Apreciación jurídica del Análisis de Tráfico en el contexto informático venezolano

Una propuesta legal a la violación virtual de la Privacidad

Legal appreciation of Traffic Analysis in the venezuelan informatic context

A Legal proposal to virtual violation of Privacy

Daniel A. Quintero R.
Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)
dquintero@cenditel.gob.ve

Fecha de recepción: 10/09/2020
Fecha de aceptación: 15/10/2020
Pág: 2- 23

Resumen

Se presenta un estudio sobre el análisis de tráfico en Venezuela, aplicación informática que posibilita el establecimiento de las rutinas, tendencias e intereses de una persona o grupo, nutriéndose de las denominadas inferencias, con las que se infringe el derecho a la privacidad. Partiendo de la conjugación de los aspectos técnicos con los principios teóricos, se presentará una propuesta sustentada en la Teoría del Delito para enmarcar el análisis de tráfico como una acción típica, antijurídica y culpable, buscando una reformulación en primera instancia del artículo 21 de la Ley Especial contra los Delitos Informáticos (LECDI), que debe complementarse con decisiones estratégicas dentro de la Ley de Infogobierno, para procurar en el futuro un Subsistema de Anonimato.

Palabras Clave: análisis de tráfico, inferencias, delito, privacidad, anonimato.

Abstract

A study is presented on the traffic analysis in Venezuela, a computer application that enables the establishment of routines, tendencies and interests of a person or group, drawing on so-called inferences, with which the right to privacy is infringed. Starting from the conjugation of the technical aspects with the theoretical principles, a proposal based on the Theory of Crime will be presented to frame the traffic analysis as a typical, unlawful and guilty action, seeking a reformulation in the first instance of article 21 of the Law Special Against Computer Crimes (LECDI), which

must be complemented with strategic decisions within the Infogvernment Law, to ensure in the future an Anonymity Subsystem.

Keywords: traffic analysis, inferences, crime, privacy, anonymity.

En realidad, lo más importante no es la tecnología sino la capacidad de los ciudadanos para afirmar su derecho a la libre expresión y a la privacidad de la comunicación. Si las leyes de control y vigilancia sobre Internet y mediante Internet son aprobadas por una clase política que sabe que el control de la información ha sido siempre, en la historia, la base del poder, las barricadas de la libertad se construirán tecnológicamente.

Manuel Castells
[Castells, 2003]

Introducción

El predominio contemporáneo, de los sistemas informáticos en las actividades que desarrolla el ser humano, ha propiciado avances pero también dependencia, control y abusos, en palabras de Moncalvo (2007): *La evolución sofisticada de la red y su capacidad de adaptación a los diversos usos y exigencias contribuyó a que sus beneficios alcanzaran niveles masivos* [Moncalvo, 2007, p.12]. Aunado a esto, los actos que atentaban contra los derechos ciudadanos, se expandieron rápidamente en el ciberespacio, representando un viraje a la lógica decimonónica del delito.

Así pues, este enraizamiento físico/virtual, constituye un aliciente para tomar como centro de indagación el análisis de tráfico, en donde la cohabitación de la población con las redes digitales, es explotada para invadir su privacidad, precisando De Terwangne (2012):

> Cuando pensamos en la privacidad en Internet, la palabra privacidad no se debe interpretar como intimidad o secretismo. Más bien se refiere a otra dimensión de la privacidad, es decir, a la autonomía individual, la capacidad de elegir, de tomar decisiones informadas, en otras palabras, a mantener el control sobre diferentes aspectos de nuestra propia vida. [De Terwangne, 2012, p. 54]

En consonancia con lo anterior, la línea lógica de disertación llevará a observar la privacidad como derecho, en donde se concentra la matriz generadora de la trasgresión legal. Es así, como al materializarse una acción o acto que tiene un Objeto Material y un Objeto Jurídico, se amerita de una articulación penal, explica Zaffaroni (1999): *...la analítica considera al delito como una estructura, en que la tipicidad impone ciertas modalidades a la antijuridicidad y a la culpabilidad y, por ende, ambas tienen que estar sometidas a ella en este sentido* [Zaffaroni, 1999, p. 32]. De este modo, la teoría ensambla: la acción típica, antijurídica y culpable, que guiarán la propuesta para amoldar el análisis de tráfico como delito, Mejía (1979) apoyándose en Roxin (1972) amplía:

> *las concretas categorías del delito —tipicidad, antijuridicidad y culpabilidad— deben sistematizarse y contemplarse desde un principio bajo el prisma de su función políticocriminal*, a cuyo respecto señala que la función del tipo consiste en dar cumplimiento al principio de legalidad, la de la antijuridicidad en dar solución a los conflictos que se suscitan en el seno de la sociedad, y la de la culpabilidad resulta acuñada por los fines de la pena. [Mejía, 1979, p. 34]

Por tanto, este abordaje investigativo estudiará el análisis de tráfico de datos informáticos desde una percepción integral, que permita la comprensión de un hecho que tiene una afectación social, empero, no cuenta con una tipificación en el marco de la ley, no siendo posible su punibilidad en el contexto normativo actual. Es de resaltar, que este artículo tomó referencialmente el estudio titulado: *Consideración Legal y Criminalística del Análisis de Tráfico en las Tecnologías de Información y Comunicación en Venezuela enmarcados en la Privacidad*, el cual fue efectuado entre los años 2014 y 2015, bajo la modalidad investigativa del *Proyecto Factible*, se detalla en Arias (2012):

> (...) consiste en la elaboración de una propuesta de un modelo operativo viable, o una solución posible a un problema de tipo práctico, para satisfacer necesidades de una institución o grupo social. La propuesta debe tener apoyo, en una investigación de campo, o en una investigación documental; y puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. [Arias, 2012, p. 32-33]

En atención a lo puntualizado, el mencionado trabajo conjugó la experimentación técnica, la revisión documental y la fundamentación teórica, para erigir una propuesta legal. De tal manera, en el presente texto se sintetizan y actualizan un conjunto de contenidos al año 2020, que se desarrollan a continuación.

Aspectos teóricos sobre el Análisis de Tráfico

Inicialmente, se debe señalar que el encasillar una utilidad informática *per se* como un peligro no es sencillo, habida cuenta que su usabilidad varía de lo neutro a lo amenazante según los fines que pretenda el ejecutor, siendo herramientas bipolares que incluso contrarrestan posibles agresiones por medios informáticos a infraestructuras críticas, [Wright et al., 2009] detallan:

> El análisis del tráfico de la red es uno de los medios cada vez más comunes para la identificación de las amenazas de seguridad y proporcionar una gestión eficiente de los recursos de la red, tanto dentro de las redes locales e Internet. Desafortunadamente, estas mismas técnicas de análisis a menudo conducen a violaciones de la privacidad del usuario. [Wright et al., 2009, p. 1]

Conforme a lo precitado, la dualidad del análisis de tráfico evidencia usos no intrusivos, aunque se advierte que también tiene aplicabilidades que pueden afectar el derecho a la privacidad, pero se encuentra sin ser debidamente estudiada jurídicamente. Esta técnica, se apoya informáticamente en los llamados *sniffer*, Avast (2020) especifica lo siguiente:

ISSN: 2244-7423

> No todos son malos. En muchas ocasiones, los administradores utilizan estas herramientas para mantener un flujo constante de tráfico en sus redes. No solo las personas bien intencionadas utilizan los *sniffers* de red. Los ciberdelincuentes pueden pinchar una red para ver todo el tráfico que se envía a través de la misma. Al supervisar el uso de Internet, incluyendo los correos electrónicos y los mensajes instantáneos, un hacker podría acceder a las credenciales de inicio de sesión, información privilegiada y datos financieros. Por eso los *sniffers* son tan peligrosos en manos equivocadas. [Avast, 2020]

Tomando como referencia, lo que explica la firma checa de software, entonces el *sniffers* tiene una operatividad importante en el desarrollo de la extracción de los datos, aplicando lo que develan Cole, et al. (2005) *El análisis de tráfico es la capacidad del sniffer para romper los campos relevantes (como la dirección IP) de los paquetes capturados. Un sniffer con buena capacidad de análisis de tráfico puede mostrar fácilmente campos especificados dentro del paquete* [Cole et al., 2005, p. 128].

Es así, como se empieza a configurar imperceptiblemente una vulneración de los datos personales, que usa métodos subrepticios para ir interceptando la comunicación entre el emisor-receptor, pudiendo inferir el relacionamiento del intercambio, admiten Das, et al., (2012) que: *El atacante simplemente escucha la comunicación de redes, para llevar a cabo el análisis de tráfico, para determinar la ubicación de los nodos claves, la estructura de enrutamiento, e incluso los patrones de comportamiento de la aplicación* [Das et al., 2012, p. 253]. En algunos casos, se puede trascender la observación, pretendiendo la captura el desciframiento de los datos contenidos en el tráfico, Qadeer (2010) añaden que:

> El sniffer captura estos paquetes mediante el establecimiento de la tarjeta NIC en modo promiscuo y, finalmente, los decodifica. La información descodificada se puede utilizar en cualquier forma dependiendo de la intención de la persona que trate de decodificar los datos (es decir propósito malicioso o beneficioso).[Qadeer et al., 2010, p. 311]

Conviene subrayar, que la problemática se ha intentado atender con métodos criptográficos para dificultar al intruso el desciframiento, que resulta una medida importante pero no la solución, Fu et al., (2003) argumentan: *Es bien sabido que incluso si el contenido de los paquetes se ha cifrado, las características del tráfico, tales como tasas de tráfico, patrón o densidad, pueden revelar importante información esencial acerca de las aplicaciones* [Fu et al., 2003, p. 1]. Por ello, para un analista de tráfico la simple información como el tiempo y duración, resultan ser valiosas para hacer las inferencias[1], pudiendo determinar con bastante certeza: identidades y ubicación. Además, un seguimiento paciente y detallado de los mensajes cifrados conduce a conclusiones interesantes, mencionan Back et al., (2001) que:

[1]Nota del Autor: Conforme al Diccionario Digital de Nuevas Formas de Lectura y Escritura (2020): en lógica [para las consideraciones de la investigación sobre análisis de tráfico este concepto es acertado], el término inferencia designa el hecho de que, en una relación entre dos proposiciones, la primera contiene una implicación y la segunda una consecuencia. [Red de Universidades Lectoras, 2020]

> Un fisgón que intercepta sólo los mensajes cifrados entre el usuario y el primer nodo de la cadena, así como los mensajes de texto no cifrado entre el nodo final y el servidor web puede asociar los datos cifrados con el texto usando la longitud de datos y el tiempo de transmisión. [Back et al., 2001, p. 3]

Dicho de otro modo, el análisis de tráfico da pie para que la minuciosidad o generalidad que se apliquen violenten igualmente a la privacidad, ya que incluso desde datos ambiguos se puede captar información de interés, concuerdan Danezis y Clayton (2007): *Los datos pueden ser imprecisos o incompletos – pero simplemente sabiendo los patrones de comunicación 'típicos' se puede inferir información acerca de una comunicación particular que se ha observado* [Danezis y Clayton, 2007, p. 1]. Entonces, la obtención de las fuentes para efectuar los análisis de tráfico es variada, pudiendo aprovecharse tanto las redes inalámbricas como alámbricas, para proceder a realizar la observación y revisión, confirman Guan, et al., 1999:

> La información sobre la densidad del tráfico se puede obtener fácilmente en entornos inalámbricos mediante la observación de las fuentes de frecuencia de radio. En las redes de cable, esto se puede hacer colocando correctamente el analizador de paquetes, mediante el uso de herramientas de gestión de redes comerciales, o por otros medios. [Guan et al., 1999, p. 744]

Lo anteriormente expuesto, presenta un campo de acción considerable que no encuentra más restricciones que las capacidades técnicas del intruso para la extracción de la información, de forma amplia se podría hacer referencia a dos tipos de análisis de tráfico, que persiguen un mismo objetivo pero con diferente nivel de prolijidad, Murdoch y Zieliński (2007) mencionan:

> El primero trata el anonimato en la red como una çaja negraz sólo inspecciona el tráfico que entran y sale de la red. El segundo enfoque además analiza las corrientes dentro de la red, y por lo tanto mejora la precisión de los ataques.[Murdoch y Zieliński, 2007, p.7]

Por esta razón, el plano técnico ha tomado la delantera ante la displicencia legislativa, surgiendo algunas medidas para frenar el problema del análisis de tráfico con el apoyo del llamado: *anonimato informático*, que ha tenido serias dificultades para su aceptación debido al carácter claroscuro del término que pareciera ligarse con una ocultación sospechosa del usuario, Danezis (2004) aclara:

> Las comunicaciones anónimas son estudiadas en el contexto de la seguridad informática, ya que están teniendo lugar en un contexto adverso. El actor intenta proteger su anonimato vis-a-vis respecto a otras partes que tratan de descubrir los vínculos ocultos. Esta información tiene algún valor para los que realizan la vigilancia e implicaría algún coste para el sujeto si fuera revelada. [Danezis, 2004, p. 19]

De este modo, la referida propuesta se perfila como uno de los mecanismos ante el uso irrestricto de métodos que afectan el derecho a la privacidad. Aunque, el anonimato es una

alternativa técnica no sólo muestra un camino para amilanar una amenaza, tiene también el potencial de atender sistémicamente el problema, Sumoza (2008) sugiere:

> Por otro lado el anonimato además de estar relacionado al conjunto anónimo y al tiempo en el que se está ejecutando la acción, también tiene relación al contexto donde se aplica, es decir, un sujeto puede ser anónimo en relación al contexto envío y recepción de correos electrónicos, pero puede no serlo en ese mismo instante de tiempo para el contexto interacción con una base de datos. [Sumoza, 2008, p.8]

Vinculado al concepto previo, para palear el alto nivel de exposición de los datos que fluyen a través de las plataformas informáticas, se procura que los sistemas anónimos alcancen la no observancia de la Red, Raymond (2001) recomienda: *... esconder todos los modelos de comunicación (cuántos, en qué momento y a quién los mensajes son enviados y recibidos). Nótese que la no observancia de la Red implica la ineficacia del análisis de tráfico* [Raymond, 2001, p.2]. En otras palabras, los mecanismos para lograr la *no observancia de la red*, conllevan la puesta en marcha de un engranaje anti-tráfico (pro anonimato) que imposibilite el seguimiento a los paquetes transmitidos, algunas premisas del mismo son esgrimidas en Deng et al. (2004):

- Que un intruso no pueda determinar un destino de paquetes por inspeccionar el contenido del mismo.
- Que un intruso no pueda encontrar la dirección del flujo de datos mediante el análisis de la correlación de tiempo entre los paquetes enviados por los nodos secundarios y paquetes enviados por sus nodos principales.
- Que un intruso no pueda encontrar la dirección de transmisión de datos, haciendo el análisis estadístico de la tasa de transmisión de paquetes de cada nodo dentro de su rango. [Deng et al., 2004, p. 6]

En líneas generales, mientras se mantenga la interrelación de los factores del sistema anónimo se conseguirá la robustez técnica, pero cada pieza debe ser correctamente engranada, ya que el atacante siempre intentará aplicar argucias informáticas para extraer la información y poder efectuar sus inferencias. En síntesis, el carácter integral del conjunto anónimo se enlaza a cuatro grandes premisas que deben tener una relación armónica, arguyendo Sumoza (2008):

> En el estudio de los sistemas anónimos, la no relacionabilidad sólo tiene sentido práctico si previamente se han definido las propiedades del anonimato, seudonimato y no-observabilidad de dichos sistemas, y se han caracterizado las entidades o ítems de interés que se desean relacionar (por parte del atacante). [Sumoza, 2008, p. 9]

Ejercicio Técnico con Herramientas para el Análisis de Tráfico

Con el fin de ilustrar la capacidad de las aplicaciones informáticas para el análisis de tráfico, se efectuó un ejercicio **en un entorno de prueba controlado para no afectar la privacidad**

de ninguna persona o institución, aplicando *software* especializado para constatar los datos que pueden ser obtenidos. En una fase preliminar, se evaluaron las herramientas que podían ser aplicadas, siendo la decisión final el hacer uso articulado de *interfaces* desarrolladas para el análisis de tráfico[2]. Por consiguiente, la captura del tráfico de las comunicaciones se realizó en un periodo de cuatro (04) días, lográndose obtener un millón siete mil trescientos cincuenta y ocho (1.007.358) datos y/o paquetes, presentando todo tipo de información desde la más general hasta detalles concretos (Ver figura 1).

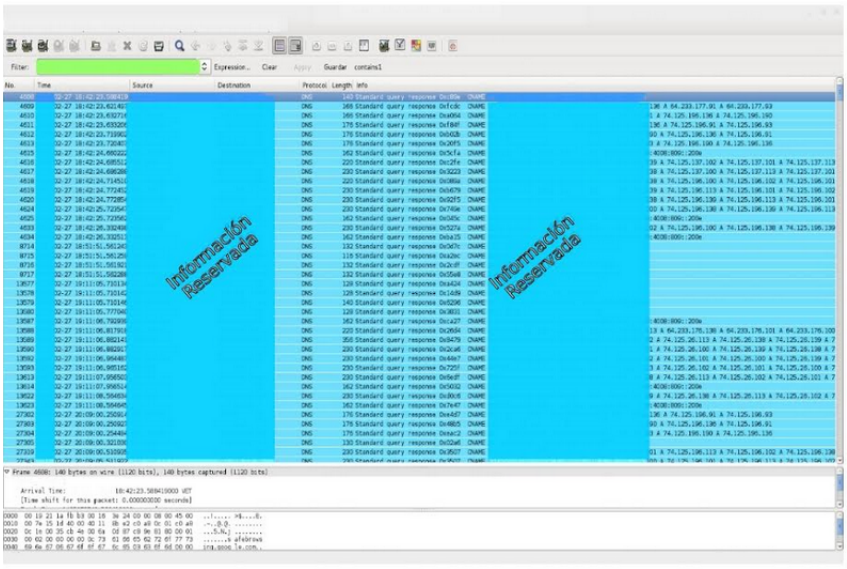

Figura 1: Captura general de paquetes
Fuente: tomado de uno de los sistemas informáticos de análisis de tráfico utilizados en el ejercicio.

En una segunda parte, con el uso combinado de una biblioteca de captura de paquetes, más una aplicación configurada en modo *sniffer* y un *software* de inspección profunda para filtrar los datos, se alcanzó la administración y procesamiento del grueso de los archivos obtenidos con relativa sencillez. Es así, como se encontraron casi dos mil paquetes con datos que permitieron hacer inferencias sobre los gustos, necesidades, prioridades e intereses, que en definitiva son el centro de atención de un analista de tráfico.

Aunado a lo reseñado, en la exploración más directa se contaba con filtros adaptables, permitiendo una búsqueda minuciosa de sistemas de correo, redes sociales o portales web,

[2]Nota del Autor: se reserva la enunciación de las interfaces, programas, suites y software utilizados, así como algunos datos para no facilitar prácticas que permitan acciones que puedan afectar la privacidad. Se debe hacer mención, que el ejercicio técnico fue supervisado y monitoreado por un (01) experto del área informática del Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL). Concluido el mismo, se efectuó un examen exhaustivo de los resultados por parte de tres (03) ingenieros de la misma institución con conocimientos en la materia, que mediante una Matriz de Validación evaluaron la aplicación de las herramientas, procesamiento de los datos y productos obtenidos.

lográndose divisar en el entorno de la Red *sniffeada*: direcciones IP, conexiones telefónicas, servicios de chat y el uso compartido de paquetes, insumos que son fundamentales para poder triangular rutinas o tendencias en una persona.

Finalmente, el análisis del protocolo TCP (uno de los más usados en internet) dejó aspectos relevantes en la captura, posibilitando el contemplar y extraer datos vinculados a las actualizaciones del sistema operativo, ubicándose además el uso de una dirección de correo institucional con especificaciones del gestor de correo.

En tal sentido, hay relevancias técnico/jurídicas en cuanto a los resultados obtenidos del ejercicio, en el caso de las técnicas ya se habían detallado en los *Aspectos teóricos sobre el Análisis de Tráfico* lo amenazante del uso irrestricto de la herramienta, mostrando la práctica en el entorno de prueba controlado la certeza de lo explicado ut supra. Para asimilar las diversas variables expresadas, se presenta un cuadro que sintetiza la acción tecnológica en relación al derecho protegido:

Tabla 1: El Análisis de Tráfico y su Afectación a la Privacidad

Información extraída al voluntario en el entorno de prueba controlado durante cuatro (04)días	**Posibles inferencias del Analista**	**Viola el derecho a la privacidad**
1.007.358 paquetes generales.	Se puede hacer todo un mapeo de los relacionamientos y hábitos del usuario siguiendo los cruces de las IP.	Sí
1.826 paquetes específicos.	Al saber los tipos de comunicaciones, su frecuencia, origen y destino se facilita el perfilamiento del usuario.	Sí
Se obtuvieron datos de actividades realizadas en un servicio de chat, dinámicas de sesiones en redes sociales y gestión de archivos en línea.	Se reconocieron tres proveedores de servicios informáticos privados que amplían las opciones para caracterizar las rutinas digitales del usuario.	Sí
Se identificó el tipo de sistema operativo. Además se detectó el gestor de correo utilizado y las especificaciones de un usuario institucional.	Las particularidades técnicas de los *software* que utiliza el usuario para gestionar sus actividades en línea, aportaron inferencias importantes sobre su rutina laboral.	Sí

Fuente: Cuadro elaborado por el autor de la investigación.

Fundamentación Jurídica de la Propuesta

Asumiendo la exposición teórica y la praxis técnica como fundamentos para sustentar la propuesta en el ámbito legislativo, se procede a encauzar la conceptualización jurídica. Partamos con el Código Penal (2005), en la primera parte del Artículo 1 indica: *Nadie podrá ser castigado por un hecho que no estuviere expresamente previsto como punible por la ley, ni con penas que ella no hubiere establecido previamente* [Código Penal, 2005, p. 1]. Las expresiones de la norma sustantiva, es lo que se conoce como el Principio de Legalidad en materia penal, denotándose en lo que respecta al análisis de tráfico la necesidad de una ingeniería jurídica que permita cubrir la totalidad de aspectos como: acción típica, antijurídica y culpable en la norma especial, ya que en estos momentos aplica el aforismo: *Nullum crimen, nulla poena sine praevia* lege[3]

Sin duda, la viabilidad de una propuesta emana de la posibilidad de llevarla a cabo. En estos momentos, el vacío legal en relación al análisis de tráfico es proporcional a la amenaza sobre la privacidad, lo que exterioriza una necesidad legal y una problemática por solventar. Como se expone en la presente investigación, hay una posibilidad concreta de resolución y satisfacción mediante un ejercicio de hermenéutica jurídica:

- Para iniciar, hay que efectuar la interpretación legal de los resultados técnicos, intentando presentar una propuesta de acción (acto) que traduzca el proceder informático (análisis de tráfico) en una descripción de conducta que pueda enmarcarse dentro de un tipo penal. En virtud de esto, el hecho informático sobre el cual se respalda el infractor y que lesiona un derecho, debe contenerse en una legislación que lo describa e incrimine.[4]
- Seguidamente, basados en la lógica jurídica hay que determinar los elementos propios de la antijuridicidad del análisis de tráfico. En este punto, se entrelaza la acción del sujeto activo con un principio normativo (no necesariamente penal) para apreciar nítidamente lo que es contrario al derecho: ante la violación a los datos informáticos personales, íntimos, no públicos (por vía del análisis de tráfico) se trastoca un bien jurídico protegido constitucionalmente como la privacidad.
- En el último eslabón, se deben determinar los presupuestos de la culpabilidad del infractor para establecer la capacidad del sujeto activo de ser punible por una acción típica y antijurídica (el análisis de tráfico).

Elementos Legales de la Propuesta

Con respecto a las normas venezolanas, la privacidad [digital] es abordada por el constituyente de manera indubitable en el último párrafo del artículo 60 de la

[3]Nota del Autor: esta máxima jurídica fue creación de Paul Johann Anselm Von Feuerbach, incluida en su: Tratado de Derecho Penal común vigente en Alemania (1801), pudiendo traducirse del latín como: No hay delito, ni hay pena sin ley.

[4]Nota del Autor: No basta con redactar un tipo penal clásico, como mínimo se deben tomar como referencia las orientaciones jurídicas y técnicas del Convenio de Budapest Sobre La Ciberdelincuencia. Precisamente este documento tiene importantes aportes sobre el llamado *tráfico informático* [Consejo de Europa, 2001].

Constitución de la República Bolivariana de Venezuela (2009) quedando instituido: *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos* [Constitución de la República Bolivariana de Venezuela, 2009, p. 16]. A pesar que el lineamiento constitucional es contundente sobre la protección de este derecho, esto no ha sido desarrollado plenamente en los textos que subsecuentemente han sido aprobados para atender la privacidad en el ciberespacio.

Un caso latente, lo encarnaría la Ley Especial contra los Delitos Informáticos (2001), sorprendiendo que hay dieciséis (16) definiciones introductorias en el artículo 2, pero ninguna hace referencia a la privacidad informática. A lo largo de toda la normativa, la palabra *privacidad* es usada solamente en tres ocasiones, una dentro del título del capítulo III y las otras en los artículos 20 y 21. Empecemos por revisar el artículo 20 de la LECDI, que versa sobre la Violación de la Privacidad de la Data o Información de Carácter Personal, se puede leer:

> Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero. [Ley Especial contra delitos Informáticos, 2001, p.5]

En relación a lo destacado en el precepto citado, los llamados contratos de adhesión electrónicos contentivos de parámetros extraterritoriales, suelen amarrar legalmente al usuario de una plataforma digital, siendo una de las vías para menguar la privacidad informática. En efecto, producto del desconocimiento jurídico las personas *ceden* sus datos a terceros, diluyendo la salvaguarda del Estado por una inducida *buena pro*[5]. Por tanto, relativizado el consentimiento del *Sujeto Pasivo*, el Objeto Jurídico lesionado se difumina, en resumidas cuentas la redacción del artículo vigésimo dificulta la cobertura estatal para proteger efectivamente la privacidad informática, abriéndose la posibilidad para el desempeño sin límites de técnicas como el análisis de tráfico.

Seguidamente, se encuentra el artículo 21 que toca lo relativo a la Violación de la Privacidad de las Comunicaciones, que debería ser la *piedra angular* para neutralizar los abusos que se comenten por intermedio de los dispositivos computacionales, conteniendo las siguientes precisiones:

[5]Nota del Autor: hay que llamar la atención, que en lo atinente a los contratos de adhesión, encontraremos que de forma amplia y no dirigido al ámbito digital es la Ley Orgánica de Precios Justos (2015), en el numeral décimo del artículo 7 donde se indica el derecho de los ciudadanos: *A la protección en los contratos de adhesión que sean desventajosos o lesionen sus derechos o intereses* [Ley Orgánica de Precios Justos, 2015, p.p. 14-15].

> Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. [Ley Especial contra delitos Informáticos, 2001, p.p. 5-6]

De manera similar al artículo 20, lo dispuesto en el vigésimo primero no blinda la privacidad informática, en vista que ninguna de las acciones que describe: *acceda*, *capture*, *intercepte*, *interfiera*, *reproduzca*, *modifique*, *desvíe* o *elimine*, explica concretamente la gama de actos que se acometen con el análisis de tráfico.

Así pues, las claves para destrabar esta inatención legislativa podría ser una mixtura que atienda las falencias legales detectadas en los dos artículos o apuntalando uno. Se considera que robusteciendo el artículo 21, mejoraría radicalmente las debilidades que se han conseguido, se pasa a enunciar diez líneas para reforzarlo:

- **I-** Inclusión en la descripción de la Acción (Acto) 1: *analice*.
- **II-** Adición en el Objeto Material del Delito: *tráfico de paquetes*.
- **III-** Adjuntar en la redacción de la Acción (Acto) 2: *efectúe inferencias, perfilamientos o sintetice información ajena.*
- **IV-** Complementar el Sujeto Pasivo con: *persona natural o jurídica.*
- **V-** Remarcar el Sujeto Activo con: *la persona natural o jurídica venezolana o extranjera.*
- **VI-** Atender el consentimiento con: *sin la autorización debidamente suscrita por la persona natural o jurídica a la que pertenecen de conformidad a las leyes contractuales venezolanas.*
- **VII-** Clarificar un Objeto Jurídico del Delito: *la privacidad informática.*
- **VIII-** Aumentar la punibilidad con: *prisión de cuatro a ocho años.*
- **IX-** Cambiar unidades tributarias por el criptoactivo venezolano: *multa de un mil a dos mil Petros.*
- **X-** Agregar indemnizaciones para el afectado: *por un monto no menor a la cifra máxima de la multa.*

Con lo anteriormente expuesto, se logran conjugar más armónicamente la tipicidad, la antijuridicidad y la culpabilidad[6], intentando evitar cabos sueltos. Del mismo modo, se

[6]En relación a los tres conceptos, los catedráticos venezolanos Grisanti, H., y Grisanti, A. (2006) los esquematizan dentro del llamado delito singular, afirmando sobre la tipicidad que: *es un elemento del delito que implica una relación de perfecta adecuación, de total conformidad, entre un acto de la vida real y un tipo penal* [Grisanti y Grisanti, 2006, p. 11]. Posteriormente, explican la antijuricidad en estos términos: *es un elemento del delito que entraña una relación de contradicción o contraste entre un acto de la vida real y las normas objetivas del Derecho Positivo vigente.* [Grisanti y Grisanti, 2006, p. 11]. Finalmente, para ellos, la culpabilidad: *es el conjunto de presupuestos que fundamentan la reprochabilidad personal del acto típicamente antijurídico.*[Grisanti y Grisanti, 2006, p. 12]

ISSN: 2244-7423

determinan de mejor manera los sujetos del delito, particularmente el activo que se adapta a la dinámica extraterritorial de las transnacionales o los actores extranjeros. En lo vinculado al consentimiento, se busca clarificar la temática de los contratos de adhesión electrónicos al hacer obligante que la autorización sea según las normas que apliquen en el territorio nacional. En el mismo sentido, ante lo delicado del bien que se protege es necesario la imposición de sanciones más representativas que disuadan a los posibles infractores, añadiéndose dos años a la pena mínima y máxima. Sobre el peso impositivo, la legislación especial debe referenciar sus multas en *criptoactivos* y hacer vinculante la garantía de indemnización del afectado, pudiendo quedar el artículo de la siguiente manera:

> **La persona natural o jurídica venezolana o extranjera**, que mediante el uso de tecnologías de información: acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe, elimine, o **analice**, cualquier: mensaje de datos, señal de transmisión, comunicación, **tráfico de paquete**s, o **efectúe inferencias, perfilamientos o sintetice información ajena desde éstos para fines particulares o comerciales, sin la autorización debidamente suscrita por la persona natural o jurídica a la que pertenecen de conformidad a las leyes contractuales venezolanas, violando su privacidad informática**, será sancionada con prisión de **cuatro a ocho años**, multa de un **mil a dos mil Petros (1000 a 2000 Petros) e indemnización para el afectado por un monto no menor a la cifra máxima de la multa.** (Ver Figura 2)

Figura 2: Propuesta de Penalización del Análisis de Tráfico: artículo 21 LECDI
Fuente: propuesta elaborada por el autor de la investigación.

Análisis de Factibilidad de la Propuesta

Resulta de importancia indicar que existen varias dimensiones para poder evaluar un proyecto normativo en el ámbito informático, que en general se asocian a su factibilidad: Social, Legislativa, Tecnológica/Temporal y Estratégica, todas ellas necesarias para examinar los objetivos y fines que se plantean.

Factibilidad Social: la aplicabilidad de una norma, debe ser concomitante con una necesidad de la ciudadanía. En este sentido, si se toma como referencia el reporte del segundo trimestre del año 2019 de la Comisión Nacional de Telecomunicaciones (CONATEL), el cual estima que dentro de la población de siete (07) años en adelante por cada cien (100) habitantes, cincuenta y nueve (59) utilizan el servicio de la Internet, con una cifra de usuarios en el país que se ubica en dieciséis millones setecientos treinta y tres mil cuatrocientos ochenta y siete personas (16.733.487) [CONATEL, 2019], se puede deducir que en Venezuela la magnitud de la vulnerabilidad ante el análisis de tráfico es irrebatible. En resumen, el porcentaje poblacional que se apoya en medios digitales en su vida cotidiana demuestra categóricamente su pertinencia social.

Factibilidad Legislativa: históricamente las sociedades han adaptado sus normativas penales a las influencias políticas, sociales y económicas, que van matizando la percepción de la criminalidad. Actualmente, el componente cibernético se ha insertado dentro de los elementos a tener en cuenta para legislar. En vista que un derecho constitucional como la privacidad está siendo violentado por una sigilosa técnica (como se ha confirmado), se debe proceder a una reforma de la LECDI, que según el artículo 204 de nuestra constitución le compete:

1. Al Poder Ejecutivo Nacional
2. A la Comisión Delegada y a las Comisiones Permanentes.
   [Constitución de la República Bolivariana de Venezuela, 2009, p. 55]

Por lo tanto, se deberían promover las modificaciones legislativas mediante uno de los canales constitucionales, para efectuar las consultas y discusiones pertinentes sobre la inclusión del análisis de tráfico como delito. En consecuencia, la propuesta es esencialmente factible en lo jurídico, ya que su desarrollo está plenamente ajustado a derecho. (Ver anexos: Modelo de Proyecto de Ley de Reforma Parcial de la Ley Especial Contra los Delitos Informáticos (LECDI)).

Factibilidad Tecnológica/Temporal: la propuesta entrelaza el contexto digital con la realidad social, evaluando un hecho cibernético que se mantendrá en el tiempo, por otra parte, se ajusta a la contemporaneidad legal venezolana, en vista que con el [Decreto 825, 2000] para promover el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela, el Estado asumía la preponderancia de los medios informáticos en el ejercicio público y privado, la iniciativa que aquí se impulsa persigue salvaguardar ese espacio cibernético.

Factibilidad Estratégica: esta perspectiva siempre debe ser la que marque los desarrollos legislativos, técnicos y procedimentales, sin embargo, la falta de análisis prospectivos han llevado

ISSN: 2244-7423

a que se hagan las cosas de manera invertida. En primera instancia, cubierta la necesidad penal, un plano central y organizador es el estratégico que se relaciona con la proyección estructural, específicamente en lo concerniente al Sistema Nacional de Protección y Seguridad Informática, contenidos en la Ley de Infogobierno (2013):

1. Subsistema de Criptografía Nacional
2. Subsistema Nacional de Gestión de Incidentes Telemáticos
3. Subsistema Nacional de Informática Forense
4. Subsistema Nacional de Protección de Datos. [Ley de Infogobierno, 2013, p. 20]

Debiendo valorarse la inclusión de un quinto eslabón: el **Subsistema Nacional de Anonimato**, que se encargue de aspectos **lógicos**: protocolos de comunicación; **físicos**: servidores, dispositivos de Red; y **humanos**: personal cualificado en ámbitos tecnosociales, que puedan dar respuestas integrales a la problemática como política pública. En tal sentido, Sumoza (2014) propone:

> Una de las opciones estratégicas, es la de contar con sistemas que provean anonimato en la Red, es decir, sistemas que impidan que se pueda descubrir quién, cuándo y cómo alguien o algo (una máquina o dispositivo) se comunica, o realiza o se vincula con una acción en general. En otras palabras, la intención es contar con sistemas que impidan ataques de espionaje como el análisis de tráfico a través del cual se pueda obtener información que comprometa la seguridad de una nación. (Entrevista personal realizada por el autor de la investigación, 24 de noviembre de 2014)[Quintero, 2014]

A manera de cierre, hay dos instancias legales inmediatas que deben ser apuntaladas para atender el análisis de tráfico, una mediante su atención como delito en el marco de la reforma de la LECDI, y otra que está en un plano macro que proyecta el anonimato como una dimensión para proteger por intermedio de un subsistema a la privacidad (Ver Figura 3).

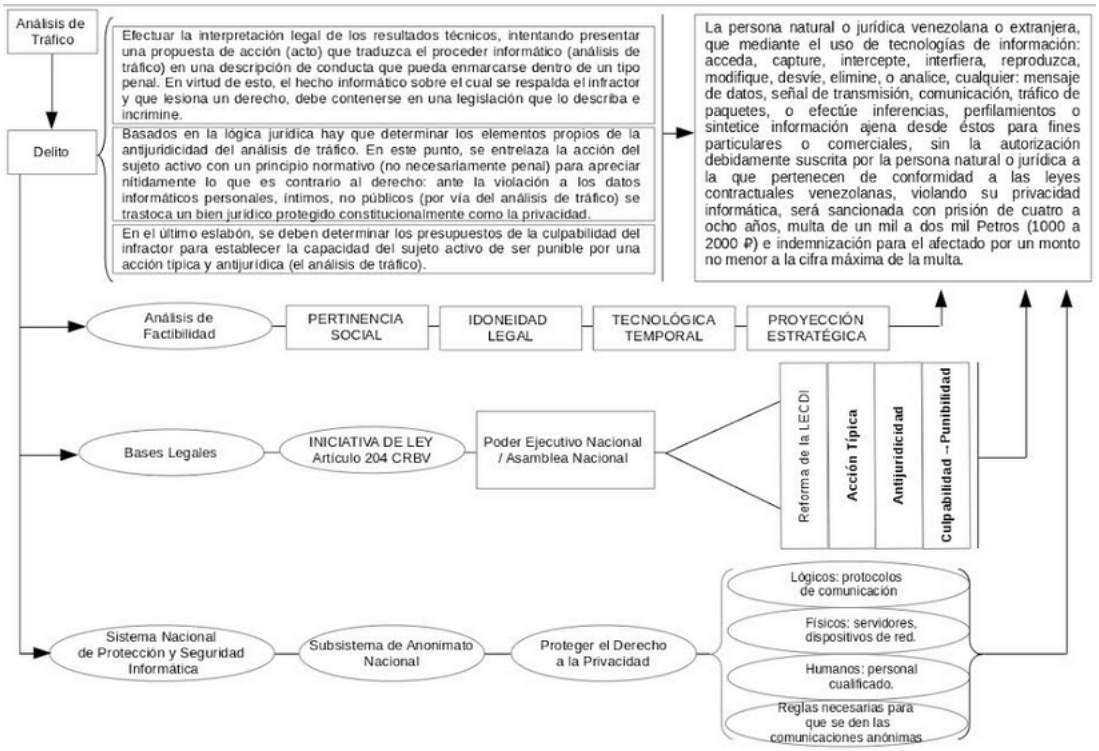

Figura 3: Síntesis Descriptiva de la Propuesta Estratégica para atender el Análisis de Tráfico
Fuente: esquema elaborado por el autor de la investigación.

Recomendaciones Finales

- Si bien en su momento la LECDI significó un desarrollo destacable en las normativas informáticas en Venezuela, se requiere la inclusión no sólo del análisis de tráfico como delito, sino de una gran variedad de nuevas amenazas que pueden atentar contra la libertad e integridad de los ciudadanos en el ciberespacio.
- Es importante que el Estado venezolano promueva la conformación de un Subsistema Nacional de Anonimato, que pase a integrar el Sistema Nacional de Protección y Seguridad Informática, ya que de lo contrario se estaría obviando el contexto (no relacionabilidad, anonimato, seudonimato y no-observabilidad).
- Se debe socializar el conocimiento sobre el análisis de tráfico, para comprender la repercusión que tiene sobre el derecho a la privacidad, y cómo se puede ver afectado incluso la eficacia y valor jurídico de la información inteligible en formato electrónico que promueve la Ley de Mensajes de Datos y Firmas Electrónicas (2001) [Decreto 1.204, 2001], ya que los datos o paquetes han sido observados por un tercero no autorizado siendo mellada la integridad.
- En relación a los organismos de seguridad, hay que formar a los funcionarios competentes

en herramientas de análisis de tráfico para que comprendan su uso y prevengan el abuso de las mi [Resolución 027, 2012], que reconoce el carácter auxiliar para la justicia moderna de la Informática Forense.

- En vista del uso extensivo de las redes informáticas, el Estado venezolano debe tener una concepción estratégica e integral para construir una institucionalidad en temas cibernéticos, que dinamice la consecución de disposiciones como la [Resolución 320, 2006], que instauró las políticas, normas y procedimientos de Seguridad Informática física y lógica en los bienes informáticos de los Órganos y Entes de la Administración Pública.
- Es cardinal, el apuntalar la industria tecnológica nacional para que tenga capacidad de desarrollar *software* y *hardware* con estándares libres, especializados en privacidad, anonimato, *ciberseguridad* y *criminalística*, que contribuyan a cubrir las necesidades visualizadas en el [Decreto Nro. 3.390, 2004], sobre migración gradual y progresiva de órganos y entes de la Administración Pública Nacional hacia el Software Libre, que fue posteriormente derogado por la Ley de Infogobierno que asumió sus premisas.
- En lo investigativo, se deben apoyar iniciativas para crear grupos de trabajo multidisciplinarios que asuman el estudio de los fenómenos tecnosociales, que estén en capacidad de formular las políticas públicas para el presente y planificar prospectivamente los escenarios del futuro.

Conclusiones

El presente artículo, contextualizó la actualidad nacional con respecto al análisis de tráfico, constatándose que producto de las inferencias tras la captura de datos y paquetes se tiene acceso a información personal que deja seriamente expuesta a la ciudadanía y al propio Estado.

Así pues, se desglosó jurídicamente la acción virtual bajo la óptica de la Teoría del Delito, proyectándose los resultados del ejercicio técnico sobre lo establecido en la Ley Especial contra los Delitos Informáticos (LECDI), quedando patente el divorcio con la cotidianidad cibernética del año 2020.

En vista de lo descrito, se efectuó una propuesta de reforma normativa que debería ser presentada por intermedio del Ejecutivo Nacional o la Comisión Permanente de Ciencia, Tecnología e Innovación de la Asamblea Nacional de la República Bolivariana de Venezuela, para la reformulación en primera instancia del artículo 21 de la precitada ley.

Igualmente, se expuso la importancia de constituir un Subsistema de Anonimato que abarque aspectos lógicos, físicos y humanos. De este modo, se atendería estratégicamente la problemática, configurándose una infraestructura nacional manejada por el Estado para limitar que sistemas o herramientas informáticas violenten la privacidad.

Finalmente, una investigación que entrelazó aspectos propios de las ciencias jurídicas y la informática, permitió enfocar adecuadamente una temática que a nivel venezolano tiene escaso nivel de disertación. Aunque el abogado clásico no suele involucrarse a fondo con temas tecnológicos, es fundamental que los juristas comprendan que hay derechos,

obligaciones y delitos que se generan en el mundo digital, no atender estos escenarios los relega profesionalmente.

Bibliografía

[Arias, 2012] Arias, F. (2012). El Proyecto de Investigación. Introducción a la Metodología Científica. Editorial Episteme. C.A. Sexta Edición.

[Avast, 2020] Avast Sofware (2020) ¿Qué hacen los sniffers? Recuperado de: https://www.avast.com/es-es/c-sniffer

[Back et al., 2001] Back, A., Möller U., Stiglic A. (2001). Traffic analysis attacks and trade-offs in anonymity providing systems. *In Information Hiding* (pp. 245-257). Springer Berlin Heidelberg. (January). [Archivo PDF].

[Castells, 2003] Castells, M., (2003). Internet, libertad y sociedad: una perspectiva analítica. Lección inaugural del curso académico 2001-2002 de la UOC. Internet Interdisciplinary Institute (IN3) de la Universitat Oberta de Catalunya (UOC). Recuperado de: http://www.ub.edu/prometheus21/articulos/obsciberprome/castells.pdf

[Código Penal, 2005] Código Penal de 2005. Gaceta Oficial de la República Bolivariana de Venezuela Nro 5768E del 13 de abril 2005.

[Cole et al., 2005] Cole, E., Nordfelt, M., Ring, S., y Ted, F. (2005). *Cyber Spying Tracking Your Family's (Sometimes) Secret Online Lives*. Syngress.

[CONATEL, 2019] Comisión Nacional de Telecomunicaciones (2019). Cifras del Sector Telecomunicaciones II TRIMESTRE 2019. Observatorio Estadístico. CONATEL. Recuperado de: https://www.conatel.gob.ve/informe-cifras-del-sector-segundo-trimestre-2019/

[Consejo de Europa, 2001] Consejo de Europa (2001). Convenio de Budapest sobre la Ciberdelincuencia. Serie de Tratados Europeos. Nro. 185. Budapest, 23.XI.2001. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[Constitución de la República Bolivariana de Venezuela, 2009] Constitución de la República Bolivariana de Venezuela de 2009. Enmienda Nro. 1 aprobada mediante Referendo Constitucional, Gaceta Oficial de la República Bolivariana de Venezuela (Extraordinaria) Nro. 5.908, de fecha 19 de febrero de 2009.

[Danezis, 2004] Danezis, G. (2004). Better Anonymous Communications. This dissertation is submitted for the degree of Doctor of Philosophy. University of Cambridge, Computer Laboratory, Queens' College, January 2004. Reino Unido. [Archivo PDF]. Recuperado de: http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/thesis.pdf

[Danezis y Clayton, 2007] Danezis, G., y Clayton, R. (2007). *Introducing traffic analysis (pp. 95-117). Auerbach* Publications, Boca Raton, FL. Estados Unidos. [Archivo PDF]. Recuperado de: http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/TAIntro-book.pdf

[Das et al., 2012] Das, S., Kant, K. Zhang, N., (2012). *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier.

[De Terwangne, 2012] De Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. IDP. Revista de Internet, Derecho y Política, (13), 53-66. [Archivo PDF]. Recuperado de: https://www.redalyc.org/pdf/788/78824460006.pdf

[Decreto 825, 2000] Decreto-825 de 2000. Acceso y uso de Internet como política prioritaria para el desarrollo cultural, económico, social. Gaceta Oficial de la República Bolivariana de Venezuela N° 36.955, de fecha lunes 22 de mayo de 2000.

[Decreto 1.204, 2001] Decreto Nro. 1.204 de 2001. Ley de Mensajes de Datos y Firmas Electrónicas (2001). Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148, de fecha 28 de febrero de 2001.

[Decreto Nro. 3.390, 2004] Decreto No 3390 de 2004. Migración gradual y progresiva de órganos y entes de la Administración Pública Nacional hacia el Software Libre desarrollado con Estándares Abiertos. Gaceta Oficial de la República Bolivariana de Venezuela Nro. 38.095, de fecha 28 de diciembre de 2004. (derogado por la Ley de Infogobierno).

[Deng et al., 2004] Deng, J., Han, R., y Mishra, S. (2004). Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. *In Dependable Systems and Networks, International Conference on* (pp. 637-646). (June). IEEE. [Archivo PDF]. Recuperado de: https://www.researchgate.net/publication/4080119_Intrusion_tolerance_and_antitraffic_analysis_strategies_for_wireless_sensor_networks/link/02e7e53bc935070479000000/download

[Red de Universidades Lectoras, 2020] Red de Universidades Lectoras (2020). *Diccionario Digital de Nuevas Formas de Lectura y Escritura.* Inferencia. Recuperado de: http://dinle.usal.es/searchword.php?valor=Inferencia

[Fu et al., 2003] Fu, X., Graham, B., Bettati, R., y Zhao, W. (2003). On effectiveness of link padding for statistical traffic analysis attacks. In Distributed Computing Systems. Proceedings. *23rd International Conference on* (pp. 340-347). (May). IEEE. [Archivo PDF] Recuperado de: https://www.researchgate.net/publication/4017116_On_effectiveness_of_link_padding_for_statistical_traffic_analysis_attacks/link/5891da5ba6fdcc1b414684de/download

[Guan et al., 1999] Guan, Y., Li, C., Xuan, D., Bettati, R., y Zhao, W. (1999). Preventing traffic analysis for real-time communication networks. *In Military Communications Conference Proceedings*. MILCOM 1999. IEEE (Vol. 1, pp. 744-750). IEEE. [Archivo PDF]. Recuperado de: https://ieeexplore.ieee.org/document/822783

[Grisanti y Grisanti, 2006] Grisanti, H., y Grisanti, A. (2006) *Manual de Derecho Penal* (Parte Especial). Vadell Hermanos.

[Ley de Infogobierno, 2013] Ley de Infogobierno de 2013. Gaceta Oficial de la República Bolivariana de Venezuela Nro. 40.274, de fecha 17 de octubre de 2013.

[Ley Orgánica de Precios Justos, 2015] Ley Orgánica de Precios Justos (2015). Gaceta Oficial de la República Bolivariana de Venezuela Nro. 40.787, de fecha 8 de noviembre de 2015.

[Ley Especial contra delitos Informáticos, 2001] Ley Especial contra los Delitos Informáticos de 2001. Gaceta Oficial de la República Bolivariana de Venezuela Nro. 37.313, de fecha 30 de octubre de 2001.

[Mejía, 1979] Mejía, E. (1979). La teoría del delito desde Von Liszt y Beling a hoy. IDEARIUM. [Archivo PDF]. Recuperado de: http://www.um.edu.ar/ojs2019/index.php/Idearium/article/download/697/678

[Moncalvo, 2007] Moncalvo, A. (2007). Pensar y Emprender un Impacto Tecnológico en la Sociedad y la Cultura. LibrosEnRed.

[Murdoch y Zieliński, 2007] Murdoch, S. y Zieliński, P. (2007). Sampled traffic analysis by internet-exchange-level adversaries. *In Privacy Enhancing Technologies* (pp. 167-183). Springer Berlin Heidelberg. (January). [Archivo PDF]. Recuperado de: https://link.springer.com/chapter/10.1007/978-3-540-75551-7_11

[Qadeer et al., 2010] Qadeer, M. Zahid, M., Iqbal, A., y Siddiqui, M. (2010). Network traffic analysis and intrusion detection using packet sniffer. In Communication Software and Networks. ICCSN'10. *Second International Conference on* (pp. 313-317). (February). IEEE. [Archivo PDF]. Recuperado de: https://link.springer.com/chapter/10.1007/978-3-540-75551-7_11

[Quintero, 2014] Quintero, D. (24 de noviembre de 2014). Entrevista personal realizada al experto en anonimato Rodolfo Leonardo Sumoza Matos.

[Raymond, 2001] Raymond, J. (2001). Traffic analysis: Protocols, attacks, design issues, and open problems. *In Designing Privacy Enhancing Technologies* (pp. 10-29). Springer Berlin Heidelberg. (January). [Archivo PDF]. Recuperado de: https://link.springer.com/chapter/10.1007/3-540-44702-4_2

[Resolución 320, 2006] Resolución Nro 320 de 2006. Políticas, normas y procedimientos de Seguridad Informática física y lógica, en los bienes informáticos de los Órganos y Entes de la Administración Pública. Gaceta Oficial de la República Bolivariana de Venezuela Nro 38.414, de fecha 06 de Abril de 2006.

[Resolución 027, 2012] Resolución-027 de 2012. Centro Nacional de Informática Forense (CENIF), Gaceta Oficial de la República Bolivariana de Venezuela Nro. 39.847, de fecha 20 de enero del 2012.

[Sumoza, 2008] Sumoza, R. (2008). *Sistemas Anónimos en Escenarios Globales.* Proyecto Fin de Máster en Investigación en Informática por la Universidad Complutense de Madrid. [Archivo PDF]. Recuperado de: https://core.ac.uk/download/pdf/19713087.pdf

[Wright et al., 2009] Wright, C., Coull, S. y Monrose, F., (2009). *Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.* In NDSS. (February). [Archivo

PDF]. Recuperado de: https://www.ndss-symposium.org/wp-content/uploads/2017/09/wright.pdf

[Zaffaroni, 1999] Zaffaroni, E. (1999). *Tratado de Derecho Penal*. Parte General. EDIAR.

Anexo 1

Modelo realizado por el autor del artículo de un Proyecto de Ley de Reforma Parcial de la Ley Especial Contra los Delitos Informáticos (LECDI)

Exposición de Motivos

En ejercicio de la garantía establecida en el artículo 48 de la Constitución de la República Bolivariana de Venezuela al secreto e inviolabilidad de las comunicaciones privadas en todas sus formas y en concordancia con el artículo 60 del precitado texto constitucional que estipula que las leyes limitarán el uso de la informática para garantizar el honor, la intimidad personal o familiar de los ciudadanos y ciudadanas, se propone una reforma parcial de la Ley Especial Contra los Delitos Informáticos (LECDI), basándose el presente proyecto de Ley en los siguientes argumentos:

Tomando en cuenta, que una de las técnicas que conspira contra la privacidad informática es el Análisis de Tráfico, por la promoción de un conjunto de hechos lesivos a bienes jurídicos protegidos –constitucionalmente– que son Objeto Jurídico del Delito, atentando contra la seguridad informática individual y degenerando en un problema a escala estatal por el Objeto Material del Delito al que lesionan, se impone la necesidad de atender este proceder que puede definirse como aquel acto cometido por un individuo u organización nacional o extranjera que mediante sistemas informáticos extrae ilegalmente información (entiéndase: por el simple hecho de analizar o inferir los datos o paquetes ajenos para su aprovechamiento o lucro).

Actualmente, en nuestro país los delitos informáticos –donde el derecho a la privacidad resulta ser el primer afectado– tienen una incidencia cada vez más común y con una tendencia al alza. Iniciado el nuevo milenio el Estado venezolano fue pionero a nivel subcontinental al fijar su atención en la delicada coyuntura que representaba el no limitar ciertas acciones en el ámbito de las TIC. No obstante, convencidos de que los delitos informáticos mantienen una constante metamorfosis en sus acciones contra bienes públicos y privados, es que nos apoyamos de este acontecer para sugerir la tipificación como delito de un sigiloso proceso que flagela flagrantemente la privacidad de todos los ciudadanos y ciudadanas que hacen uso del espacio cibernético para comunicarse o intercambiar paquetes como lo es el Análisis de Tráfico.

En atención a lo expuesto, se considera que el Análisis de Tráfico no debe permanecer sin ser previsto legalmente, correspondiendo al Estado venezolano el valorar su relevancia legislativa. En resumidas cuentas, incluirlo en el contexto penal es poner coto a individualidades y organizaciones que aprovechan el vacío legal para extraer irrestrictamente todo tipo de datos de ciudadanos e instituciones –valiéndose del desconocimiento del potencial dañino de esta técnica informática– para proceder a inferir el comportamiento tanto individual como colectivo, en búsqueda de perfilar a los usuarios de la Internet y poder ejercer multiplicidad de acciones posteriores que van desde aplicar ataques a las debilidades detectadas o simplemente vender la información al mejor postor, poniendo en tela de juicio que exista un ejercicio y goce efectivo del derecho de los internautas venezolanos a la privacidad.

PRIMERO. Se propone reformar el artículo 21 en la forma siguiente:

ISSN: 2244-7423

Violación de la privacidad informática, data, información, o paquetes ajenos de carácter personal.

Artículo 21. La persona natural o jurídica venezolana o extranjera, que mediante el uso de tecnologías de información: acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe, elimine, o analice, cualquier: mensaje de datos, señal de transmisión, comunicación, tráfico de paquetes, o efectúe inferencias, perfilamientos o sintetice información ajena desde éstos para fines particulares o comerciales, sin la autorización debidamente suscrita por la persona natural o jurídica a la que pertenecen de conformidad a las leyes contractuales venezolanas, violando su privacidad informática, será sancionada con prisión de cuatro a ocho años, multa de un mil a dos mil Petros (1000 a 2000 Petros) e indemnización para el afectado por un monto no menor a la cifra máxima de la multa.