Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay

Por Jorge Rolón Luna, Maricarmen Sequera Buzarquis
con las contribuciones de Katitza Rodríguez y David Bogado

Marzo 2016

ELECTRONIC FRONTIER FOUNDATION

TEDIC

Jorge Rolón Luna, Jurista. Estudió Derecho internacional de derechos humanos en Universidad de Oxford, y Università degli Studi di Roma Tor Vergata. Profesor de la Facultad de Ciencia de la Comunicación en la Universidad Católica de Asunción, Ex Magistrado (1996-2002), Ex comisionado en el Mecanismo Nacional de Prevención contra la Tortura en Paraguay (2012-2015).

Maricarmen Sequera Buzarquis, Directora Ejecutiva de la ONG TEDIC. Abogada de la Universidad Nacional de Asunción, especialista en Propiedad Intelectual. Trabajó en la Dirección de Relaciones Internacionales de la Presidencia de la República del Paraguay (2009-2011). Realizó investigaciones sobre Política y Derecho en Beijing, China en el año 2011. Vivió en París, Francia durante unos años donde amplió conocimientos sobre derechos humanos en el entorno digital.

Informe preparado en alianza con la Electronic Frontier Foundation. Agradecemos los aportes de Katitza Rodríguez, Directora Internacional de Derechos Humanos por la revisión sustantiva del informe, David Bogado, Latin American Community Development Coordinator y Kim Carlson, International Coordinator por la corrección de estilo y formato.

El presente reporte forma parte del proyecto regional "Vigilancia y Derechos Humanos" llevado a cabo en ocho países de América Latina por la Electronic Frontier Foundation (EFF), una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

TEDIC es una organización sin fines de lucro que desarrolla tecnología cívica y defiende los derechos humanos en Internet en pos de una Cultura libre en Paraguay.

Índice de contenido

Introducción

Paraguay tuvo 35 años de dictadura, la más larga de América Latina.[1] Durante este tiempo, las comunicaciones eran interceptadas por el Estado de forma sistemática e ilegal, registrando una gran cantidad de información sensible en las bases de datos de de las agencias de inteligencia. Un ejemplo de ello es la base de datos de la Policía, descubierta en 1992, hoy denominada "Archivo del Terror"[2].

A 27 años de la caída del régimen autoritario, el país se encuentra en una etapa democrática. Sin embargo, estas instituciones democráticas incluidas en la Carta Magna aún son muy endebles, configurando lo que se denomina *baja institucionalidad*.

En esta coyuntura fueron apareciendo las llamadas *leyes de excepción*, *leyes de emergencia*, que a través de excepciones legislativas, configuran un sistema penal de emergencia, con el objetivo de atender situaciones reales o supuestamente críticas. Este tipo de normas son consideradas herramientas jurídicas para serenar a una sociedad sacudida por los fenómenos de la violencia, el delito o la inestabilidad.

Estas situaciones supuesta o realmente insostenibles generan a su vez una suerte de inflación y populismo penal. Éstos fenómenos descansan en la creencia que el delito puede ser resuelto con el sólo recurso del endurecimiento de las penas, la penalización de nuevas conductas, las restricciones al derecho a la defensa, la no vigencia efectiva de las garantías judiciales, la intrusión descontrolada en la vida privada de las personas. Esto ha desembocado en un Neopunitivismo, el cual se expresa en cambios normativos que eventualmente vulneran normas y principios constitucionales, normas penales y procesales penales y del derecho internacional de los derechos humanos, aparte de reconfigurar el rol del derecho en la resolución de los conflictos sociales.

Algunas leyes ya vigentes en el país, algunas rechazadas y otras en estudio en el Congreso de la Nación, apuntaron y apuntan en esa dirección. Al cierre de esta edición (Marzo de 2016), se encuentra trabajando una Comisión de Reforma Penal, que tiene por objeto la revisión de las normas penales y procesales penales en el país[3]. El posicionamiento punitivista y *securitista* (la "seguridad" ante todo, aunque se lleve por delante derechos individuales) parte de un concepto equivocado: aquel según el cual el delito es un fenómeno que se resuelve (o no) en los cuatro ámbitos del sistema penal: leyes penales, práctica policial, administración de justicia y sistema penitenciario.

El mismo criterio utilizado para el análisis del recurso irracional a la prisión preventiva como herramienta de política criminal puede ser utilizado análogamente para, por ejemplo, analizar la intrusión descontrolada en la vida privada de las personas como herramienta en la lucha contra ciertos delitos.

Es posible observar que en todo el mundo estos derechos fundamentales son últimamente asediados por leyes y proyectos legislativos que muchas veces recortan derechos y garantías constitucionales reconocidos en constituciones y tratados internacionales vigentes[4]. Ello usualmente sucede en medio de circunstancias coyunturales en las que supuestamente se encuentra en juego la seguridad ciudadana. Por otro lado, se suman situaciones como la supuesta adquisición por parte del Estado paraguayo de alta tecnología en materia de vigilancia con poca o casi nula información sobre sus capacidades técnicas y el nivel de interferencia con las libertades fundamentales[5].

Este trabajo analiza el marco normativo y constitucional sobre protección de derechos fundamentales frente a la vigilancia gubernamental aplicable a Paraguay. Estudia también las principales leyes que facultan a las autoridades a ejecutar actos de vigilancia de las comunicaciones en el entorno digital, específicamente las propias del sistema de persecución penal y del servicio de inteligencia. Con base en tal análisis, el presente estudio examinará si la normativa nacional cumple con los estándares fijados en los estándares internacionales de derechos humanos, utilizando los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* como guía[6]. Teniendo en cuenta la complejidad técnico-jurídica, en el presente estudio utilizaremos los términos *vigilancia* y *comunicaciones* tal como las recogen los mencionados *Principios*[7]:

- «Vigilancia de las Comunicaciones» en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.

- «Comunicaciones» abarca las actividades, interacciones y transacciones transmitidas por medios electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados.

I.
Marco Constitucional

1.1 Fuerza normativa de los tratados internacionales en materia de derechos humanos en la Constitución

En el preámbulo de la Constitución de la República de Paraguay del año 1992 (en adelante CR) se deja sentado que el Paraguay reconoce la validez del derecho internacional de los derechos humanos, al reconocer que:

> *"...los principios de la democracia republicana, representativa, participativa y pluralista, ratificando la soberanía e independencia nacionales, e integrado a la comunidad internacional".*

En el articulado se observan varias menciones del sistema internacional. En primer término, se citan las disposiciones más trascendentes:

> *Artículo 137 – De la Supremacía de la Constitución*
>
> *La Ley Suprema de la República es la Constitución, ésta, los tratados, convenios y acuerdos internacionales aprobados y ratificados, las leyes dictadas por el Congreso y otras disposiciones jurídicas de inferior jerarquía, sancionadas en consecuencia, integran el derecho positivo nacional en el orden de prelación enunciado... (...)*
>
> *Artículo 141 – De los Tratados Internacionales*
>
> *Los tratados internacionales válidamente celebrados, aprobados por ley del Congreso, y cuyos instrumentos de ratificación fueran canjeados o depositados, forman parte del ordenamiento legal interno con la jerarquía que determina el artículo 137 (...)*
>
> *Artículo 145 – Del Orden Jurídico Supranacional*
>
> *La República del Paraguay, en condiciones de igualdad con otros Estados, admite un orden jurídico supranacional que garantice la vigencia de los derechos humanos (...)*
>
> *Artículo 143 – De las Relaciones Internacionales*

La República del Paraguay, en sus relaciones internacionales, acepta el derecho internacional y se ajusta a los siguientes principios: (...) 5. la protección internacional de los derechos humanos..."

Otras normas referidas a la cuestión internacional son:

Artículo 122 – De las Materias que no Podrán ser Objeto de Referéndum

No podrán ser objeto de referéndum: 1. Las relaciones internacionales, tratados, convenios o acuerdos internacionales;

Artículo 142 – De la Denuncia de los Tratados

Los tratados internacionales relativos a los derechos humanos no podrán ser denunciados sino por los procedimientos que rigen para la enmienda de esta Constitución.

Artículo 215 – De la Comisión Delegada

Cada Cámara, con el voto de la mayoría absoluta, podrá delegar en comisiones el tratamiento de proyectos de ley, de resoluciones y de declaraciones. Por simple mayoría, podrá retirarlos en cualquier estado antes de la aprobación, rechazo o sanción por la comisión.

No podrán ser objetos de delegación el Presupuesto General de la Nación (...), los tratados internacionales...

Artículo 224 – De las Atribuciones Exclusivas de la Cámara de Senadores

Son atribuciones exclusivas de la Cámara de Senadores: 1. iniciar la consideración de los proyectos de ley relativos a la aprobación de tratados y de acuerdos internacionales;

Artículo 238 – De los Deberes y Atribuciones del Presidente de la República

Son deberes y atribuciones de quien ejerce la presidencia de la República:

(...) 7. (...) firmar tratados internacionales ...

De una lectura atenta de esos artículos se colige lo siguiente: Paraguay acepta un orden jurídico supranacional; los tratados, acuerdos internacionales forman parte de su orden jurídico y tienen mayor jerarquía que las leyes; los acuerdos internacionales no pueden ser derogados por la vía del referéndum; para la denuncia de un tratado internacional en materia de derechos humanos se debe seguir el mismo procedimiento que para la enmienda constitucional.

Por otro lado, el más reciente desarrollo jurisprudencial de la Corte Interamericana de Derechos Humanos (en adelante Corte IDH) establece que es un deber de los magistrados judiciales ejercer un control de convencionalidad[8]. Esta obligación viene a su vez de la mano de otros señalamientos importantes por parte de la Corte IDH, como por ejemplo lo relativo a la inderogabilidad de las normas relativas a derechos humanos, aún si vienen refrendadas por la voluntad popular[9]. La Corte IDH ha dejado sentada la obligatoriedad del control de convencionalidad en cuanto a sus actos y disposiciones para los funcionarios de todos los estamentos estatales[10].

1.2 Marco constitucional

1.2.1 Derecho a la privacidad[11]

Existen numerosas definiciones del derecho a la privacidad: en algunas, se enfatiza su carácter de espacio, de reducto infranqueable de la libertad individual de la persona, que no puede ser invadido, traspasado o penetrado por terceros, sean éstos particulares o el Estado. Por otro lado, el derecho a la privacidad en su dimensión positiva incluye el derecho de toda persona de controlar sus datos personales. La intimidad es un derecho humano fundamental y es cardinal para el mantenimiento de sociedades democráticas. Es esencial a la dignidad humana.

Sobre este derecho, el artículo 33 de la Constitución Nacional de la República (CN) sostiene que:

Del derecho a la intimidad

> *"La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte el orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantiza el derecho a la protección a la intimidad, de la dignidad y de la imagen privada de las personas".*

El derecho a la privacidad, refuerza otros derechos tales como: la libertad de expresión y prensa, el derecho de las personas a recibir información veraz, responsable y ecuánime, el derecho a informarse, la libertad de asociación que están contemplados en la CR[12].

Por su parte, el artículo 36 de la CR estatuye:

Del derecho a la inviolabilidad de patrimonio documental y la comunicación privada

> *"El patrimonio documental de las personas es inviolable. Los registros cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas, cablegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de*

valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre todo aquello que no haga relación con lo investigado".

1.2.2 Protección de personales

El artículo 135 de la CR consagra el derecho a la protección de datos:

> *"Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos".*

Adicionalmente, la Ley 1682/01[13], modificada por Ley 1969/02, regula el tratamiento de los datos de carácter privado.

De acuerdo con su artículo 1:

> *"Esta ley tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. No se aplicará esta Ley en ningún caso a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar".*

Según dicha ley, está prohibida la publicación o difusión de datos personales "sensibles"[14]. Sin embargo es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercado. Los datos de personas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente con autorización expresa del titular o cuando consten en fuentes públicas y cuando se trate de

informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimento de disposiciones legales específicas[15].

Por otro lado, la ley autoriza la publicación y difusión de datos personales que la norma consideran públicos tales como el nombre, apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional de las personas[16]. Una nueva modificación se encuentra en estudio en el Congreso al cierre de edición del presente informe[17], y no es posible saber cuáles serán los cambios definitivos que tendrá la ley.

El caso más emblemático en materia de *hábeas data*[18] fue la acción interpuesta por el Sr. Martín Almada en 1992[19]. Almada, una víctima de la dictadura militar de Alfredo Stroessner (1954 – 1989), logró descubrir a través del *hábeas data* los archivos secretos de la policía stronista bautizados como "Archivo del Terror". Este Archivo ha sido declarado Patrimonio Intangible de la Humanidad por la UNESCO. Si bien estos miles de documentos revelan las prácticas policiales, cabe resaltar que hasta el momento no han sido publicados otros archivos importantes como los archivos militares o los de la cancillería paraguaya.

En la actualidad, el recurso de *hábeas data* se instaura ante un juez de primera instancia. Sin embargo, cuando se trata de información que pudiera estar contenida en el "Archivo del Terror", basta con una solicitud. Éste pedido debe presentarse ante el Centro de Documentación y Archivo dependiente de la Corte Suprema de Justicia (donde se encuentra el mencionado Archivo). En ese caso, el ciudadano deberá solo diligenciar un formulario y adjuntar una copia de su documento de identidad. Se le entregará una copia de todos los documentos que contengan su nombre, y un breve reporte acerca de qué sección del archivo general se encuentra localizado el documento solicitado. Ningún magistrado judicial que tenga competencia podrá negarse a entender en las acciones o recursos previstos en los artículos anteriores; si lo hiciese injustificadamente, sería enjuiciado y, en su caso, removido, conforme al artículo 136 de la CR.

1.2.3 Vigilancia de las comunicaciones

Como ya se ha apuntado más arriba, el derecho a la intimidad está protegido constitucionalmente en el derecho paraguayo. El artículo 30 de la CR, además, establece lo siguiente:

> *"De las señales de comunicación electromagnéticas*
>
> *La emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la soberanía nacional, promoverá el pleno empleo de las mismas según los derechos propios de la República y conforme con los convenios internacionales ratificados sobre la materia. La ley asegurará, en igualdad de oportunidades, el libre acceso al aprovechamiento del espectro*

electromagnético, así como a los instrumentos electrónicos de acumulación y procesamiento de información pública, sin más límites que los impuestos por las regulaciones internacionales y las normas técnicas. Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución."

Como se puede leer en la parte final del artículo, el Estado debe asegurar a sus ciudadanos que los instrumentos electrónicos de acumulación y procesamiento de información no sean utilizados para vulnerar la intimidad de los mismos y otros derechos establecidos en la norma constitucional. Por lo tanto, hay una clarísima obligación estatal ya reconocida en este artículo de respetar la privacidad de las personas, a la vez que un reconocimiento del riesgo que entrañan estos medios técnicos y de las potencialidades negativas que encierran.

II.

Marco Legal

2.1 Vigilancia estatal de las comunicaciones en la legislación penal y procesal penal

Al analizar la normativa penal se deben tener en cuenta las siguientes consideraciones:

En primer lugar, la norma penal no debe intervenir en todas las conductas que sean dañosas ni proteger todos los bienes jurídicos. Ella debe proteger solo aquellas más importantes con el fin de no banalizar esos bienes más valiosos ni saturar los tribunales y fiscalías.

En segundo lugar, no debe proteger a los bienes jurídicos de todas las agresiones, sino sólo de aquellas más importantes, por el carácter fragmentario del derecho penal[20].

En tercer lugar, debe intervenir solamente cuando se haya observado que otros mecanismos u otras vías no resultan eficaces para prevenir determinadas conductas. También cuando se tenga una importante convicción de la protección que el medio empleado puede dar. Esto se denomina el principio de subsidiariedad[21].

Los mismos criterios funcionan a la hora de analizar los medios que el Estado puede autorizar perseguir delitos graves. El Estado debe someter sus medidas de vigilancia a este análisis. Una intrusión desproporcionada, amparada en la posibilidad de que alguna infinitesimal parte de la población puede eventualmente cometer un delito colisiona con ese principio de intervención mínima que es deseable por parte de los Estados:

> *"En torno a este problema viene a la vez tematizada la función —utilitaria y garantista— del Derecho Penal como técnica de tutela de los ciudadanos contra la ofensa de derechos subjetivos e intereses fundamentales, sean individuales o colectivos. La idea del bien jurídico que se remite al principio de la ofensividad de los delitos como condición necesaria de la justificación, de las prohibiciones penales, se configura como límite axiológico externo (con referencia a bienes considerados políticamente primarios) o interno (con referencia a bienes estimados, constitucionalmente protegidos) del Derecho Penal. Por otra parte las políticas del Derecho Penal parecen orientarse hoy en sentido diametralmente opuesto. En efecto, prosigue la expansión incontrolada de la intervención penal que parece haber llegado a ser, (...) el principal instrumento de regulación jurídica y de control social..."*[22].

Finalmente, se deben aplicar los estándares internacionales propios del tema concreto en análisis; en este caso, aquello que tiene que ver con la vigilancia de las comunicaciones, la cual comprende, como mencionamos antes, el *"monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas"*[23].

2.1.1 Código penal

El Código Penal, Ley N° 1160/97 (en adelante CP)[24] regula la lesión del derecho a la comunicación y a la imagen. En particular, indica que aquel que sin consentimiento del afectado: (i) escuchara mediante instrumentos técnicos; (ii) grabara o almacenará técnicamente; o (iii) hiciera, mediante instalaciones técnicas, inmediatamente accesible a un tercero, la palabra de otro, no destinada al conocimiento del autor y no públicamente dicha, será castigado con pena privativa de libertad de hasta dos años o con multa.

La misma norma se aplica a quien, sin consentimiento del afectado, produjera o transmitiera imágenes: (i) de otra persona dentro de su recinto privado; (ii) del recinto privado ajeno; (iii) de otra persona fuera de su recinto, violando su derecho al respeto del ámbito de su vida íntima. La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme a los anteriormente citado.

> *Art. 146: Violación del Secreto de Comunicación*
>
> *"1°) El que, sin consentimiento del titular: abriera una carta cerrada no destinada a su conocimiento;*
>
> - *Abriera una publicación, en los términos del artículo 14, inciso 3°, que se encontrara cerrada o depositada en un recipiente cerrado o destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación; lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero,*
> - *Será castigado con pena privativa de libertad de hasta un año o con multa.*
>
> *2°) La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5°, última parte".*

2.1.2 Código Procesal Penal

La Ley N° 1286 del 8 de julio de 1998 establece en los siguientes artículos:

Artículo 198 – "Intercepción y secuestro de correspondencia: Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Regirán las limitaciones del secuestro de documentos u objetos".

Artículo 199 – "Apertura y examen de correspondencia: Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta. Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario".

Artículo 200 – "Intervención de comunicaciones: El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas. El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. La intervención de comunicaciones será excepcional". (...)

Artículo 228 – "Informes: El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar".

De la lectura de las normas transcritas más arriba se colige que rigen las siguientes cinco reglas:

- Cuando se trata de interceptación de cualquier tipo de correspondencia incluida el correo electrónico, únicamente el juez de la causa tiene la potestad de ordenar ello;
- La falta de autorización judicial es causal de nulidad del procedimiento;
- El juez es quien se hace cargo del contenido de la información interceptada, poniéndola a conocimiento del Ministerio Público, debiendo destruir la evidencia *a posteriori;*

- La excepcionalidad de la intervención de las comunicaciones privadas.

En síntesis, ni en la norma procesal penal ni en la norma penal se establece que en caso de algún delito específico el órgano de persecución penal (Ministerio Público) puede vulnerar el derecho a la privacidad si no cuenta con la autorización judicial previa en el marco de una investigación criminal.

2.2 Vigilancia estatal de las comunicaciones en la normativa de telecomunicaciones

2.2.1 Ley N° 642/95 de Telecomunicaciones

Esta Ley del año 1995, crea el ente regulador de las telecomunicaciones (la *Comisión Nacional de Telecomunicaciones,* Conatel) y protege expresamente la inviolabilidad de las comunicaciones:

> *Artículo 89 – "Se establece la inviolabilidad del secreto de la correspondencia realizada por los servicios de telecomunicaciones y del patrimonio documental, salvo orden judicial. Esta disposición es aplicable tanto al personal de telecomunicaciones, como a toda persona o usuario que tenga conocimiento de la existencia o contenido de las mismas."*
>
> *Artículo 90 – "La inviolabilidad del secreto de la correspondencia de telecomunicaciones importa la prohibición de abrir, sustraer, interferir, cambiar texto, desviar curso, publicar, usar, tratar de conocer o facilitar que persona ajena al destinatario tenga conocimiento de la existencia o el contenido de comunicaciones confiadas a prestadores de servicios y la de dar ocasión para cometer tales actos".*

2.2.2. Decreto del Poder Ejecutivo 14135/96[25] (Anexo)

> *Artículo 9º: "Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones, cuando deliberadamente una persona que no es la que efectúa la comunicación ni es la destinataria, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación. Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación efectuada a través de los servicios de telecomunicaciones, están obligadas a preservar y garantizar la inviolabilidad y el secreto de la misma. Los concesionarios o licenciatarios y autorizados a prestar o utilizar servicios de telecomunicaciones, están obligados a adoptar las medidas más idóneas para*

garantizar la inviolabilidad y el secreto de las comunicaciones efectuadas a través de tales servicios".

La normativa transcrita refuerza lo establecido en la normativa procesal en cuanto a lo siguiente:

- La inviolabilidad de las comunicaciones;
- La obligación que tienen los prestadores públicos o privados o cualquier persona que tenga conocimiento del contenido de una comunicación de preservar y garantizar la inviolabilidad o secreto de la misma o no hacerla accesible a un tercero;
- La necesidad de autorización judicial para cada caso.

2.2.3 Resolución del ente regulador

La Resolución 1350/2002 de Conatel[26] contradice la Ley 642/95 de Telecomunicaciones. Esta resolución otorga facultades a las compañías operadoras de servicios de telefonía para almacenar por un periodo de seis meses el registro de detalles de llamadas de todos los usuarios en Paraguay:

Artículo. 1. – "Establecer el plazo de seis (6) meses, como periodo obligatorio de conservación del registro de detalles de llamadas entrantes y salientes de todas las líneas que conforman la cartera de clientes de las diferentes operadoras del servicio de telefonía móvil celular (STMC) y/o Sistema de Comunicación Personal (PCS)".

Los registros de llamadas telefónicas, los SMS y los datos de localización de dispositivos móviles ya son almacenados por un periodo de 6 meses mediante la resolución de Conatel que data del año 2002, tiempo en el que ocurrieron varios secuestros extorsivos que sacudieron a la sociedad paraguaya[27].

Esta medida pre-investigativa para cualquier tipo de ilícito no sólo refleja una desproporción en cuanto al fin perseguido, sino que también deja de lado el ideal de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina *"derecho penal mínimo"*[28].

2.3 Vigilancia estatal de las comunicaciones en la legislación de inteligencia y contrainteligencia

2.3.1 Sistema nacional de inteligencia

Los artículos 6, 24, 25, 26 y 27 de la Ley Nº 5241/14 que crea el *Sistema Nacional de Inteligencia* (SINAI) desarrolla el derecho a la inviolabilidad del patrimonio documental, al decir:

Artículo 6 – "Inviolabilidad del patrimonio documental. Las comunicaciones telefónicas, postales, facsimilares o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de lectura no autorizada o no accesible al público, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial, siempre que fuesen indispensables para los objetivos concretos definidos en esta ley" (...)

Título III- Procedimientos de obtención de Información
Artículo 24. – "Excepcionalidad. Los procedimientos de obtención de información establecidos en este Título, sólo se podrán aplicar cuando los órganos e instituciones del Sistema Nacional de Inteligencia (SINAI) no puedan obtener dicha información por fuentes abiertas. La información a ser obtenida debe ser estrictamente indispensable para el cumplimiento de los objetivos estatales de resguardar la paz y seguridad nacional, la estabilidad institucional, la protección del pueblo de amenazas de terrorismo, el crimen organizado, el narcotráfico y la defensa del régimen democrático constitucionalmente consagrado".

Artículo 25. – Clasificación. "Los procedimientos referidos en el artículo anterior, son los siguientes:

1. *La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;*
2. *La intervención de sistemas y redes informáticos;*
3. *La escucha y grabación electrónica audiovisual; y,*
4. *La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información".*

Artículo 26.- "Autorización judicial. Será competencia del Secretario Nacional de Inteligencia, solicitar la autorización judicial para emplear los procedimientos señalados en el artículo anterior. La solicitud deberá ser formulada ante el Juez Penal de Garantías de Turno del lugar en el cual se habrá de realizar el procedimiento respectivo.

El Juez podrá o no ordenar, por resolución fundada, bajo pena de nulidad, la realización de los procedimientos a que se refiere el artículo anterior, dentro del plazo de 24 (veinticuatro) horas, sin más trámite. La resolución que la ordene, deberá especificar los medios que se emplearán, la

individualización de la o las personas a quienes se aplicará la medida y el plazo por el cual se decreta, que no podrá ser superior a 90 (noventa) días, prorrogable por una sola vez hasta por igual período".

Artículo 27. – "Examen. El Secretario Nacional de Inteligencia deberá entregar el resultado del procedimiento al Juez que lo ordenó, quien procederá a escuchar para sí el contenido, y también podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas".

Los caracteres de la interceptación de comunicaciones e intrusión en la privacidad por parte de las instituciones de inteligencia tiene cinco particularidades a tener en cuenta:

1. Excepcionalidad e indispensabilidad de la interceptación de las comunicaciones de que se trate
2. Únicamente cuando la interceptación tiene relación con bienes jurídicos o intereses estatales establecidos en la norma;
3. Autorización judicial requerida bajo pena de nulidad;
4. Identificación precisa de la/s persona/s a ser investigadas (prohibición de interceptaciones masivas o innominadas);
5. Tiempo limitado de la investigación de inteligencia.

2.4 Otras normativas vinculadas a la vigilancia estatal de las comunicaciones

2.4.1 Ley especial sobre represión al tráfico de drogas y estupefacientes[29]

L a *Secretaría Nacional Antidrogas* (SENAD) es la institución dependiente del Poder Ejecutivo que, de acuerdo con la ley que la crea:[30] *"coordinará las acciones entre los entes gubernamentales que trabajan en programas de lucha contra el narcotráfico y la drogadicción"*, aunque sin tener cobertura constitucional ni legal termine actuando como una fuerza de seguridad. La norma le faculta a lo siguiente:

Artículo 88. – "El juez podrá autorizar en cada caso y por tiempo determinado, a solicitud de la Secretaría Nacional Antidroga (SENAD) o del fiscal, a que ellos o sus agentes debidamente individualizados, fotografíen o filmen a los sospechosos y sus movimientos a que intercepten, registren, graben a reproduzcan sus comunicaciones orales, cablegráficas o electrónicas. La solicitud contendrá el tipo de secuencias que se propone

fotografiar o filmar o el tipo de comunicaciones que se propone interceptar, registrar, grabar o reproducir, los medios técnicos que se utilizarán para ese efecto, y los logros que se estimen obtener mediante la aplicación de dichos procedimientos. El juez podrá exigir al solicitante elementos de juicio adicionales que respalden la solicitud. Se transcribirán en acta o se conservarán solamente los documentos recolectados que tengan relación con los hechos investigados".

Artículo 89. – "El juez autorizante y el Ministerio público efectuarán el seguimiento y control de cada operativo e investigación, pudiendo impartir instrucciones sobre su desarrollo.

El juez y el Ministerio Público serán permanentemente informados del curso de los operativos e Investigaciones y las evidencias obtenidas serán puestas a su disposición".(...)

Artículo 91. – "Todos los que autoricen, controlen o intervengan en operaciones encubiertas o en entregas vigiladas deberán guardar estricta reserva sobre ellas y estarán obligados a respetar la intimidad personal y familiar y la vida privada de las personas".

Las interceptaciones de comunicación establecidas en la norma se encuentran en el capítulo relativo a las "Entregas vigiladas" y a las "Operaciones encubiertas".

De la lectura de los artículos transcritos más arriba, se colige lo siguiente:

1. Necesidad de autorización judicial en cada caso;
2. Excepcionalidad de la interceptación de comunicaciones y correspondencia;
3. Señalamiento concreto del tipo de comunicación que se quiere interceptar;
4. Pertinencia de la interceptación (qué se pretende lograr con la misma);
5. Posibilidad de que el juez solicite razones adicionales para el dictado de la medida, si lo considera necesario;
6. Limitación en el tiempo de la interceptación;
7. El control y el seguimiento de cada operativo e investigación estarán a cargo del juez y del fiscal respectivo;
8. Obligación de quienes participan en los operativos ("Entregas vigiladas" u "Operaciones encubiertas") de guardar estricta reserva y respetar la intimidad de las personas.

2.4.2 Ley de comercio electrónico

Otra normativa que pone en riesgo la privacidad de las comunicaciones en el territorio paraguayo es la Ley 4868/13 de Comercio Electrónico. En su artículo 10[31] obliga a las empresas proveedoras de Internet en Paraguay y proveedores de servicios de alojamiento de datos a almacenar como mínimo 6 meses los datos de tráfico o "relativos a la comunicaciones electrónicas".

La ley no cuenta con los estándares mínimos para salvaguardar la información privada de los usuarios, ni criterios para justificar más datos de lo que la empresa privada necesita. Este artículo limita al poder judicial y policial a acceder a los datos almacenados por las empresas.

2.4.3 Otras normas relativas a la retención obligatoria de datos

El Paraguay no cuenta con una norma específica que obligue a las empresas de telefonía o proveedoras de servicios de Internet a retener los datos de las comunicaciones de la población entera con fines de persecución penal[32]. Sin embargo, sí existe la retención voluntaria con fines comerciales.

Una propuesta legislativa que obligaba a las compañías proveedoras de Internet al almacenamiento masivo de metadatos de comunicaciones de todos los usuarios por un periodo de 12 meses para supuestos fines de investigación criminal, llegó a tener media sanción en el Congreso paraguayo a finales del año 2014. Tras una campaña de rechazo a este proyecto de ley, el Senado rechazó la propuesta apodada como "Pyrawebs" (en idioma guaraní "pyragüé" significa pies peludos y hace alusión a las tareas de espionaje de la policía durante la dictadura militar).

2.5 Proyectos de ley que ponen en peligro las comunicaciones en Internet

2.5.1 Proyecto contra el crimen organizado

Según lo establece el artículo 1 del anteproyecto, su objetivo es el de "*... fijar las reglas y procedimientos relativos al uso de técnicas especiales de investigación en el marco de las investigaciones vinculadas al Crimen Organizado*"[33].

Como en toda norma de carácter especial, sus reglas y procedimientos revisten un carácter excepcional y otorgan atribuciones no usuales a los agentes del Estado afectados a investigaciones de este carácter.

El objetivo del proyecto, dice la exposición de motivos, es luchar de manera idónea contra las organizaciones criminales, las cuales, en un mundo globalizado utilizan a su favor la tecnología disponible y los cuantiosos recursos económicos con los que cuentan, fruto de su actividad ilegal. Para tal efecto, el Estado debe prever la adecuación de sus estructuras y de

sus modos de enfrentar este tipo de criminalidad, destacándose entre estas herramientas, las técnicas especiales de investigación, entendidas, según la exposición de motivos del proyecto de ley:

> *"Como aquellas técnicas o herramientas que permitan la obtención de elementos o medios probatorios que posibiliten obtener información útil con el objeto de combatir la delincuencia organizada, tal y como disponen tanto la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 1988, (Convención de Viena de 1988), como la Convención de Naciones Unidas sobre Delincuencia Organizada Transnacional (Convención de Palermo). En atención a las disposiciones previstas en estos instrumentos internacionales y a las experiencias recogidas de la práctica, las técnicas especiales de investigación más eficaces en la lucha contra la criminalidad organizada son: la intervención de las comunicaciones, la entrega vigilada, el agente encubierto, el informante y el agente revelador, la existencia de figuras dentro del proceso que permitan garantizar la protección de testigos, la reserva de identidad según procediere y cualesquiera otras que garanticen la celeridad y éxito de las investigaciones desarrolladas para tal efecto, entre otros".*

En el caso de este proyecto en análisis, se observa que se establecen claramente cuáles son los delitos a los que se aplica estas técnicas especiales de investigación. La lista es bastante amplia, incluye 17 tipos penales del Código Penal, leyes especiales contra el narcotráfico,[34] la ley especial que sanciona la trata de personas previsto en el Código Aduanero;[35] la ley de Armas de Fuego;[36] la ley antiterrorista[37] y otras leyes penales[38].

El proyecto establece que, como parte de las investigaciones de este tipo de delitos, se podrá realizar "vigilancia electrónica", definida de la siguiente manera:

> *"... la vigilancia electrónica es la técnica especial de investigación que permite la utilización de todos los medios tecnológicos y/o electrónicos conocidos o a conocerse, que permitan obtener información y elementos de prueba con respecto a la comisión del hecho punible investigado o que permitan identificar a los autores y partícipes".*

Según el proyecto, las características de la utilización de estos medios especiales de vigilancia pueden ser:[39]

- Idóneas, necesarias e indispensables para el esclarecimiento de los hechos punibles investigados;
- Decididas en cada caso autorizando su uso cuando la naturaleza de la medida lo exija;

- Siempre que exista sospecha fundada acerca de la realización de uno o más hechos punibles que comprendan el crimen organizado;
- Las técnicas especiales de investigación deben responder siempre a los principios de necesidad, razonabilidad y proporcionalidad;
- La solicitud la realizará para cada caso el Ministerio Público; se requerirá siempre de autorización judicial de acuerdo a los parámetros establecidos en el artículo 125 del Código Procesal Penal;
- Seguimiento y control de las interceptaciones a cargo del Ministerio Público; sin perjuicio, esto último, del control que ejercerán los superiores jerárquicos de los agentes intervinientes.

2.5.2 Proyecto de protección de niños y adolescentes contra contenidos nocivos de Internet[40]

Al cierre de esta edición, se encuentra en discusión en el primer trámite constitucional del Congreso Nacional un proyecto de ley que pretende regular el filtrado de contenidos en Internet de las redes públicas inalámbricas (*Wi-Fi)* e inclusive a nivel de los de Proveedores de Servicios de Internet (ISP en inglés):

> *Artículo 3: De la Protección activa "Los proveedores de servicios de internet (ISP) deberán brindar e instalar de manera obligatoria y gratuita, a sus clientes y usuarios, los cuales deberán declarar al momento de suscribir el correspondiente contrato de prestación de servicios, o en cualquier momento posterior, si niñas, niños o adolescentes tendrán acceso a Internet, o a cualquiera que lo solicite, un software específico con sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos no aptos de conformidad al artículo 2°, con los respectivos manuales e indicaciones para su uso.*
>
> *La Comisión Nacional de Telecomunicaciones (CONATEL), a través de su unidad técnica competente, establecerá mediante normas técnicas los requisitos y condiciones mínimas que deberá cumplir el referido software, así como lo relativo a la implementación y puesta a disposición del mismo".*

Este proyecto de ley desconoce los principios de *neutralidad de la red*[41], como pilar esencial para la libertad de expresión y privacidad de los usuarios ya que otorga amplio poder a terceros, en este caso a las Proveedoras de Servicios de Internet, para realizar el filtrado de contenidos de la navegación de sus usuarios en Internet.

III.

Jurisprudencia sobre vigilancia de las comunicaciones

Paraguay cuenta con una emblemática sentencia del máximo tribunal sobre vigilancia de las comunicaciones.

La Corte Suprema de Justicia rechazó un recurso extraordinario de casación a través de la sentencia N° 674/10[42]. La resolución judicial fue dictada en la causa que investigó el secuestro y asesinato de Cecilia Cubas, la hija del ex Presidente de la República Raúl Cubas Grau (agosto 1998 – marzo 1999). Cecilia Cubas fue raptada el 21 de septiembre de 2004, cuando un grupo de criminales rodeó su vehículo, a metros de su domicilio en las afueras de la capital Asunción. Cubas fue brutalmente asesinada y posteriormente, hallada muerta el 16 de febrero de 2005[43].

El recurso extraordinario de casación solicitado por los acusados del secuestro y asesinato de Cecilia Cubas fue declarado *no ha lugar*. La Corte Suprema expresó que la Fiscalía cumplió todas las garantías procesales y que no hubo violación de las comunicaciones al solicitar —y obtener— sin orden judicial, los metadatos de las llamadas telefónicas producidas por los sospechosos autores del secuestro y asesinato.

> *"La respuesta brindada por el Tribunal de Alzada fue expresa y satisfactoria. De conformidad al articulo 228 del CPP, el Ministerio Público puede solicitar informes a cualquier persona o entidad pública o privada. El artículo 316 del CPP dentro de las facultades del Ministerio Público, reafirma que "podrá exigir informaciones de cualquier funcionario o empleado público, conforme a las circunstancias del caso. Todas las autoridades públicas están obligadas a colaborar con la investigación, según sus respectivas competencias y a cumplir las solicitudes o pedidos de informes que se realicen conforme a la ley".- Además, el haber accedido el Ministerio Público a los informes, para luego procesarlos, no implicó vulneración alguna, ya fuera de orden constitucional o legal. Como bien se ilustró, la información brindada facilitó los datos de los titulares de línea, la fecha, hora, número de teléfono entrante y saliente, y el lugar geográfico de donde se realizaban. A lo que se accedió fue al detalle del cruzamiento de llamadas, y no al contenido de aquéllas, donde el bien jurídico vulnerado sí hubiera sido la inviolabilidad de las comunicaciones y el derecho a la intimidad"*[44].

En resumen, el posicionamiento de la Corte Suprema sobre la inviolabilidad de la comunicación es el siguiente:

- Lo prescrito por el artículo 36 de la Constitución Nacional, sobre del derecho a la inviolabilidad del patrimonio documental y la comunicación privada, protege la comunicación en sí, las palabras que pudieron haberse dicho entre sí las partes acusadas en este proceso a través de un teléfono; no así los datos relativos de estas comunicaciones (con quién, cuándo, frecuencia, horarios, entre otros), que fueron el objeto de trabajo por parte del perito.

- Prueba pericial sobre cruce de llamadas: en el peritaje del cruce de llamadas, se colige que los datos aludidos son las anotaciones de la telefónica consistentes en el número telefónico investigado, las llamadas entrantes y salientes de dicho número como así los horarios de las mismas; nada de esto hace a la comunicación telefónica que consiste en el mensaje que una persona dice y otra escucha por medio de un aparato telefónico.

- Prueba de peritos: En el peritaje del cruce de llamadas se trabaja sobre los datos que quedan asentados en las llamadas telefónicas de manera posterior a una comunicación, y no sobre las comunicaciones que generaron dichos datos, estando protegida por nuestra Constitución la comunicación, no así lo que fue objeto del peritaje.

- En el peritaje del cruce de llamadas en el que la comunicación en sí no fue objeto de peritaje sino los datos que arrojó dicha comunicación, la orden judicial no era obligatoria ya que el trabajo pericial no afectaba al ámbito de protección constitucional y en segundo lugar, porque la referida orden judicial está presente en razón a los oficios del Ministerio Público.

- En el peritaje del cruce de llamadas, las comunicaciones telefónicas no fueron examinadas, no se sabe con certeza lo que se pudieron haber dicho las personas poseedoras de los números investigados; no hubo interceptación, ya que no consta que un tercero haya estado escuchando dichas comunicaciones con tecnología apropiada para ello y por lo tanto haya podido grabarla y tampoco fueron reproducidas, ya que si no fueron interceptadas y grabadas, tampoco fue posible reproducirlas.

Resulta llamativo (y preocupante) que la Corte tenga estas consideraciones sin evaluar los criterios internacionales que hoy día se están debatiendo sobre los metadatos. Analizando desde la perspectiva de la aplicación de los Derechos Humanos en la Vigilancia de la Comunicaciones, se considera que el Ministerio Público no posee la atribución de requerir informes de tal característica, porque vulnera la privacidad, más aun habiéndolos solicitado sin orden jurisdiccional de respaldo.

Tampoco toma en cuenta la decisión de la Corte Interamericana de Derechos Humanos sobre el caso contencioso en el que se condenó al Brasil[45] por el uso ilegal de escuchas telefónicas en un proceso penal: la misma Corte señaló que el derecho a la privacidad protege tanto al contenido de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación como los metadatos o datos de tráfico, entendidos éstos como

> *"el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar contenido de la llamada mediante la grabación de las conversaciones".*

IV.

Tecnología de vigilancia de las comunicaciones

El Estado a través del Ministerio del Interior ha llamado recientemente a licitación pública para la compra de tecnología en materia de equipamiento de seguridad institucional[46]. El pliego de bases y condiciones no describe las características especiales del software por razones de confidencialidad. El Congreso Nacional ha hecho un pedido de informe, pero se desconoce la respuesta[47].

A esto se suman una serie de cables diplomáticos filtrados por la organización Wikileaks [48]. Uno de los cables describe que el entonces Ministro del Interior Rafael Filizzola, durante el gobierno de Fernando Lugo (2008 - 2012), se habían mantenido conversaciones con la embajada de los EE.UU., para conocer acerca de un nuevo programa de interceptación ampliado a teléfonos celulares. Sobre dicho punto, a finales del año 2014, el Comandante de la Policía Nacional admitió en declaraciones televisivas que buscan utilizar la modalidad de escuchas telefónicas sin orden judicial solo para la prevención y persecución de hechos punibles ligados al secuestro y la extorsión[49].

Paraguay ha estado presente en la prensa internacional tras las divulgaciones sobre países interesados por la tecnología para la vigilancia. Según los correos electrónicos filtrados por *Wikileaks*[50], el fiscal de la Unidad de Delitos Informáticos del Ministerio Público, Ariel Martínez habría mantenido conversaciones a mediados del 2014 para la compra del software espía de la empresa italiana *Hacking Team*[51]. El producto estrella de *Hacking Team* es un sistema que permite interceptar computadores, videollamadas, correos electrónicos, mensajes instantáneos y contraseñas: el Sistema de Control Remoto (RCS). Según la investigación de *Privacy International*,[52] el software puede eludir el cifrado de los programas informáticos, por lo que es capaz de revisar la comunicación y el registro de llamadas, ver el historial de navegación *web*, archivos y fotos eliminadas de un dispositivo. Además, puede utilizarse para tomar control del micrófono y de las cámaras integradas del teléfono móvil y usarlos para espiar. Según el desmentido oficial, la compra no fue concretada[53].

Otra tecnología de vigilancia que implica a Paraguay es la del software FinFisher. Una publicación de *The Citizen Lab*[54], el laboratorio multidisciplinario de la Universidad de Toronto que expone acerca de las características y uso del sistema *FinFisher*,[55] citó a Paraguay como uno de los países que han adquirido dicha tecnología con funcionalidad similar al de la empresa italiana *Hacking Team*. El informe asegura desconocer acerca de la institución que lo controlaría localmente.

Es evidente que el Estado paraguayo, si ya no se ha expandido tecnológicamente con sistemas avanzados de vigilancia de las comunicaciones, está en el proceso de hacerlo, o al menos está proyectándolo y todo esto, sin las salvaguardas adecuadas: no existen regulaciones que obliguen a una rendición de cuentas, a la supervisión pública con respecto al uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones, ni a reportes de transparencia tanto en lo que tiene que ver con proceso penal como con su utilización por parte de las agencias de inteligencia.

No se cuenta con una supervisión por parte de un órgano independiente para observar tanto la autorización de la solicitud de vigilancia como para la ejecución de la misma. Tampoco existen mecanismos de notificación al usuario afectado en el proceso penal ni rendición de cuentas cuando la vigilancia la realizan agencias de inteligencia: la ciudadanía no puede ejercer control democrático acerca del ejercicio de tales facultades por parte del Estado.

V.

Marco Institucional

A continuación se muestra un organigrama de los órganos involucrados en la persecución penal en el país (incluyendo la Policía Nacional). Luego, un diagrama del proceso penal para poder interceptar una comunicación.

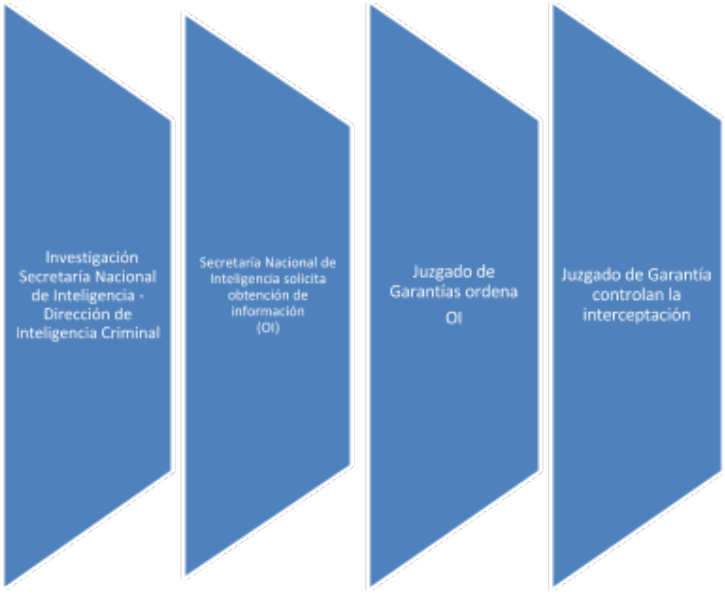
Fig. 1: Organigrama de instituciones involucradas en vigilancia de las Comunicaciones

Fig. 2: Procedimiento para interceptar comunicaciones

A continuación, se muestra un organigrama del sistema de inteligencia en el país y su funcionamiento. Luego, un diagrama del proceso que realizan los cuerpos de inteligencia para obtener información[56].

Fig. 3: Sistema de inteligencia de Paraguay

Fig. 4: Procedimientos de los cuerpos de inteligencia para vigilancia de las comunicaciones



VI.

Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

En este apartado, analizaremos si la normativa paraguaya cumple con los estándares fijados en los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*[57]. Los Principios están firmemente enraizados en el derecho internacional de los derechos humanos y el cumplimiento de tales estándares es identificable como un apego al marco de respeto de derechos fundamentales que ya es posible encontrar tanto en las normas constitucionales internas, como en los instrumentos internacionales de derechos humanos suscritos y ratificados por Paraguay. El cumplimiento de tales Principios, en consecuencia, equivale al respeto de las normas supralegales vigentes. Desde la perspectiva del respeto a los derechos fundamentales, son plenamente exigibles a la acción estatal.

A continuación analizaremos algunas disposiciones de la normativa nacional que autoriza la actividad que regula la vigilancia de las comunicaciones y su apego a los Principios:

- LEGALIDAD: "*Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo".*

Las revelaciones del *Citizen Lab* sobre la supuesta adquisición por parte del Estado paraguayo de *software* malicioso causa serias preocupaciones. Su uso en el país no está claramente autorizado por la legislación interna, ni mucho menos regulado específicamente en cuanto a su forma de utilización y alcances. En algunos casos, las normas como el artículo 200 de la CPP, son tan vagas e imprecisas que dejan abierta la puerta para futuros usos de cualquier tipo de herramienta, inclusive el uso de software malicioso: una forma de vigilancia mucho más invasiva que una mera interceptación de comunicaciones. La existencia de estas normas imprecisas ameritan una discusión pública en el Congreso y en otros ámbitos sobre la necesidad de establecer garantías adicionales. Transparencia, supervisión pública, autorización judicial previa, entre otras.

- PROPORCIONALIDAD: "*Las decisiones sobre la vigilancia de las comunicaciones deben tomarse sopesando el beneficio que se persigue contra el daño que se causaría a los derechos de los individuos y contra otros intereses en conflicto, y debería incluir un examen de la sensibilidad de la información y de la gravedad de la infracción al derecho a la privacidad. Asimismo la información será accesada solo por el juez competente y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización. (...) Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud. (...) Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales".*

Las normas nacionales expresan que la intervención de las comunicaciones deben ser de carácter excepcional. Sin embargo, la forma masiva y previa de interceptar las comunicaciones con fines de investigación penal contradice este principio. Un ejemplo de esto es la citada Resolución de Conatel, que obliga a las compañías de telefonía móvil a realizar un almacenamiento de metadatos de llamadas telefónicas y mensajes de texto por seis meses.

- AUTORIDAD JUDICIAL COMPETENTE: "*Las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente".*

Las leyes y resoluciones expuestas y analizadas más arriba, contienen un imperativo — cuando se trata de interceptación de comunicaciones— en cuanto a la necesidad de solicitar siempre a través de una orden de juez competente, por resolución fundada, bajo pena de nulidad. De acuerdo con los artículos 166, 168 y 169 del Código Procesal Penal, situaciones como esas son causales de nulidades absolutas que no pueden ser saneadas y mucho menos convalidadas. No existen entidades autorizadas para intervenir una comunicación privada sin orden judicial de acuerdo con el orden jurídico vigente en el Paraguay. No es posible que una prueba obtenida ilegalmente, como por ejemplo la interceptación ilegal de una comunicación, sea subsanada *a posteriori* por un juez.

- NOTIFICACIÓN DEL USUARIO: "*Los individuos deberían ser notificados de una decisión que autoriza la vigilancia de las comunicaciones con el tiempo e información suficientes para permitirles apelar la decisión, y deberían tener acceso a los materiales presentados en apoyo de la solicitud de autorización".*

El retraso en la notificación solo se justifica en las siguientes circunstancias:

1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y

2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y

3. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

El marco legal de Paraguay no contiene mecanismos de notificación diferida al usuario afectado por algún tipo de intrusión a su vida privada, se trate de un proceso penal o de la labor de órganos de inteligencia.

- TRANSPARENCIA: "*Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones".*

Las normas que regulan la vigilancia de comunicaciones no contienen la obligación de reportes de transparencia, ni para el proceso penal ni para labores de inteligencia. En informes anuales de la Policía Nacional, el Ministerio Público y la SENAD no se publican el número de solicitudes aprobadas y rechazadas, ni un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

- SUPERVISIÓN PÚBLICA: "*Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones".*

Actualmente en Paraguay no existe una tutela efectiva, ni se cuenta con un órgano independiente que supervise las solicitudes de vigilancia tanto en el proceso penal ni de labores de órganos de inteligencia. No cuenta con una ley de protección de datos personales propiamente dicha que salvaguarde los abusos del sector público y privado con relación a los derechos fundamentales involucrados en el ámbito de la comunicación privada. Hoy la única institución jurídica que se utiliza es el *Habeas Data*, una garantía constitucional.

- INTEGRIDAD DE LAS COMUNICACIONES Y SISTEMAS: "*Los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a construir la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de Comunicaciones del Estado".*

Cabe recordar que los artículos 9° y 10° del proyecto de Ley de conservación de datos de tráfico ("Pyrawebs"), establecía sanciones a las empresas prestadoras de servicio de acceso a

Internet que incumpliesen con la obligación de retener los datos de tráfico. Para tal efecto, se facultaba al ente administrativo correspondiente (CONATEL) a dictar reglamentos y aplicar sanciones administrativas de acuerdo a la Ley N° 642 de Telecomunicaciones.

Sin embargo, no se disponen de las garantías necesarias para la protección de los usuarios frente a los abusos o la violación de la confidencialidad de las comunicaciones, de conformidad con las obligaciones estatales en materia de derechos humanos. Las personas que pudieran ser afectadas por el uso ilegal de sus datos personales o la violación de la privacidad de sus comunicaciones quedan expuestas a una situación de indefensión legal incompatibles con las obligaciones de la República del Paraguay en la materia.

Por otro lado, se debe rescatar que no existen normas ni reglamentos que atenten contra la expresión anónima o contra el uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

VII.
Conclusiones y desafíos

El debate sobre la vigilancia de las comunicaciones en la era digital es cada vez más relevante en el Paraguay. Lo es también la creciente necesidad de las personas de participar en línea, expresar y compartir sus puntos de vista políticos sin sentirse intimidados o vigilados injustamente. Cualquier control de las actividades en Internet debe ir acompañado de políticas públicas y un equilibrio en cuanto a las leyes que interfieren con la vida privada de las personas para que eventuales invasiones sean legítimas, proporcionales, idóneas y necesarias.

El marco de protección de los derechos humanos provee de una protección robusta. Sin embargo, ese marco no es lo suficientemente específico para cubrir las nuevas situaciones planteadas por estas tecnologías.

Con base en lo analizado y desarrollado durante todos estos capítulos, se ha observado que el marco legal paraguayo debe elevar los estándares de protección de la privacidad en las comunicaciones y fortalecer las instituciones jurídicas que salvaguardan estos derechos y sostienen una democracia aún débil pero presente luego de 35 años de un implacable régimen dictatorial.

De acuerdo a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, debemos señalar lo siguiente:

- Es necesario fortalecer las instituciones penales para una mejor interpretación de la leyes nacionales e internacionales sobre vigilancia de las comunicaciones dado el avance de las técnicas y tecnologías de vigilancia. La jurisprudencia de la Corte Suprema analizada en este trabajo permite apuntar que se precisa de mayor conocimiento de las técnicas de vigilancia y la afectación del derecho a la vida privada. Los aportes de los relatores internacionales de derechos humanos y jurisprudencia internacional forman parte de un acervo que es indispensable socializar con los magistrados y agentes fiscales.

- Fortalecer los controles del funcionamiento de las actividades de inteligencia y contrainteligencia. Será importante trabajar de la mano de las Comisiones de Derechos Humanos del Congreso, la Defensoría del Pueblo y la Contraloría General de la República, instituciones públicas que deben priorizar un compromiso con la transparencia, acceso a la información pública y la defensa de los derechos humanos; con el fin de ponerles de presente los alcances que deberían tener para realizar un control adecuado y efectivo a las labores de investigación criminal que requieran de cualquier tipo de intrusión en la vida privada de las personas.

- En cuanto a la transparencia, el Estado debe hacer público el uso y alcance de las leyes de vigilancia de las comunicaciones. Debe publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas: un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora (agencias de seguridad, fiscales y jueces respectivamente), el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. El Estado paraguayo debe proporcionar a la ciudadanía información suficiente para que pueda comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la vigilancia de las comunicaciones.

- Se debe modificar el artículo 10 de la Ley de Comercio Electrónico, en lo que hace a la retención de datos de comunicaciones en Internet para fines comerciales; asimismo se debe modificar la resolución de CONATEL sobre almacenamiento de datos de llamadas telefónicas, por no cumplir con los principios de proporcionalidad, necesidad, idoneidad y debido proceso.

- Es necesario discutir y debatir en el Congreso Nacional lo relativo a los estándares internacionales en la vigilancia de las comunicaciones y que esta discusión incorpore a la ciudadanía y a las organizaciones de la sociedad civil. Esto evitará el surgimiento de proyectos abusivos como el de retención obligatoria de datos de tráfico ("Pyrawebs"). Se precisa además de marcos legales para la navegación segura en Internet en defensa de niños, niñas y adolescentes que no incluyan medidas desproporcionadas, y evitar así la creación innecesaria de nuevos hechos punibles que desean proteger a la sociedad de hechos sin mayor capacidad de daño, por ese carácter fragmentario del derecho penal ya señalado previamente.

- Se necesita proteger a los denunciantes: la ley debe reconocer la inmunidad de las personas que, de buena fe, denuncien la violación de la ley, actos de corrupción o violaciones a derechos humanos en incumplimiento de un deber de secrecía. Esta inmunidad debe estar explícitamente reconocida en la legislación que impone sanciones penales o administrativas por el incumplimiento de estos deberes de secrecía ("whistleblower").

- Aquellas personas cuyas comunicaciones están siendo vigiladas deben ser notificados —en los casos en que la ley no obligue a lo contrario— de la decisión de autorizar la vigilancia de comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras alternativas y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. Ello le permitirá a la persona afectada conocer el contenido y alcance de la invasión de su privacidad y que pueda, en consecuencia, ejercer su derecho de acceso a la justicia para remediar cualquier abuso.

- Los medios tecnológicos supuestamente adquiridos por el Estado —o en proceso de serlo— eluden la adecuada protección de los datos de carácter personal que no se encuentren sujetos a investigaciones penales. Es imperioso además contemplar mecanismos de control, custodia y preservación de los datos que hayan sido colectados como consecuencia de las medidas de vigilancia legítima que hayan sido dispuestas. Estos mecanismos deben estar bajo gestión y responsabilidad estatal. Este tipo de vigilancia no satisface el principio de proporcionalidad, ya que el marco legal no obliga la destrucción de todo el material recopilado en la interceptación de la comunicación que no resulte de relevancia para la investigación.

- Las autoridades no han informado a través de ninguna de sus agencias acerca del procedimiento y el protocolo de actuación para operar plataformas como *FinFisher*, cuestión que resulta de importancia para conocer las razones y motivos por el cual estaría operando semejante sistema de vigilancia electrónica en el país. La existencia del mencionado sistema ni fue confirmada oficialmente, ni tampoco desmentida oficial y enfáticamente, por lo cual se realiza este señalamiento.

- Debido proceso: Es indispensable asegurar que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enunciados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público en general. Específicamente, al debatirse los derechos de una persona, ésta tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley.

- Es indispensable respetar las garantías constitucionales pero también hacer público los expedientes investigativos en el futuro, contemplado el principio de publicidad de los mismos, inclusive después de llevados a cabo los procedimientos de vigilancia.

- Debate y diálogo para una nueva ley de datos personales: una ley que salvaguarde la intimidad y privacidad de los individuos, debería establecer garantías para la tutela judicial efectiva de los datos de carácter personal, que permitan a las personas que hayan sido afectadas por una medida de vigilancia abusiva, la debida restitución de sus derechos vulnerados y una reparación adecuada. Es necesario también la creación de un órgano independiente que proteja estas garantías.

- Supervisión Pública: el Estado paraguayo debería establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la vigilancia de las comunicaciones; y asimismo, poder formular declaraciones

públicas en cuanto a la legalidad de dichas acciones, incluyendo la medida en que cumplan con estos Principios. Deben establecerse mecanismos de supervisión independientes, además de cualquier supervisión ya proporcionada desde el mismo Estado.

1 Cortés, Martín. "*Paraguay tuvo la dictadura más larga y silenciosa de América Latina*". Infojus Noticias. 22 de Marzo de 2014. Disponible en: http://www.infojusnoticias.gov.ar/entrevistas/paraguay-tuvo-la-dictadura-mas-larga-y-silenciosa-de-america-latina-82.html [Fecha de consulta: 22 de Julio, 2015].

2 Jacinto Flecha, Víctor. "*El descubrimiento del Archivo del Terror en 1992".* Secretaría de Cultura. 28 de Mayo de 2011. "*Base de datos de: prontuarios de detenidos, controlados y demorados; declaraciones indagatorias; informes sobre personas, actividades sociales, estudiantes y sindicales, controles a personas, entrada y salida de personas por puntos de fronteras, colección de fotos y detenidos, reuniones, huellas dactilares, etc.* Disponible en: http://www.cultura.gov.py/lang/es-es/2011/05/el-descubrimiento-del-archivo-del-terror-en-1992/ [Fecha de consulta: 2 de Diciembre, 2015].

3 Ley N° 5.140/13. "Que modifica los Artículos 10, 20 Y 30 de la Ley No 2.403 "Que crea la Comisión Nacional para el Estudio de la Reforma del sistema Penal y Penitenciario".

4 Por ejemplo, USA Patriot Act del 26 de setiembre de 2001, o la "Ley Orgánica de Seguridad Ciudadana", más conocida como Ley Mordaza de España ¸por citar un ejemplo.

5 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "*Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*," [No prestes atención al servidor detrás del proxy: continúa proliferación de Mapeo de FinFisher], CitizenLab. 15 de Octubre de 2015. Disponible en: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/ Fecha de consulta: 2 de Diciembre, 2015]. Cáceres, Víctor. *Los drones llegan a Paraguay*. ABC Color, 27 de Setiembre de 2013. Disponible en: http://www.abc.com.py/especiales/fin-de-semana/los-drones-llegan-a-paraguay-622049.html Fecha de consulta: 2 de Diciembre, 2015].*El Gobierno de Brasil empleará tres UAV para el monitoreo de la triple frontera del Sur*. Infodefensa, 17 de Noviembre de 2011. Disponible en: http://www.infodefensa.com/es/2011/11/17/noticia-el-gobierno-de-brasil-empleara-tres-uav-para-el-monitoreo-ininterrumpido-de-la-triple-frontera-del-sur-2.html Fecha de consulta: 2 de Diciembre, 2015].WikiLeaks,The HackingTeam Archives. Paraguay, Uruguay Report

6 *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. Disponible en: https://es.necessaryandproportionate.org/text. Análisis Jurídico Internacional de Apoyo y Antecedentes https://es.necessaryandproportionate.org/analisislegal, Universal Implementation Guide for the International Principles on the Application of Human Rights To Communications Surveillance, https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Fecha de consulta: 2 de Diciembre, 2015].

7 *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (2014). Disponible en: https://es.necessaryandproportionate.org/text [Fecha de consulta: 2 de Diciembre, 2015]. Ver también La Rue Frank, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, A/HRC/23/40, 17 Abril, 2013, pág 3.

8 El "control de convencionalidad" establecido por la Corte Interamericana de Derechos Humanos en el caso "Almonacid Arellano" y completado por otros, especialmente "Trabajadores cesados del Congreso", ordena a los jueces nacionales reputar inválidas a las normas internas (incluida la Constitución) opuestas a la Convención Americana sobre Derechos Humanos, y a la interpretación dada a ésta por la Corte Interamericana. Es un instrumento eficaz para construir un *ius commune* interamericano en materia de derechos personales y constitucionales. Su éxito dependerá del acierto de las sentencias de la Corte Interamericana, y de la voluntad de seguimiento de los tribunales nacionales. (Ver el Informe Especial N° 5/2014, Mecanismo Nacional de Prevención de la Tortura de Paraguay, disponible online: http://:www.mnp.gov.py Los tres *leading cases* en materia de control de convencionalidad por parte de la Corte IDH son "*Caso Almonacid Arellano y otros vs. Chile, párr. 124; Caso Gomes Lund y otros (Guerrilha do Araguaia) Vs. Brasil, párr. 176, y Caso Furlan y familiares Vs. Argentina. Excepciones Preliminares, Fondo, Reparaciones y Costas.* Sentencia de 31 de agosto de 2012. Serie C No. 246, párr. 302.

9 "El hecho de que la Ley de Caducidad (de Uruguay) haya sido aprobada en un régimen democrático y aún ratificada o respaldada por la ciudadanía en dos ocasiones no le concede, automáticamente ni por sí sola, legitimidad ante el Derecho Internacional...". Corte Interamericana de Derechos Humanos. Caso Gelman vs. Uruguay, Sentencia de 24 de Febrero de 2011, párrafo 238.

10 Así, en varias sentencias la Corte ha establecido que es consciente que las autoridades internas están sujetas al imperio de la ley y, por ello, están obligadas a aplicar las disposiciones vigentes en el ordenamiento jurídico. Pero cuando un Estado es parte en un tratado internacional como la Convención Americana, todos sus órganos, incluidos sus jueces y demás órganos vinculados a la administración de justicia en todos los niveles, también están sometidos al tratado, lo cual les obliga a velar para que los efectos de las disposiciones de la Convención no se vean mermados por la aplicación de normas contrarias a su objeto y fin, de modo que decisiones judiciales o administrativas no hagan ilusorio el cumplimiento total o parcial de las obligaciones internacionales. Es decir, todas la autoridades estatales, están en la obligación de ejercer *ex officio* un "control de convencionalidad" entre las normas internas y la Convención Americana, en el marco de sus respectivas competencias y de las regulaciones procesales correspondientes. En esta tarea, deben tener en cuenta no solamente el tratado, sino también la interpretación que del mismo ha hecho la Corte Interamericana, intérprete última de la Convención Americana. (Caso Gelman Vs. Uruguay Resolución de la Corte Interamericana de Derechos Humanos, de 20 de marzo 2013 Supervisión de cumplimiento de Sentencia, párrafo 66.).

11 En la presente investigación, entendemos que el derecho a la privacidad abarca el derecho a la vida privada y el derecho a la intimidad, el secreto o inviolabilidad de las comunicaciones y la protección de los datos personales y la inviolabilidad del domicilio.

12 Véase artículo 26 y 28 de la Constitución de la República del Paraguay.

13 "Que reglamenta la información de carácter privado". Actualizada con la Ley 1.969/02. "Que modifica, amplía y deroga varios artículos de la Ley N° 1682/2001 'Que reglamenta la información de carácter privado'"

14 La norma considera datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias.

15 Véase Artículo 3, 4 y 5 de la Ley 1682/01.

16 Véase Artículo 6 de la Ley 1682/01.

17 *"La Cámara de Senadores aprobó hoy una versión modificada que reglamenta la difusión y el trato de informaciones de carácter privado (Informconf). La propuesta vuelve a pasar a la Cámara de Diputados. La comisión de Legislación del Senado modificó el proyecto aprobado por Diputados y dispuso que solo las personas que adeuden el equivalente o más de tres salarios mínimos sean incluidas en el sistema de Informconf. Además, el Senado también aprobó que las personas que paguen su deuda sean excluidas de este sistema en un plazo máximo de 24 horas (...) La propuesta fue enviada de vuelta a Diputados, que debe ratificarse o aprobar la versión del Senado para su posterior sanción en el Congreso"*. Ver: Diario ABC Color, 19 de mayo de 2015, p. 8.

18 Expediente N: 561, folio 174, año 1992: *Acción de habeas data a favor de Martín Almada*, Juzgado en lo Criminal 3er turno, Juez José Agustín Fernández.

19 *"En fecha 14 de septiembre de 1992, a las 8:10 horas, ante el juzgado de Primera Instancia Criminal del Tercer Turno, ha sido presentada una solicitud de habeas data por el Dr. Martín Almada, bajo patrocinio de los abogados Pedro Darío Portillo y Rodolfo Aseretto"*. Museo de la Justicia – Poder Judicial. Disponible en:

http://www.pj.gov.py/contenido/132-museo-de-la-justicia/132 [Fecha de consulta: 3 de Diciembre, 2015].

20 Mir Puig, Santiago. *Derecho Penal Parte General*, Barcelona Editorial Tecfoto, 1996, p. 90: *"Un segundo principio derivado de la limitación del Derecho penal a lo estrictamente necesario, es el postulado del «carácter fragmentario del Derecho penal». Significa que el Derecho penal no ha de sancionar todas las conductas lesivas de los bienes que protege, sino sólo de las modalidades de ataques más peligrosas para ellos".*

21 Mir Puig, Santiago. Op. Cit. P. 89: "Para proteger los intereses sociales el Estado debe agotar los medios menos lesivos que el Derecho penal antes de acudir a éste, que en este sentido debe constituir un arma subsidiaria, una últimaratio". García Ramírez, Sergio. Op. Cit. "...el derecho penal debe representar la última ratio legis". Milanese, Pablo. El Moderno Derecho Penal y la Quiebra del Principio de Intervención Mínima. www.derechopenalonline.com/febrero2004/milaneseintervencion.htm: "La subsidiariedad consiste en recurrir al Derecho penal, como forma de control social, solamente en los casos en que otros controles menos gravosos son insuficientes, es decir, «cuando fracasan las demás barreras protectoras del bien jurídico que deparan otras ramas del derecho».

22 Ferrajoli, Luigi. *Derecho Penal Mínimo y Bienes Jurídicos Fundamentales*. http://www.corteidh.or.cr/tablas/r16993.pdf [Fecha de consulta: 2 de Diciembre, 2015].

23 *Principios Internacionales* cit.

24 Véase artículo 144.

25 *"Por el cual se aprueba las normas reglamentarias, de la Ley Nº 642/95 'De telecomunicaciones'".*

26 Comisión Nacional de Telecomunicaciones (CONATEL). *RESOLUCIÓN Nº 1350/2002.- Por la cual se establece la obligatoriedad de registro de detalles de llamadas por el plazo de seis meses*. Disponible en: http://www.buscoley.com/pdfs/r_1350_2002.pdf [Fecha de consulta: 3 de Diciembre, 2015].

27 Última Hora. *Los casos de secuestros en Paraguay*. Disponible en: http://www.ultimahora.com/los-casos-secuestros-paraguay-n460811.html [Fecha de consulta: 28 de Diciembre, 2015].

28 *"Derecho penal mínimo significa la reducción al mínimo de las circunstancias penales y su codificación general mediante la despenalización de todas aquellas conducta que no ofendan bienes fundamentales y que saturan el trabajo judicial con un dispendio inútil e inocuo de aquel recurso escaso y costoso que es la pena y tienen el triple efecto del debilitamiento general de las garantías, de la ineficacia de la maquinaria judicial y de la devaluación de los bienes jurídicos merecedores de tutela penal."* Ferrajoli, Luigi. Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura. Revista Pena y Estado año 1 número 1–Argentina 1995: Editores del Puerto s.r.l. p. 113.

29 Ley Nº 1881 Que Modifica La Ley Nº 1340 Del 22 de Noviembre De 1988 "Que Reprime El Tráfico Ilícito De Estupefacientes Y Drogas Peligrosas Y Otros Delitos Afines Y Establece Medidas De Prevención Y Recuperación De Fármacodependientes".

30 A este respecto, debe tenerse en cuenta lo que establece el artículo 172 de la CR: "La Fuerza Pública está integrada, en forma exclusiva, por las fuerzas militares y policiales".

31 Ley 4868/13 de *Comercio Electrónico*. Disponible en: http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf Fecha de consulta: 2 de Diciembre, 2015].

32 *Pyrawebs*, Tedic. Disponible en: http://pyrawebs.tedic.org/ [Fecha de consulta: 2 de Diciembre, 2015].

33 Proyecto de ley presentado por los senadores Fernando Silva Facetti, Enrique Bacchetta y Roberto Acevedo el 2 de octubre de 2013.

34 Ley 1340 Del 22 de Noviembre de 1988 "*Que Reprime El Tráfico Ilícito De Estupefacientes Y Drogas Peligrosas Y Otros Delitos Afines Y Establece Medidas De Prevención Y Recuperación De Fármacodependientes*" y sus modificatorias.

35 Ley Nº 4788 "Integral contra la trata de personas" Ver también Ley Nº 2.422/04, *Código Aduanero*.

36 Ley 4036/10 de "*Armas de Fuego, sus piezas y componentes, municiones, explosivos, accesorios y afines*".

37 Los previstos en la Ley 4024/10 "*Que castiga los hechos punibles de Terrorismo, Asociación Terrorista y Financiamiento del Terrorismo*".

38 Los previstos en la Ley 4439/11 "*Que modifica y amplía varios artículos de la Ley 1160/97 Código Penal y la Ley 3440/08 Que modifica varias disposiciones de la Ley N° 1160/97, Código Penal*".

39 Artículo 6 del Anteproyecto.

40 SILpy - Sistema de Información Legislativa. Proyecto de Ley: *DE PROTECCION DE NIÑOS Y ADOLESCENTES CONTRA CONTENIDOS NOCIVOS DE INTERNET*. http://sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F103933 [Fecha de consulta: 3 de Diciembre, 2015].

41 Comisión Nacional de Telecomunicaciones (CONATEL). *RESOLUCIÓN DIRECTORIO W 190/2009 POR LA CUAL SE ESTABLECE EL REGLAMENTO DE LOS SERVICIOS DE ACCESO A INTERNET, TRANSMISION DE DATOS*. Disponible en: http://www.conatel.gov.py/files/marcoregulatorio/resoluciones/RD_190_2009_-_INTERNET_RES_DIR_CON_ANEXO.pdf [Fecha de consulta: 3 de Diciembre, 2015].

42 Acuerdo y Sentencia Nº 674/10 "*Recurso Extraordinario De Casación Interpuesto Por La Defensora Pública Sandra Rodríguez Samudio En La Causa Anastacio Mieres Burgos Y Otros S/ Secuestro Y Otros*". Expte. N° 773, Folio 245".

43 ABC Color. *Especial Caso Cecilia Cubas*. Disponible en: http://www.abc.com.py/multimedia/caso-cecilia-cubas/ [Fecha de consulta: 2 de Diciembre, 2015].

44 Corte Suprema de Justicia. Sala Penal: *Materia Penal. Inviolabilidad De La Comunicación Privada. Pruebas. Medios De Prueba. Prueba De Peritos. Cruce De Llamadas*. Acuerdo y Sentencia N° 711 del 20/08/14.

45 https://web.archive.org/web/20140527113509/http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

46 Licitación Pública de Adquisición de Equipamientos y Periféricos para la Seguridad Interna del Ministerio del Interior (Policía Nacional) Página 10 https://www.contrataciones.gov.py/sicp/download/getFile?cid=45685&fileName=OAwkXiYNi6QOh%2BTIKqR3782C1d%2Fp2D6FjIiEs6npdi%2F1ZqqfT7VKyeTQxatNaWt5IxSb9jusPNXO1wj6SydKziVsfoYTRYq%2BBaCsYn4it67q6WhpQnEfFfcXrCqQvEbOmkkgUBngwr4ij3Ea4EbM7A%3D%3D [Fecha de consulta: 2 de Diciembre, 2015].

47 http://www.agendalegislativa.com.py/senado/5922-senado-pide-informe-al-ministerio-del-interior-sobre-equipos-de-escuchas-telefonicas [Fecha de consulta: 2 de Diciembre, 2015].

48 Wikileaks https://wikileaks.org/plusd/cables/10ASUNCION97_a.html [Fecha de consulta: 2 de Diciembre, 2015].

49 Informe Canal 4 Telefuturo: *Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro* - 26/11/2014 https://www.youtube.com/watch?v=3Bkdspxhae8 [Fecha de consulta: 2 de Diciembre, 2015].

50 WikiLeaks - *The Hackingteam Archives. Paraguay - Uruguay Report*. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/249535 [Fecha de consulta: 3 de Diciembre, 2015].

51 *The Hacking Suite for Governmental Interception*. Disponible en: http://www.hackingteam.it/ [Fecha de consulta: 3 de Diciembre, 2015].

52 Privacy International. *Briefing for the Italian Government on Hacking Team's surveillance* [Informe para el Gobierno italiano sobre la vigilancia de Hacking Team]. Disponible en: https://www.privacyinternational.org/sites/default/files/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team's%20surveillance%20exports.pdf [Fecha de consulta: 3 de Diciembre, 2015].

53 ABC Color. *Gobierno negoció espionaje*. 9 de Julio de 2015. Disponible en: http://www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html [Fecha de consulta: 2 de Diciembre, 2015].

54 https://citizenlab.org/ [Fecha de consulta: 2 de Diciembre, 2015].

55 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "*Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*," [No prestes atención al servidor detrás del proxy: continúa proliferación de Mapeo de FinFisher], CitizenLab. 15 de Octubre de 2015. Disponible en: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

56 La información podrá ser obtenida a través de los siguientes medios: "1) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; 2) La intervención de sistemas y redes informáticos; 3) La escucha y grabación electrónica audiovisual; y, 4) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información". Artículo 25 de la Ley N° 5241/14, que establece el SINAI.

57 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text [Fecha de consulta: 2 de Diciembre, 2015].; EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal; [Fecha de consulta: 2 de Diciembre, 2015], Access, Guía Universal de Implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://eff.org/r.4gac [Fecha de consulta: 20 de julio, 2015].