros y viables que estén acordes al contexto social en que nos encontramos y la justicia llegue de manera oportuna a nuestros ciudadanos.

Efectivamente, nos queda claro que, principalmente el reto queda en el campo de los legisladores y de los más altos operadores la justicia en nuestro país, para que puedan hacer las reformas correspondientes y no sigamos contemplando cómo la delincuencia nos sigue avasallando sin piedad.

Finalmente, nuestro principal objetivo en este trabajo está directamente orientado a brindar un aporte a labor que desarrollan los docentes en las aulas universitarias en materia de derecho y para todos los operadores de la justicia en nuestro país, incluyendo a nuestro legisladores, desarrollen actividades académicas, deliberativas y de análisis respecto a la normatividad relacionada con los delitos informáticos y de este modo se actualice y contribuya a la solución de los problemas sociales que hoy afecta a nuestra sociedad.

Recomendaciones

Finalmente, después de auscultar la realidad de nuestro país y nuestra ciudad de Lima Metropolitana, nos atrevemos a instar a nuestras autoridades gubernamentales, par que depongan sus interese particulares y observen con detenimiento las necesidades más urgentes de nuestra sociedad y a través de sus órganos competentes se realicen las modificaciones y actualizaciones necesarias de nuestra legislación peruana en lo concerniente a los delitos informáticos.

Asimismo, es indispensable que se continúe implementando los espacios de formación permanente, actualizada y sofisticada al personal que está a cargo de velar por la seguridad y la aplicación de la justica en nuestro país.

Del mismo modo, es imperante que la formación preventiva y profunda llegue a todos los ciudadanos, debiendo recibir una formación ciudadana donde sea consciente de sus derechos y deberes que la Constitución y las leyes le amparan.

Finalmente, en consonancia con Chávez (2018), “se debe capacitar al personal y a todos los operadores que hacen lucha frontal a estos delitos, para que de esta forma no se vulneren todo tipo de medios de prueba que puedan servir como material idóneo para contrarrestar este tipo de delitos”.

Referencias Bibliográficas

Chávez, E. (2018). *El delito contra datos y sistemas de información en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2018.* Lima, Perú. Universidad Nacional Federico Villareal.

Chilcon, M. (2020). *El Ciber Crimen en el Perú y su incidencia en la Seguridad Nacional.* Lima, Perú. Centro de Altos Estudios Nacionales.

Echevarría, G. (2015). *Delitos Informáticos y el Derecho Constitucional a la seguridad pública*. Ambato, Ecuador: Universidad Técnica de Ambato.

Fayos, A. (2016). *Los Derechos a la Intimidad y a la privacidad en el siglo XXI.* Madrid, España: Editorial Dykinson; ISBN: 977-84-9086-240-8.

Ley N° 30171. (2015). *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. Lima, Perú: https://cdn.www.gob.pe/uploads/document/file/200326/197055_Ley30171.pdf20180926-32492-1l0lzim.pdf.

Maldonado, M. (2014). *El Delito Informático, vulnera el principio de la garantía constitucional y legal, sobre el honor de las personas establecidos en la constitución de la república*. Loja, Ecuador: Universidad Nacional de Loja.

Maldonado, E. (2015). *Los Delitos Informáticos y el Derecho Constitucional a la Seguridad Jurídica*. Babahoyo, Ecuador: Universidad Regional Autónoma de Los Andes.

Ministerio del Interior. (2017). *Ciber Policías contra los Delitos Informáticos*. Lima, Perú: Oficina de Comunicación Social.

Narváez, B., & Recalde, G. (2018). *El Delito Informático en América*. Quito, Ecuador. UNIANDES Revista Jurídica Vol. 1 N° 2.

Posso, D. (2015). *Los Delitos informáticos y la violación de los derechos constitucionales del ofendido*. Ambato, Ecuador: Universidad Técnica de Ambato.

Rendon, D. (2012). La eficacia de la prueba digital en el proceso penal colombiano. Medellín, Colombia: Universidad de Medellín.

Ruiz, C. (2017). *Análisis de los Delitos Informáticos y su violación de los derechos constitucionales de los ciudadanos*. Loja, Ecuador: Universidad Nacional de Loja.

Sequeiros, I. (2016). *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano - 2016*. Huánuco, Perú. Universidad de Huánuco.

Velástegui Córdova, M. E. (2019). Los Delitos Informáticos y su incidencia en la provincia de Pastaza. *Revista digital de ciencias jurídicas de UNIANDES,* 46-50.

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS* N° 48, 283-304.

Zorrilla, K. (2018). *Inconsistencias y ambigüedades en la Ley de delitos informáticos ley N° 30096 y su modificatoria Ley N° 30171, que imposibilitan su eficaz cumplimiento*. Huaraz, Perú: Universidad Nacional de Ancash "Santiago Antiguos de Mayolo".