Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay

Por Fabrizio Scrollini, Ana Tudurí y Katitza Rodríguez

Diciembre de 2015

ELECTRONIC FRONTIER FOUNDATION

Informe preparado para la Electronic Frontier Foundation. Agradecemos los aportes de Kim Carlson y David Bogado de EFF por la corrección de estilo y formato.

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

Índice de contenido

I.

La Vigilancia estatal de las comunicaciones en Uruguay

En julio de 2013 el diario El País alertó sobre la compra secreta de un software de vigilancia conocido como "El Guardián".[1] El incidente provocó un pronunciamiento de la sociedad civil[2] y del sistema político uruguayo, preocupados ambos por la compra y uso de esta tecnología. Más allá de las particularidades de este incidente, el mismo puso de manifiesto que el estado uruguayo está extendiendo su habilidad de vigilar las comunicaciones de sus habitantes, adquiriendo por primera vez tecnología que aumenta ésta capacidad de forma exponencial. Ello justifica nuestro interés de realizar un mayor análisis acerca del marco regulatorio existente para el desarrollo de las actividades de vigilancia. Uruguay, un país tradicionalmente conocido por su seguridad jurídica e instituciones sólidas, enfrenta ahora un nuevo desafío para los derechos humanos en el siglo XXI sin una guía clara de cómo resolverlos.

La relevancia del problema es mayor. Tradicionalmente las comunicaciones entre las personas han sido consideradas protegidas de la interceptación por parte de autoridades del Estado. Sólo en momentos de crisis institucional, como durante la pasada dictadura militar (1973-1985), las comunicaciones de los habitantes del país fueron intervenidas ilegalmente con el objeto de reprimir la actividad política. La conexión entre la privacidad de las comunicaciones, el derecho de reunión y asociación, y eventualmente la libertad de expresión es bastante clara. Si las comunicaciones de las personas pueden ser monitoreadas por los Estados sin mayor control, los derechos referidos se ven amenazados.

Si bien las tecnologías para vigilar las comunicaciones han estado disponibles hace más de un siglo,[3] es la capacidad y alcance a gran escala de esta actividad que crea nuevos retos para la protección de la privacidad en la era digital. Debido a la complejidad del tema en sus aspectos técnicos, jurídicos y políticos, conviene aclarar que en este informe utilizaremos los términos vigilancia de las comunicaciones el siguiente sentido:

- *Vigilancia de las comunicaciones:* monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, que se derive o surja de ellas.[4]

- *Datos de las comunicaciones*: Información sobre las comunicaciones de una persona (correos electrónicos, llamadas telefónicas y mensajes de texto enviados y recibidos, mensajes y publicaciones en las redes sociales), identidad, cuentas en red, direcciones, sitios web visitados, libros, otros materiales leídos, vistos o escuchados, búsquedas realizadas, recursos utilizados, interacciones (orígenes y destinos de las comunicaciones, personas con las que interactúa, amigos, familia, conocidos, horarios y ubicación de un individuo, incluyendo su proximidad a otros);[5]

En este informe se analiza el marco constitucional e internacional de los derechos humanos frente a la vigilancia estatal de las comunicaciones. Luego se revisa la normativa, jurisprudencia y doctrina nacional que autoriza la vigilancia de las comunicaciones. También se señalan dos casos de vigilancia relevante y plantea preguntas en el contexto del marco legal disponible.

Este documento propone una mirada al marco regulatorio uruguayo a la luz de los estándares internacionales de derechos humanos, usando los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones como guía.[6]

El cumplimiento de los Principios es un indicador fuerte de respeto a derechos fundamentales que ya se encuentran recogidos en las normas constitucionales internas y los instrumentos internacionales de derechos humanos suscritos y ratificados por Uruguay.

El documento culmina con una serie de recomendaciones para el gobierno y la sociedad civil en Uruguay estableciendo una serie de preguntas, decisiones y consecuencias sobre el actual y tal vez futuro régimen de vigilancia de las comunicaciones en el país.

II.

Marco normativo

2.1 Protección constitucional de la libertad de expresión y la privacidad de las comunicaciones

Las libertades fundamentales, como el derecho a la privacidad, libertad de expresión, libre asociación y el derecho a la información, cuentan con una amplia protección legal a nivel nacional e internacional. En el ámbito nacional estos derechos se encuentran tutelados por la Constitución de la República Oriental del Uruguay en los artículos 7, 29, 72, 82 y 332. Específicamente la libertad de expresión está consagrada en el artículo 29 de la constitución, que indica:

> *"Es enteramente libre en toda materia la comunicación de pensamientos por palabras, escritos privados o publicados en la prensa, o por cualquier otra forma de divulgación, sin necesidad de previa censura..."*

Al igual que el artículo 13 de la Convención Americana sobre Derechos Humanos, la libertad de expresión en el derecho uruguayo, puede ser ejercida por todos los medios y no puede ser objeto de censura previa, sino de responsabilidades ulteriores.

En referencia a la privacidad de las comunicaciones, la constitución en el artículo 28 establece ya desde sus orígenes decimonónicos:

> *"Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general."*

Consecuentemente la interceptación de la correspondencia y las comunicaciones personales procederá excepcionalmente cuando una ley lo establezca por razones de interés general.

2.2 Tratados internacionales

En el ámbito internacional el artículo 12 de la Declaración Universal de los Derechos Humanos prevé la protección de las comunicaciones privadas.[7] Con un texto similar este derecho está previsto en el artículo 17 del Pacto Internacional de Derechos Civiles y

Políticos[8] y en el artículo 11 de la Declaración Americana de los Derechos y Deberes del Hombre.[9] Uruguay ha suscrito y ratificado estos tratados.

Sin embargo, a diferencia de otros países en la región, las normas de tratados de derechos humanos no son automáticamente incorporados al derecho nacional. Los tratados se incorporan al orden jurídico nacional cuando son aprobados por el Parlamento.

Existen interpretaciones en la doctrina uruguaya que señalan que estos derechos se encuentran reconocidos debido al carácter *iusnaturalista* de su Constitución reflejado en el artículo 72 y 332. La doctrina nacional habla de la "autoejecutabilidad" de las normas de derechos humanos, es decir, la posibilidad de invocar estos derechos de forma efectiva aún cuando el parlamento o el ejecutivo no los hubiese reglamentado.[10]

2.3 Marco legal

2.3.1 La vigilancia en la legislación uruguaya

La vigilancia de las comunicaciones estuvo inicialmente regulada en el artículo 212 del Código Proceso Penal Uruguayo (en adelante C.P.P.),[11] y el artículo 146.2 del Código General del Proceso, que señala que la vigilancia puede ser utilizada como un medio de prueba no prohibido por ley.[12]

La vigilancia en materia de comunicaciones genera resistencia en algunos operadores judiciales (notoriamente en los abogados defensores).[13] Sin embargo, la vigilancia se considera un medio lícito de prueba en los tribunales uruguayos siempre y cuando se haya obtenido conforme a ley.[14]

La legalidad de la interceptación de las comunicaciones se fundaba en el artículo 212 del CPP. Ella procede en casos que existieran motivos graves para creer que esta medida podría garantizar la prueba suficiente en la comprobación de un delito. Esto incluye la interceptación de correspondencia y otras comunicaciones. Esta norma no prevé la notificación a la persona cuyas comunicaciones se están interceptando luego de finalizada la medida.

Luego, la ley No. 18.494 sobre control y prevención de lavados de activos y del financiamiento del terrorismo en su artículo 5 instaura la vigilancia electrónica como un medio al que puede recurrirse en la investigación de ciertos delitos que la norma prevé.

Este artículo indica que:

> *"Artículo 5º. (Vigilancias electrónicas).- En la investigación de cualquier delito se podrán utilizar todos los medios tecnológicos disponibles a fin de facilitar su esclarecimiento.*
>
> *La ejecución de las vigilancias electrónicas será ordenada por el Juez de la investigación a requerimiento del Ministerio Público. El desarrollo y la colección de la prueba deberá verificarse bajo la supervisión del Juez competente. El Juez competente será el encargado de la selección del material destinado a ser utilizado en la causa y la del que descartará por no referirse al objeto probatorio.*
>
> *El resultado de las pruebas deberá transcribirse en actas certificadas a fin que puedan ser incorporadas al proceso y el Juez está obligado a la conservación y custodia de los soportes electrónicos que las contienen, hasta el cumplimiento de la condena. Una vez designada la defensa del intimado, las actuaciones procesales serán puestas a disposición de la misma para su control y análisis, debiéndose someter el material al indagado para el reconocimiento de voces e imágenes. Quedan expresamente excluidas del objeto de estas medidas las comunicaciones de cualquier índole que mantenga el indagado con su defensor y las que versen sobre cuestiones que no tengan relación con el objeto de la investigación."*

De este extenso artículo es importante resaltar cinco aspectos: el objeto de la vigilancia, el proceso correspondiente, los medios previstos, el rol del indagado y los delitos comprendidos:

1. Con relación al *objeto de la vigilancia* según la doctrina local,[15] abarca la interceptación telefónica, mensajes de texto, correos electrónicos, intervención de teléfonos satelitales, cámaras de vídeo, micrófonos, la recolección de datos de la comunicación (metadatos), entre otros.

2. Con relación al *proceso*, no se determina un criterio de selección del material que se ha grabado ya que en la práctica ello se deja al criterio del juez actuante. Consecuentemente el/la magistrada/o, operando inicialmente bajo un sistema penal de corte inquisitorio,[16] decidirá qué material será considerado o no parte de un proceso. La norma establece a texto expreso lo siguiente:

> "*...Quedan expresamente excluidas del objeto de estas medidas las comunicaciones de cualquier índole que mantenga el indagado con su defensor y las que versen sobre cuestiones que no tengan relación con el objeto de la investigación..."*

El Dr. José Luis G. González,[17] señala que, en la práctica, sólo se puede ejercer un control sobre el material interceptado cuando se entrega a la defensa una copia de la transcripción de

la escucha durante la audiencia. Por lo tanto, la notificación a la persona se difiere hasta el momento de la audiencia.

No existe claridad acerca de los criterios que el Juez debe seguir para descartar la información. Conforme al artículo 24 de la ley 18.331, los datos personales registrados con fines policiales se deberían descartar cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. En el proceso legal, la autoridad judicial competente determina la intervención y supervisa la misma a requerimiento del Ministerio Público (Fiscalía).

El procedimiento para que opere la vigilancia consiste en: (i) La autorización *de la vigilancia electrónica* debe constar en resolución fundada del Juez; (ii) Debe existir un memorándum policial que establezca los motivos de la investigación que fundamentan la solicitud al Fiscal; (iii) el Fiscal debe fundamentar por qué motivo la realiza. En conclusión, se trata de una resolución fundada que no puede materializarse en un mandato verbal del Juez.[18]

La ejecución de la vigilancia electrónica es ordenada por el Juez de la investigación a requerimiento del Ministerio Público (Fiscalía). El desarrollo y la recolección de la prueba deberá verificarse bajo la supervisión de Juez competente. El Juez competente será el encargado de la selección del material destinado a ser utilizado en la causa y la que descartará por no referirse al objeto probatorio.

3. En cuanto a los *medios previstos*, la ley parece dar vía libre al estado para utilizar "todos los medios tecnológicos disponibles". Una interpretación extensiva de la norma podría decir que esta disposición permite la autorización de varios tipos de técnicas y tecnologías de vigilancia como el uso de programas maliciosos (*malware* en inglés). Sin embargo, esta norma al ser antigua, no fue redactada teniendo en cuenta el nivel de intrusión de las nuevas técnicas y tecnologías en materia de vigilancia.

Además el marco jurídico Uruguayo debe siempre interpretarse en conjunto con los tratados internacionales de derechos humanos. En particular, la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica). También debe aplicarse el requisito constitucional de necesidad de orden judicial previa para poder realizar actividades de investigación.

4. En cuanto al *rol del indagado* se establece que: "...Una vez designada la defensa del intimado, las actuaciones procesales serán puestas a disposición de la misma para su control y análisis, debiéndose someter el material al indagado para el reconocimiento de voces e imágenes..."

5. Con relación a los *delitos comprendidos,* la norma indica que la *autorización de vigilancia* se puede utilizar "en la investigación de cualquier delito...", inclusive aquellos delitos menores. El uso de mecanismos de vigilancia debería limitarse a una lista taxativa de delitos con cierta entidad penal.[19] Si bien la ley donde se regula el proceso de vigilancia refiere a delitos vinculados al lavado de activos, en general se han ido expandiendo a otros tipos delictivos originalmente no contemplados en esta normativa.El Fiscal especializado en crimen organizado Juan Gómez afirma sobre esta norma que "la ponderación con la que los jueces manejan esta herramienta, que es totalmente necesaria en algunos tipos de investigaciones, como las vinculadas al narcotráfico".[20]

El Ministerio del Interior justifica la aplicación de medidas de vigilancia y el uso del sistema El Guardián en esta disposición, lo cual es insuficiente.

La legislación uruguaya contempla otras posibilidades donde la vigilancia podría ser de recibo. En caso de suspensión de garantías individuales, ésta sólo se puede dar por motivos del (Art. 31 de la Constitución) y las medidas prontas de seguridad (Art. 168 ord. 17). Ambas medidas suponen una restricción general a los derechos fundamentales bajo supuestos de conmoción interior o amenaza exterior al país. Por otra parte no existe en la legislación uruguaya una disposición que regule la autorización de la vigilancia en casos de emergencia, donde exista un riesgo inminente de peligro para la vida humana.

El Código Penal (en adelante C.P.) uruguayo pena la interceptación de comunicaciones en varios artículos.[21] En particular el C.P. tipifica la violación de correspondencia escrita (incluyendo los correos electrónicos) mediante la interceptación, destrucción u ocultación de la correspondencia. El delito se agrava si quien lo comete es un funcionario público. También el C.P. castiga la revelación de la información. La regulación establece penas mínimas para quienes realicen estos actos. Estas penas son en general, poco significativas en el contexto del Código Penal Uruguayo. Las cortes locales han ocasionalmente procesado personas por estos delitos.[22]

2.3.2 Los delitos informáticos y su conexión con la vigilancia

En Uruguay no existe normativa específica sobre "delitos informáticos". Para solucionar estos casos se recurre a la normativa penal vigente. Durante la legislatura pasada se presentó un proyecto sobre delitos informáticos por parte de la Agencia para el Gobierno Electrónico y la Sociedad de la Información (AGESIC). Este proyecto se encuentra en estudio por el Parlamento y fue rechazado categóricamente por la sociedad civil.[23]

El proyecto incluía una serie de tipos(conductas) penales demasiado amplios. Esta contenía una disposición que preveía la penalización a la llamada "ingeniería inversa" prohibiendo la modificación de los equipos informáticos por parte de los usuarios. Aunque inicialmente los llamados delitos informáticos parecerían no tener demasiado que ver con la agenda de

vigilancia, el hecho que los usuarios no puedan modificar sus equipos tiene fuertes implicancias para medidas de protección como el cifrado de las comunicaciones.

2.3.3 La retención de datos personales y su potencial uso por parte de actores privados y estatales

La ley 18.331 en su artículo 35 establece la Unidad Reguladora de Datos Personales y Acción de Hábeas Data (URCDP). La URCDP podrá aplicar medidas sancionatorias a los responsables de las bases de datos en caso de que violen la presente ley. Estas medidas consisten desde el apercibimiento, multa de hasta 500 unidades indexadas[24] hasta suspensión de la base de datos respectiva.

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)[25] entiende que se han tomado medidas pertinentes para asegurar la transparencia de la rendición de cuentas. Para sostener esta afirmación, remite a la protección de datos personales establecida en el capítulo V de la ley 18.331.[26] El mismo regula las bases de datos de titularidad pública, estableciendo que:

> *"El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función del grado de fiabilidad."*[27]

Por otra parte la norma excluye en su artículo 3 las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

De acuerdo al artículo 75 de la Ley 19.149, las empresas operadoras de servicios de telefonía móvil deberán llevar en forma actualizada una base de datos de los clientes que hubieran contratado servicios bajo cualquier modalidad, ya sea para servicios prepagos o postpagos. Esta base de datos está amparada por la Ley N° 18.331 de protección de datos personales.

2.3.4 La vigilancia de las comunicaciones en las actividades de inteligencia

Uruguay cuenta con un proyecto de ley destinado a regular el llamado Sistema Nacional de Inteligencia. Uno de los artículos del proyecto llama la atención debido a su carácter garantista:

"Artículo 14.- Toda operación de búsqueda de información que deba realizar cualquier organismo componente del Sistema de Inteligencia del Estado, involucrando procedimientos especiales que puedan afectar la libertad y privacidad de los ciudadanos, deberá ser autorizada por el Poder Judicial. A tales efectos, la Suprema Corte de Justicia determinará el órgano judicial competente para actuar en esta materia. Las actuaciones serán de carácter reservado."

Por otra parte, el artículo 15 establece una serie de principios que deberían regular a los actores en esta materia:

"Artículo 15.- En la recolección y tratamiento de la información, los organismos que integran el Sistema de Inteligencia del Estado deberán ajustar su actuación a los siguientes principios:

- *Legitimidad: sometimiento pleno a la ley y actuación de acuerdo a la subordinación y responsabilidad orgánicas;*
- *Eficiencia: adecuada relación entre los medios puestos a disposición y la calidad y oportunidad del producto obtenida la inteligencia;*
- *Financiamiento: origen y aplicación adecuados de los fondos asignados a los servicios, incluso los reservados;*
- *Legalidad: estricta observancia de la Constitución y la ley en aquellos procedimientos que, inevitablemente, requieran de actividades invasivas de la privacidad de los individuos;*
- *Necesidad y diseminación: se requerirá la información necesaria para la correcta y cabal ejecución de las funciones en cada una de las áreas anteriormente definidas, y se resguardará para tales fines;*
- *Asegurar que la información no sea empleada en beneficio de persona, organización privada o partido político alguno."*

Sin embargo, en otras secciones, el proyecto establece severas restricciones al derecho al acceso a la información pública.

III.
Casos de vigilancia relevantes

A diferencia de otros países, el Poder Judicial uruguayo no incorpora en sus fallos dictámenes de la Corte Interamericana de Derechos Humanos. Esto quiere decir que aún existiendo casos relevantes que pudieran ser de uso local, los mismos son tradicionalmente ignorados. Esto se debe a las características de los tribunales locales y que la Convención Americana de Derechos Humanos no es automáticamente incorporada al derecho uruguayo (aunque la misma sí forma parte de la legislación de este país).

En el ámbito nacional, la Suprema Corte de Justicia ha expedido la sentencia 58/2009[28] sobre la vigilancia de las comunicaciones. En el presente caso, la defensa interpone recurso de inconstitucionalidad[29] contra los artículos 212 del Código del Proceso Penal y el Artículo 161 del Código Penal. La defensa argumentó que éstas disposiciones no ofrecen garantías necesarias para proteger el derecho a la libre comunicación conforme el artículo 28 de la Constitución. La defensa, también señaló que aquellas disposiciones vulneran la libertad de expresión consagrada en el artículo 29 de la Constitución, cuando se habilita escuchas que impediría el libre desarrollo de la misma.

Para la defensa, el indagado se encuentra en desventaja al desconocer la medida que ordenó interceptar sus comunicaciones. Señaló que el artículo 212 del C.P.P. atenta contra el debido proceso previsto en el artículo 12 de la Constitución. Sostuvo que aquellas disposiciones vulneran la seguridad jurídica de los ciudadanos, el cual es inherente a un régimen democrático republicano y al principio de legalidad.

La Suprema Corte de Justicia desestimó la excepción de inconstitucionalidad interpuesta, en base a los siguientes lineamientos:

- La defensa no fundamentó debidamente el interés directo y personal que se considera lesionado, ni la referencia al caso concreto; extremos indispensables para interponer la excepción de inconstitucionalidad;
- La Corte señaló que el artículo 212 del C.P.P., no vulnera el artículo 7 de la Constitución ni desprotege los derechos allí consagrados. Indicó que la interceptación de correspondencia y otras comunicaciones sólo procede en caso de interés general, específicamente para la comprobación del delito y está sujeta a previa autorización judicial;

- Respecto al artículo 161 del C.P., se entiende que éste no es violatorio del principio de legalidad, dado que enuncia las conductas tipificadas por el mismo y la pena que resulta de su ejecución;
- Por último, sobre las escuchas telefónicas, la Suprema Corte entiende que la defensa debió formular el planteo de la excepción de inconstitucionalidad en la etapa del pre-sumario, por lo que su solicitud resultaba extemporánea.

Consecuentemente, el máximo tribunal nacional entiende que la interceptación de las comunicaciones se ajusta a la Constitución. En el mismo sentido, el Tribunal de Apelaciones[30] indica que quienes en principio no están sometidos a un proceso penal también pueden ser sujetos a vigilancia en algunas actuaciones.

Otro caso de particular relevancia es la Sentencia No. 377/2013 del Tribunal de Apelaciones Penal 2º T.[31] Este caso resuelve un recurso de apelación interpuesto por la defensa contra la sentencia que condena al encausado como autor penalmente responsable de un delito de tráfico ilícito de estupefacientes en la modalidad de organización y financiamiento. El delito ocurrió en concurrencia con el delito de introducción en tránsito y transporte de estupefacientes.[32] Se considero un agravante por haberse consumado el delito mediante la participación de una asociación ilícita o de un grupo delictivo organizado.

La sentencia afirma la pertinencia de la interceptación de escuchas telefónicas para la comprobación del delito. Incluso en una de las secciones de la misma, se detalla cuál fue el procedimiento que se siguió para la autorización de la medida de vigilancia:

- Primero, el Fiscal actuante entendió que conforme al artículo 20 de la Convención de Naciones Unidas (conocida como Convención de Palermo), ratificada por ley 17.861 por nuestro país, el artículo 212 del Código del Proceso Penal y artículo 5 de la ley 18.494 era procedente la vigilancia electrónica al encausado.
- Segundo, por auto fundado que consta en el expediente, la jueza de primera instancia dispuso la vigilancia electrónica con carácter reservado. De esta forma no invalida el medio probatorio del encausado ni de las demás personas vinculadas o identificadas en el caso por el plazo de 60 días.
- Tercero, se consideró la proporcionalidad y necesidad de la escucha, haciendo hincapié que no existía otro medio más eficaz. Para reafirmar el análisis de estos principios, vale la pena citar el siguiente fragmento de la sentencia:

> *"El Juez tiene que valorar la proporcionalidad para vulnerar la regla general y en el caso vaya si se dan esos extremos: más de dos toneladas de cocaína fueron incautadas por lo que no sólo para la justificada orden de vigilancia electrónica sino para otro medio de*

prueba no prohibido es de aplicación este principio que nació en el Siglo XIX en Europa continental como forma de contener los abusos policiales y se instala en el siglo XX hasta nuestros días."

- Por último, la sentencia aclara que no se comprobó ninguna de las nulidades invocadas respecto de las escuchas telefónicas como medio de prueba. Se remite a la Suprema Corte de Justicia ya que se expidió sobre el artículo 212 del C.P.P. autorizando la interceptación de comunicaciones de terceros si existe motivo fundado para sospechar de su participación en el delito.

3.1 El Guardián

Se trata de un sistema de vigilancia electrónica proporcionada por la empresa brasileña Digitro Tecnología Ltda. El programa permite que 30 personas en forma simultánea accedan en tiempo real a los datos de tráfico y localización de 800 celulares y 200 teléfonos fijos. También habilita la creación de 100 cuentas espejo de suscripciones de e-mails y permite monitorear información pública de tres redes sociales.[33]

El Guardián fue comprado de forma secreta eludiendo el control ciudadano por parte del poder legislativo y la sociedad civil.[34] Según reportes iniciales, El Guardián es un software privativo que costó dos millones de dólares y cuyo costo de mantenimiento es de US$ 200.000 anuales.

El Guardián tiene tres actores básicos que deben participar necesariamente en su implementación: el Ministerio del Interior, el Poder Judicial y las empresas de telecomunicaciones. Desde que el gobierno realizó la compra secreta, no ha dispuesto una regulación específica para permitir establecer con claridad cómo El Guardián va a operar.

Según versiones difundidas en la prensa, el Ministerio de Economía ha emitido un decreto reservado (no público) que establece la necesidad que Uruguay cuente con equipos de tecnología.[35] El decreto, de fecha 28 de marzo de 2014, otorga exoneraciones tributarias a las empresas de telecomunicaciones para que adquieran equipos de alta tecnología solicitados por el Ministerio del Interior. Consecuentemente las empresas de telecomunicaciones han procedido a adquirir los equipos solicitados por el referido Ministerio.

El supuesto decreto del Ministerio de Economía establecería:

- Un protocolo de colaboración entre el ministerio y las empresas para que estas sepan cómo actuar ante cada caso;
- La responsabilidad penal, las sanciones en la ejecución y el incumplimiento de la interceptación;

- El costo por las interceptaciones sería reembolsado a las operadoras o proveedor de servicios de comunicaciones;
- Especifica detalladamente el manejo de datos y su conservación;
- Solo podría acceder al sistema personal autorizado;
- Las empresas tienen la obligación de brindar información sobre la localización geográfica de origen y destino de la comunicación.

En referencia al Ministerio del Interior, en una comparecencia frente al Parlamento,[36] motivado por un llamado a Sala de la oposición, el Ministro del Interior también defendió la compra de El Guardián.

El funcionario indicó que previa a la compra de El Guardián existían al menos 22 sistemas de interceptación operando en el país sin ningún tipo de control. Según el Ministro, El Guardián ofrece la posibilidad de centralizar los procesos de vigilancia y asegurarse que los mismos se realicen de forma legal y controlada.

Según describió el Ministerio del Interior, El Guardián tiene la capacidad de monitorear a objetivos en las redes sociales "abiertas", pero no interviene en la actividad de los usuarios. También las autoridades del Ministerio afirmaron contar con las condiciones de guardar los datos recolectados en un datacenter de última generación (*sic*) que han adquirido. El Ministerio también expresó a los legisladores que existirían listas blancas, personas que no serían objetivo de este instrumento, por ejemplo los legisladores.

Actores de la sociedad civil uruguaya cuestionaron la política de secretismo respecto a la compra y los protocolos que regulan la utilización de El Guardián.[37] También se criticó la falta de un marco normativo que garantice el respeto a los derechos humanos y los valores democráticos, incluso cuando las autoridades señalaron que debe existir una autorización judicial previa y que según la ley 18.494 se trata de un medio de prueba legal.

En referencia a la Suprema Corte de Justicia, la misma habría dado el visto bueno a este sistema a través de un memorándum de entendimiento con el Ministerio del Interior.[38] Teóricamente el Ministerio y la Corte han establecido un protocolo secreto para operar este sistema.

A pedido de los autores en el contexto de esta investigación, la Corte remitió una copia de un convenio de cooperación firmado con el Ministerio del Interior. Sin embargo, el mismo no establece ningún protocolo específico en este sentido. La información remitida solo

indica la existencia de un convenio marco, el cuál es demasiado general para dar alguna pista de cómo funcionaría el Guardián en el Poder Judicial.

La situación motivó que la directora ejecutiva del Centro de Archivo y Acceso a la Información Pública (CAINFO) presentara un pedido de acceso a la información pública por la compra secreta del sistema El Guardián.[39] El pedido no fue contestado por el Ministerio del Interior, organismo que adquirió el software. CAINFO entonces acudió a la justicia para activar los mecanismos legales correspondientes a la ley de acceso a la información pública.

Este pedido fue denegado por la justicia en primera instancia por el Juzgado Letrado en lo Contencioso Administrativo de 1er. Turno. También fue denegado en segunda instancia por el Tribunal de Apelaciones en lo Civil de 5to. Turno. En consecuencia la resolución de primera instancia quedó firme, es decir, que las cortes defendieron la posición según la cual "la difusión pública de sus fortalezas y debilidades [del sistema] podría frustrar el empleo (del instrumento) en esa tarea".[40]

Los argumentos clave en la demanda para abogar a favor de la liberación se basaron en la amplia tutela del derecho al acceso a la información pública y el principio de divisibilidad de la información pública. En particular, la demandante expresó:

> *"Al examinar el marco jurídico planteado no puede más que concluirse que la información solicitada debe estar a disposición del público. En ningún caso puede admitirse una clasificación genérica de toda la información relativa a El Guardián que impida, nada más y nada menos, que el escrutinio público sobre los sistemas de vigilancia de telecomunicaciones que empleará el Estado. Ello constituiría una violación flagrante de los derechos humanos a la información y participación ciudadana e implicaría desconocer todos los estándares y garantías en materia de clasificación de información pública."*

Sin embargo, el Tribunal de Apelaciones en lo Civil de 5to. Turno argumentó que la *"parte actora equivocó su estrategia, pues en vía administrativa y en su demanda, pretendió acceso a información claramente cubierta por el secreto."* El tribunal agrega que "el derecho al acceso a la información no tiene carácter absoluto o irrestricto, pues la protección de otros derechos constitucionalmente consagrados determina que puedan existir excepciones legales al deber de brindar información correlativo a aquel derecho."

En ese sentido, el Tribunal insistió que:

> *"Parece obvio que el secreto de la operación de adquisición del sistema operativo "guardián", avalado por el Tribunal de Cuentas, radica no solamente en la compra*

en sí misma (que, incidentalmente, no fue oculta) sino que también alcanza a las características técnicas del producto adquirido, por simples razones de seguridad y protección de los derechos de todos los habitantes que se busca tutelar mediante la prevención y represión de ilícitos, a través del empleo de instrumentos como el adquirido. Se trata de un instrumento para el combate del delito y la difusión pública de sus fortalezas y debilidades podría frustar el empleo en esa tarea, dejándola librada a la actividad de "hackers" y/o personas que ilegitimamente pretendan obstaculizar o impedir investigaciones o represiones sometidas a control jurisdiccional, como bien expuso la parte demandada, con apoyo en normativa legal y administrativa específica..."

La asociación civil DATA presentó junto a CAINFO un *amicus curiae* donde desarrolló los siguientes argumentos.

"El secretismo de la regulación administrativa que regula el uso de El Guardián es sumamente preocupante. En realidad, no debería ser necesario utilizar una norma de acceso a la información para conocer una protocolo administrativo que debe ser público por defecto. El Estado no debería adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una normativa públicamente disponible.[41]

Resulta fundamental acceder a reglas que regulan el uso de El Guardián y cualquier otro sistema de vigilancia. Ello es necesario para conocer las garantías que el Ministerio del Interior, con un rol relevante dentro del nuevo sistema, ha previsto en cuanto a la recolección, sistematización, tratamiento, custodia, y destrucción de datos, entre otros, que se obtendrán mediante la intercepción de llamadas telefónicas y correos electrónicos.

La adquisición de la plataforma tecnológica El Guardián aumenta de manera exponencial la capacidad de vigilancia del Estado sobre las personas. La experiencia internacional indica que este tipo de plataforma tecnológica engloba un riesgo alto para la privacidad de las personas y puede abrir la puerta para potenciales abusos de poder.

Hoy, gracias a la prensa y a la admisión del propio Ministerio sabemos que existe un protocolo, que originalmente era desconocido por la ciudadanía. Pero poco sabemos sobre su naturaleza y su estructura. Tal noción debe ser rechazada por un Estado de derecho.

¿Cómo se resolverán los potenciales problemas de implementación en caso que los derechos de las personas sometidas a vigilancia sean vulnerados?; ¿Quién será el encargado de controlar a los funcionarios administrativos a cargo de operar la plataforma y qué procedimientos se deben seguir para llamarlos a responsabilidad?; ¿Serán también órganos secretamente constituidos por resoluciones administrativas?, son cuestionamientos que el

Ministerio del Interior debe responder, más allá del mencionado control jurisdiccional a la plataforma El Guardián.

Esta incertidumbre y secrecía no es deseable para ninguna democracia. En el caso particular de la democracia uruguaya, se vulnera el principio esencial de publicidad de las normas jurídicas. El caso es particularmente grave, porque la administración solo puede hacer lo que la ley y su reglamentación indica, y la única garantía para sus ciudadanos es el control y conocimiento de esa legislación y normativa, control que no se puede realizar si se desconoce el contenido de las normas. En conclusión, no es admisible que el Ministerio pretenda con un acto dadivoso cumplir con lo que en realidad es su deber.

El amicus curiae fue rechazado por el Tribunal.

3.2 Hacking Team

Debido a las revelaciones de los correos electrónicos de la firma italiana Hacking Team en el mes de julio de 2015, se ha tenido conocimiento que las autoridades uruguayas sostuvieron reuniones con la misma a través de un empresario paraguayo. Esta firma se dedica a la venta de tecnología ofensiva de vigilancia, lo que supone una interferencia con el derecho a la privacidad y libre expresión mas seria que una simple interceptación de comunicaciones.[42]

IV.

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

En este apartado se analiza la regulación y práctica uruguaya a la luz de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

Principio 1: 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.*[43]

En general, se cumple con este principio dado que la interceptación de las comunicaciones y la vigilancia electrónica están establecidas en las normas uruguayas que han sido citadas y analizadas en el cuerpo de este informe.

Sin embargo, estas normas no son lo suficientemente precisas ni claras cuando se trata de nuevas herramientas de vigilancia como El Guardián. Tampoco la normativa establece procedimientos expresos que autoricen el uso de tecnología ofensiva, como el software malicioso, que supone la infiltración a dispositivos electrónicos tales como teléfonos celulares o computadoras; modalidades de vigilancia que son mucho más intrusivas que una simple interceptación de una comunicación.

De igual forma, si bien la limitación existe a nivel de derecho internacional de derechos humanos y la normativa nacional, no es claro a nivel administrativo como operan estas tecnologías. Tampoco existe una discusión profunda acerca de la legalidad de las normas secretas (como el mencionado decreto reservado del Ministerio de Economía).

Finalmente, los reglamentos o acuerdos que regulan el acceso del Estado a los datos recolectados por las operadoras de telecomunicaciones no están disponibles al público. La

ausencia de una norma disponible para los usuarios no cumple con el Principio de Legalidad.

Principio 2: Objetivo Legítimo

> *Las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática.*
>
> *Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.*[44]

Del desglose de la normativa vigente, se desprende que las medidas de prevención y detección del delito corresponden a un objetivo legítimo.

La regulación uruguaya establece que, en principio es el Ministerio del Interior, el Ministerio Público y el Juez competente quienes pueden realizar las actividades de vigilancia. Sin embargo, existen otras agencias con capacidad de vigilancia que no se encuentran cubiertas por la ley y quienes consecuentemente podrían operar por fuera de objetivos legítimos. Esto es particularmente preocupante respecto a los sectores de inteligencia que no se encuentran regulados.[45]

Principio 3: Necesidad

> *Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo.*
>
> *La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.*[46]

Al desconocerse los protocolos o reglamentos de actuación del Ministerio del Interior frente a los casos de vigilancia no es posible analizar con cabalidad la vigencia o no de este principio. La práctica actual indica que según el Ministro del Interior existen al menos 22 sistemas de escucha operando en paralelo en Uruguay, pero el Ministerio no ha justificado su necesidad.[47]

Cabe mencionar, que la legislación uruguaya no ha implementado expresamente la prueba *de necesidad* conforme lo establecido por el derecho internacional de los derechos humanos.

Principio 4: Idoneidad

> *Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.*[48]

Para determinar si la vigilancia de las telecomunicaciones es el medio adecuado y propicio para lograr el objeto legítimo que la motivó deberíamos analizar cada caso. De todas maneras, se reconoce que actualmente la interceptación de telecomunicaciones está siendo utilizada con mayor frecuencia como una de las pruebas claves en la investigación de delitos de narcotráfico y otros como corrupción.

En una entrevista realizada por el diario El País al fiscal especializado en crimen organizado Juan Gómez declaró que no advierte "una tendencia exagerada en el uso" de las interceptaciones telefónicas.[49]

Gómez declaró que: *"La interceptación se dispone tras un estudio previo y en caso de la existencia de indicios que determinan si la persona está implicada en una actividad ilícita."* Pero al respecto el Dr. Fagúndez afirmó que: "es muy común" que primero la Policía intervenga el teléfono y sólo, cuando consigue información que puede ser de interés, [la Policía] tramita la autorización judicial.[50]

Principio 5: Proporcionalidad[51]

> *La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática.*
>
> *Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.*

Operadores del sistema afirman que "se valora la necesidad y la racionalidad" de la utilización de la medida, ya que es un mecanismo que invade la privacidad de las personas.[52] Sin embargo, no existe en la legislación nacional criterios adicionales que sean claros y que permitan evaluar la proporcionalidad de una medida de vigilancia.

Del examen del marco normativo vigente, se desprende que para que se trate de una medida proporcional deberán cumplirse los siguientes requisitos: (i) que se trate de la investigación

de un delito, (ii) que existan motivos graves para creer que esta medida podría garantizar la prueba suficiente en la comprobación de un delito, y (iii) que sea solicitado por el Ministerio Público al Juez de la investigación.

Principio 6: 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.*[53]

El Ministerio Público (el fiscal) es quien solicita la autorización de vigilancia al Poder Judicial. El Poder Judicial es la autoridad encargada de autorizar la solicitud. El Ministerio del Interior (la policía Nacional de Uruguay) y el Poder Judicial han realizado recientemente un convenio para la operación de El Guardián aunque el mismo no se encuentra aun en operación.

Una evaluación acerca de las capacidades y recursos del Poder Judicial requiere de un mayor análisis que está fuera del alcance del presente informe.

Principio 7: Debido Proceso

> *El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.*[54]

El marco legal que regula la vigilancia en Uruguay es insuficiente. En particular, los reglamentos o acuerdos que regula el acceso del Estado a los datos recolectados por las operadoras de teléfono e internet no están disponibles al público infringiendo tanto el Principio de Debido Proceso y el Principio de Legalidad.

Principio 8: Notificación del Usuario

> *Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados 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 soluciones y deben 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:*
>
> *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 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 el usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.*
>
> *La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones debe tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.*[55]

Esta obligación no se encuentra regulada en el marco legal uruguayo analizado previamente. Sin embargo, sí existe la notificación diferida en la que se comparte el material interceptado con el imputado para que pueda ejercer su derecho de defensa en la audiencia.

Principio 9: 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. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de*

> *solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.*[56]

Si bien la Unidad Reguladora de Datos Personales[57] sostiene que se tomaron las medidas pertinentes para asegurar la transparencia y la rendición de cuentas cuando se conduce la vigilancia, en realidad las mismas no son suficientes frente a los avances de las técnicas y tecnologías de vigilancia.

A pedido de un senador, la Suprema Corte reveló que entre enero de 2009 y marzo de 2014, los jueces con competencia en la materia penal ordenaron un total de 6.150 escuchas telefónicas,[58] lo que arroja un promedio de tres por día. En ese mismo período, las sedes que más interceptaciones dispusieron son las dos especializadas en crimen organizado, que autorizaron 2.192 interceptaciones.

Consecuentemente a la fecha se tienen datos muy parciales acerca de la utilización de medidas de vigilancia. No existe publicación proactiva de esta información ni un estándar para la publicación de la misma.

Principio 10: 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.*[59]

Uruguay cuenta con una serie de instituciones que podrían constituir dos mecanismos de supervisión de la vigilancia de las telecomunicaciones:

- Ley 18.331 que establece la protección de Datos Personales y la acción de Hábeas Data.
- Ley 18.381 que tutela el Derecho de acceso a la Información Pública y garantiza la transparencia de la gestión pública del Estado.

Sin embargo el funcionamiento en la práctica de ambos mecanismos es complejo. De igual forma existen comisiones parlamentarias que monitorean parcialmente estos temas en el Senado.

Principio 11: Integridad de las Comunicaciones y Sistemas

> *A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado.*
>
> *La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anonimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios.*[60]

El artículo 20 de la ley 18.331, determina que los operadores que exploten redes públicas o que prestan servicio de comunicación electrónicas deben garantizar la protección de datos personales. En Uruguay, no existe una norma especifica que regule la retención obligatoria de datos de la población entera por parte de las operadores de telefonía e internet por cierto periodo de tiempo, mas varias de ellas retienen los datos voluntariamente.

Principio 12: Garantías para la Cooperación Internacional

> *En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estándar disponible con el mayor nivel de protección para las personas. El principio de la doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para burlar las restricciones del derecho interno relativas a la Vigilancia de las Comunicaciones. Los procesos de asistencia judicial recíproca y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.*[61]

Uruguay ha firmado y ratificado la Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT en inglés).[62] El artículo segundo de la Convención es la única disposición de este tratado aplicable a materia de vigilancia.

El artículo indica que los Estados Partes se prestarán asistencia mutua en investigaciones, juicios y actuaciones en materia penal referentes a delitos cuyo conocimiento sea de competencia del Estado requiriente al momento de solicitarse la asistencia (...) Esta Convención se aplica únicamente a la prestación de asistencia mutua entre los Estados Partes; sus disposiciones no otorgan derecho a los particulares para obtener o excluir pruebas, o para impedir la ejecución de cualquier solicitud de asistencia".

En relación a los compromisos vigentes en Uruguay sobre cooperación internacional en materia de protección de datos, se encuentran:

- Convenios de cooperación en materia de protección de datos personales con diversos países;
- Miembro de la Red Iberoamericana de Protección de Datos y del Comité Organizador de la Conferencia Internacional de Protección de Datos;
- Convenio No 108 ante el Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional a las autoridades de control y a los flujos transfronterizos de datos.
- País adecuado a los estándares de la Unión Europea de conformidad con la "Directiva 95/46/CE", lo que significa que cumple con los estándares de protección de datos establecidos en la Unión Europea. Sin embargo este acuerdo está limitado a la protección y transferencia de datos personales entre Europa y Uruguay.

Principio 13: Garantías contra el Acceso Ilegítimo y Derecho al Recurso Efectivo

> *Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "whistleblowers" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información.*
>
> *Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue*

obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.[63]

Toda interceptación ilegal de las comunicaciones en Uruguay constituye un delito de acuerdo al código Penal Uruguayo. No existe la figura de la protección al denunciante o "whistleblower".

V.
Conclusiones

El presente trabajo ha buscado analizar el marco actual de la vigilancia en materia de comunicaciones en Uruguay. A continuación se presentan una serie de conclusiones para avanzar el debate en este país en función de los principios analizados.

5.1 Nueva Regulación

- Uruguay presenta una serie de nuevos desarrollos, que ameritan proponer una nueva regulación en materia de vigilancia de las comunicaciones y derechos humanos. El objetivo es dejar claro los límites de los poderes de vigilancia y las reglas para que el Estado pueda acceder a los datos de las personas almacenados por las operadoras de telecomunicaciones o terceras empresas.
- El caso de El Guardián así como las tratativas para la compra de tecnología ofensiva (malware), son hechos que demuestran una tendencia por parte del gobierno hacía la compra y el uso de modernas tecnologías con el fin de incrementar el alcance y capacidad del Estado de vigilar las comunicaciones de la ciudadanía.
- La regulación actual es insuficiente para limitar claramente esta actividad. En consecuencia, existe un reto latente para la privacidad, la libertad de expresión y derecho de asociación en la era digital.
- A la fecha, no conocemos caso alguno en que el gobierno de Uruguay haya usado herramientas de vigilancia contra grupos específicos de la población o con intencionalidad política.
- Uruguay requiere de una reforma normativa que asegure el derecho de las personas a comunicarse sin que sus comunicaciones sean ilegalmente interceptadas por las agencias de inteligencia y seguridad. Los Principios analizados en este trabajo puede ofrecer una guía en este sentido. La idea de proteger la integridad de las comunicaciones no es nueva, pues ya se encuentra presente en la Constitución uruguaya desde 1830. Sin embargo la capacidad técnica del gobierno se ha incrementado al utilizar sistemas que pueden facilitar la vigilancia de una gran cantidad de personas.
- En Uruguay existe un marco de protección robusta y general de los derechos humanos. Sin embargo, ese marco no es lo suficientemente específico para cubrir las nuevas situaciones planteadas por estas tecnologías.

- Este marco no establece con claridad: criterios objetivos para tener a una persona o grupo de personas bajo vigilancia; criterios objetivos para establecer la duración de un procedimiento de vigilancia y los derechos de las personas sujetas a vigilancia; reglas claras para que el Estado acceda a los datos almacenadas por las operadores de Internet y telefonía.

5.2 Necesidad y Objetivo Legítimo

- Los indicios encontrados en el curso de esta investigación muestran que existe una fuerte preocupación en las autoridades locales por la lucha contra el crimen organizado, y que la compra de estas herramientas obedece a esa prioridad. Sin embargo, no existe una justificación por parte del Estado sobre la necesidad de las mismas.
- El Estado tampoco justifica la existencia en el país de veintidós sistemas sin control previos El Guardián, pero presumiblemente aún en operaciones, que diversas agencias, utilizaban para interceptar las comunicaciones de la ciudadanía. Esta línea de base es preocupante, y requiere de acción inmediata.
- El marco actual de vigilancia opera, a nuestro entender, para un grupo determinado de delitos a pesar que las autoridades argumentan que se trata de una habilitación general. Definir un marco comprensivo y coherente para esta delicada actividad sería lo más adecuado.

5.3 Derecho a la Notificación al Usuario

- Uruguay debería establecer reglas para que el Estado notifique al usuario cuando la investigación no se encuentra en riesgo.

5.4 Autorización Judicial, Transparencia y Acceso Ilegítimo

- El marco normativo uruguayo tiene la virtud que la autorización de la vigilancia debe hacerse mediante el Poder Judicial y a pedido de un fiscal. A su vez la compra de la tecnología El Guardián tendría la virtud de permitir que este proceso pudiera auditarse dado que los usuarios quedarían registrados.
- Sin embargo, en el marco actual no es posible saber quién, bajo qué condiciones y motivos, se sometió a una persona determinada a la vigilancia. Si bien es posible esgrimir que existe una protección constitucional a este derecho, el mismo necesita de protecciones legales mas especificas.
- Tampoco es claro qué acontece con la información que se descarta en estos procesos, o con las personas que han sido expuestas a la actividad de vigilancia por error. Esto

se agrava porque en principio, la regulación sobre protección de datos personales no aplica a bases de datos en materia de defensa y seguridad.

- También debe establecerse sanciones claras para quienes utilicen estas tecnologías fuera del marco legal adecuado. La regulación del Código Penal actual es insuficiente.

5.5 Debido Proceso

- Las autoridades no han informado sobre la forma de procedimiento y el protocolo de actuación para operar la plataforma El Guardián. De la evidencia disponible surge que, tras sendas demandas judiciales, existe en Uruguay una regulación administrativa que es secreta a la ciudadanía. Esto establece una especie de "marco regulatorio secreto", similar a otros desarrollos en los Estados Unidos de América o Gran Bretaña, lo cual no es compatible con un régimen de Estado de Derecho.
- Consecuentemente es necesario que existan los contralores adecuados sobre este tipo de herramientas y su regulación, lo que incluye la publicidad de las normas con las que operan. Distinto es conocer detalles técnicos sobre su operación que pudieran vulnerar el propósito inicial de la herramienta, lo cual a la fecha nadie ha solicitado.

5.6 Transparencia

- No existe información periódica y agregada sobre las solicitudes de vigilancia autorizadas y rechazadas, desde pedidos de interceptación de comunicaciones hasta solicitudes de acceso a los datos almacenados por terceros. Si bien las autoridades han informado sobre las escuchas telefónicas al Parlamento, así como respondido algunos pedidos específicos sobre este tema, no presentan una práctica de informar sistemáticamente sobre estas actividades.
- Es necesario contemplar estándares de transparencia para el propio Ministerio y una publicación proactiva de este tipo de información. También debe establecerse un adecuado control del Poder Legislativo y la sociedad civil sobre este punto.
- La publicación de esta información probablemente ayude a un debate más amplio y franco sobre el tema. Servirá como bases para un diálogo entre las autoridades y la sociedad civil en Uruguay.

5.7 Transparencia en los Procedimientos de Compra

- Existe la necesidad de transparentar los procedimientos de compra de estas herramientas a los efectos que exista un adecuado control parlamentario de los mismos. La discusión acerca de qué principios seguir, puede ser guiada por los Principios analizados en este informe.
- Además de los aspectos legales, existen aspectos vinculados a la capacidad de los Estados, y en particular de las agencias de seguridad al evaluar la tecnología que están adquiriendo. Las soluciones que a la fecha el Estado ha adquirido no son de software libre o abierto, lo que impide auditar las mismas en caso que existan posibles puertas traseras (back-doors).

5.8 Retención Voluntaria de Datos

- Si bien la legislación uruguaya no regula la retención obligatoria de datos por parte de los operadores, poco se sabe sobre la retención voluntaria que realizan las operadoras y su cumplimiento (o no) con las normas de protección de datos.
- Los pedidos de la Justicia a los operadores de telecomunicaciones acerca de mensajes de texto y ubicación geográfica de celulares, hace suponer que los operadores de telecomunicación uruguayos retienen información sobre sus clientes mas no queda claro por cuanto tiempo ni qué tipo de datos.

5.9 Cifrado

- No existe en Uruguay prohibición para cifrar las comunicaciones, ni normas que obliguen a las empresas que proveen servicios de cifrado a colocar puertas traseras a sus productos. Los estándares en materia de derechos humanos protege el uso del cifrado como mecanismo para ejercer el derecho a la libertad de expresión y el derecho a la privacidad.

5.10 Servicios de Inteligencia

- La legislación uruguaya es incompleta en cuanto a la vigilancia realizada por las agencias de inteligencia. El proyecto no aprobado en esta materia hubiera dado una guía adecuada para estas agencias.

VI.
Bibliografía

Cortizas, G. El Guardián: Gobierno pone en marcha súper espía informático. EL País. 25 de Marzo del 2015. Disponible en: http://www.elpais.com.uy/informacion/guardian-gobierno-pone-marcha-super.html [Accedido 18 Septiembre, 2015].

Corujo Guardia, William, Acerca de las escuchas telefónicas como medio de prueba y el derecho constitucional a la intimidad. Cita Online: UY/DOC/250/2012

Declaración conjunta Vigilancia, Seguridad y Privacidad: Llamamiento para que Uruguay Adopte Estándares de Derechos Humanos, 2014. Disponible en: https://eff.org/r.1dss [Accedido 6 de Septiembre 2015]

De los Santos, F., (2015). ¿Quién vigila a los vigilantes? La Diaria. Disponible en: http://ladiaria.com.uy/articulo/2015/3/quien-vigila-a-los-vigilantes/ [Accedido 18 de Septiembre, 2015].

Diario El Observador (2015). El Guardián espiará desde enero mails y celulares. Disponible en: http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757. [Accedido 29 de Septiembre, 2015]

Diario EL PAÍS Uruguay. Los Gobiernos de la Región Potencian Capacidad para Espiar (2015). Noticias Uruguay y el Mundo actualizadas - Diario EL PAIS Uruguay. Disponible en: http://www.elpais.com.uy/informacion/gobiernos-region-potencian-capacidad-espiar.html [Accedido 17 de Septiembre, 2015]

Diario EL PAÍS Uruguay (2015). Bonomi: "El Guardián" da más garantías que el sistema actual. Noticias Uruguay y el Mundo actualizadas, Diario EL PAIS Uruguay, 2015. Disponible en: http://www.elpais.com.uy/informacion/bonomi-guardian-garantias-sistema-actual.html. [Accedido 19 de Agosto, 2015].

Diario EL PAÍS Uruguay. Polémica por escuchas telefónicas. Penalistas. Alertan "pinchazos" sin orden de juez y grabación de diálogos indagado-abogado, Diario EL PAÍS Uruguay, 04 Noviembre 2012.

EFF, ARTICLE19. Análisis Jurídico Internacional de Apoyo y Antecedentes , 2014. Disponible en: https://es.necessaryandproportionate.org/analisislegal [Accedido 16 de Septiembre 2015], Access, Guía Universal de Implementación, 2015. Disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Accedido 16 de Septiembre 2015]

Gomes, Santoro, Fernando. Prueba Ilícita y Prueba Irregular. Admisibilidad de Grabación de Voz y/o Imagen Sin Autorización. Comentario a la sentencia del Tribunal de lo Contencioso Administrativo N° 591/2011 del 16 de Agosto del 2011, Caso Francisco Casal C/ DGI. Publicado en: LJU Tomo 149 Cita online: UY/DOC/38/2014)

González, José Luis. Control y Prevención de Lavado de activos y financiamiento del Terrorismo. Ley N° 18.494, 2010. En: Revista de Facultad de Derecho, 29, 137-159. Disponible en: http://www.fder.edu.uy/contenido/penal/pdf/2010/gonzalez.pdf [Accedido 1 de Agosto, 2015]

Gros Espiell, Héctor. La Constitución y los Tratados Internacionales, Revista del Colegio de Abogados del Uruguay Volumen II, Montevideo, 2da edición.

Kutz, Christopher. De la Repugnancia de la Ley Secreta [The Repugnance of Secret Law]. Disponible en: https://www.law.upenn.edu/live/files/2398-kutz-the-repugnance-of-secret-law-full [Accedido 15 de Marzo, 2015]

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.

McMullan,Thomas (2015). The world's first hack: the telegraph and the invention of privacy. The Guardian. Disponible en: https://eff.org/r.xuol [Accedido 1 de Agosto, 2015]

Melendrez, P., 2014. Escuchas se disponen con "prudencia", dicen jueces. EL PAIS, 26 de Abril del 2014. Disponible en: http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.html [Accedido 30 de Abril, 2015].

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2014). Disponible en: https://es.necessaryandproportionate.org/text [Accedido 6 de Septiembre, 2015]

Poder Judicial Uruguay. Tribunal Civil 5º Rechaza Apelación Sobre "El Guardián" y Señala Error Estratégico de la Accionante, 2015. Disponible en: https://eff.org/r.qayy [Accedido 15 de Marzo, 2015]

Suprema Corte de Justicia, Sentencia 58/2009. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359

Tribunal De Apelaciones Penal 2º T, Sentencia 377/2013. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37314 Tribunal de Apelaciones 2º T ,Sentencia 80/2006. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359

Terra,Gonzalo (2013). Gobierno compró "El Guardián" para espiar llamadas y correos. El País. Disponible en: https://eff.org/r.5fvk [Accedido 16 de Septiembre, 2015]

Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay, 2014. El Derecho a la Privacidad en la Era Digital: A/RES/68/167. Disponible en: http://www.ohchr.org/Documents/Issues/Privacy/Uruguay.pdf [Accedido 16 de Septiembre, 2015]

1 Terra, Gonzalo (2013). *Gobierno compró "El Guardián" para espiar llamadas y correos*. El País. Disponible en: https://eff.org/r.5fvk [Accedido 16 de Septiembre, 2015].

2 *Declaración Conjunta Vigilancia, Seguridad y Privacidad: Llamamiento para que Uruguay Adopte Estándares de Derechos Humanos* (2014). Disponible en: https://eff.org/r.1dss [Accedido 6 de Septiembre, 2015].

3 McMullan, Thomas (2015). The world's first hack: the telegraph and the invention of privacy. The Guardian. Disponible en: https://eff.org/r.xuol [Accedido 1 de Agosto, 2015].

4 *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (2014). Disponible en: https://es.necessaryandproportionate.org/text [Accedido 6 de Septiembre, 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.

5 Ibíd., La Rue, pág 4.

6 *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,* 2014. Disponible en: https://es.necessaryandproportionate.org/text [Accedido 16 de Septiembre, 2015], EFF, ARTICLE19. *Análisis Jurídico Internacional de Apoyo y Antecedentes*, 2014. Disponible en: https://es.necessaryandproportionate.org/analisislegal [Accedido 16 de Septiembre 2015], Access, *Guía Universal de Implementación,* 2015. Disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Accedido 16 de Septiembre, 2015].

7 Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

8 Artículo 17: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

9 Artículo 11 Protección de la Honra y de la Dignidad: 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

10 Gros Espiell, Héctor. *La Constitución y los Tratados Internacionales*, Revista del Colegio de Abogados del Uruguay Volumen II, Montevideo, 2da edición.

11 Un nuevo Código del Proceso Penal entrará en vigencia en 2017.

12 Artículo 146: 146.1) Son medios de prueba los documentos, la declaración de parte, la de testigos, el dictamen pericial, el examen judicial y las reproducciones de hechos. 146.2) También podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho, aplicando analógicamente las normas que disciplinaría a los expresamente previstos por la ley.

13 González, José Luis (2010). *Control y Prevención de Lavado de activos y financiamiento del Terrorismo*. Ley N° 18.494. En: Revista de Facultad de Derecho, 29, 137-159. Disponible en: http://www.fder.edu.uy/contenido/penal/pdf/2010/gonzalez.pdf [Accedido 1 de Agosto, 2015].

14 Sin embargo, cierto sector de la doctrina nacional parece estar de acuerdo en la admisibilidad de la prueba aún si esta ha sido obtenida inicialmente de forma ilícita. A modo de ejemplo, si la interceptación de la comunicación se realizó sin orden judicial por un privado, la licitud de la prueba estaría en duda, y sería el tribunal quien deba evaluar si la admite o no. Consecuentemente la vigilancia por medios electrónicos, puede en principio ser utilizada como medio de prueba en un tribunal judicial siempre y cuando la evidencia haya sido obtenida conforme a la normativa nacional.

15 González, José Luis, *op. cit.*, p. 148.

16 Uruguay es uno de los pocos países en América Latina que mantiene un sistema de proceso penal basado en principios inquisitorios, a diferencia de modelos más garantistas basados en el principio acusatorio. Dicho lo anterior, cabe aclarar que nuestro sistema procesal penal es mixto inquisitivo en las primeras fases (Pre-sumario y Sumario) y acusatorio en las últimas fases (Ampliación Sumarial y Plenario). Las características que se mantienen del sistema inquisitivo son: proceso escrito, discontinuado y desconcentrado, el juez instructor será el juez que dicte la sentencia. Sobre este tema puede consultar González y Patrón. *Manual Básico del Proceso Penal* (2010). Cabe aclarar, que Uruguay ya ha aprobado un nuevo sistema basado en el principio acusatorio del proceso penal (proceso que exige una correlación entre la acusación y la sentencia), aunque este sistema aún no se ha implementado. Disponible en: http://www.fder.edu.uy/material/gonzalez-maria-prato-magdalena_manual-basico-proceso-penal.pdf. [Accedido 20 de Septiembre, 2015].

17 González, José Luis, *op. cit.*, p. 148.

18 Corujo Guardia, William, *Acerca de las escuchas telefónicas como medio de prueba y el derecho constitucional a la intimidad*. Cita Online: UY/DOC/250/2012. El mandato verbal es una práctica aceptada en el Poder Judicial uruguayo para actos administrativos dentro del Poder Judicial.

19 Artículo 8.- Los delitos tipificados en los artículos 54 a 57 del Decreto-Ley Nº 14.294, de 31 de octubre de 1974. Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=14294&Anchor=, se configurarán también cuando su objeto material sean los bienes, productos o instrumentos provenientes de delitos tipificados por nuestra legislación vinculados a las siguientes actividades:

- Crímenes de genocidio, crímenes de guerra y de lesa humanidad tipificados por la Ley Nº 18.026, 25 de Septiembre de 2006. Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18026&Anchor [Accedido 16 de Septiembre, 2015];
- Terrorismo; financiación del terrorismo; contrabando superior a US$20.000 (veinte mil dólares de los Estados Unidos de América); tráfico ilícito de armas, explosivos, municiones o material destinado a su producción; tráfico ilícito de órganos, tejidos y medicamentos; tráfico ilícito y trata de personas; extorsión; secuestro; proxenetismo; tráfico ilícito de sustancias nucleares; tráfico ilícito de obras de arte, animales o materiales tóxicos; estafa; apropiación indebida; los delitos contra la Administración Pública incluidos en el Título IV del Libro II del Código Penal y los establecidos en la Ley Nº 17.060, de 23 de diciembre de 1998 (delitos de corrupción pública). Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17060&Anchor [Accedido 16 de Septiembre 2015];
- Quiebra fraudulenta; insolvencia fraudulenta; el delito previsto en el artículo 5º de la Ley Nº 14.095, de 17 de noviembre de 1972 (insolvencia societaria fraudulenta). Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=14095&Anchor=#art5%C2%BA [Accedido 16 de Septiembre, 2015];
- Delitos previstos en la Ley Nº 17.011, de 25 de Septiembre de 1998 y sus modificativas (delitos marcarios) http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17011&Anchor [Accedido 16 de Septiembre, 2015];

- Delitos previstos en la Ley Nº 17.616, de 10 de enero de 2003 y sus modificativas (delitos contra la propiedad intelectual). Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17616&Anchor [Accedido 16 de Septiembre, 2015];

- Las conductas delictivas previstas en la Ley Nº 17.815, de 6 de Septiembre de 2004. Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17815&Anchor, en los artículos 77 a 81 de la Ley Nº 18.250 de 6 de Enero 2008. Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18250&Anchor [Accedido 16 de Septiembre, 2015],

- Conductas ilícitas previstas en el Protocolo Facultativo de la Convención de los Derechos del Niño sobre venta, prostitución infantil y utilización en pornografía o que refieren a trata, tráfico o explotación sexual de personas. Disponible en: http://www.parlamento.gub.uy/htmlstat/pl/protocolos/prot17559.htm [Accedido 16 de Septiembre, 2015] Disponible en: http://www.parlamento.gub.uy/htmlstat/pl/convenciones/conv16137.htm [Accedido 16 de Septiembre, 2015];

- La falsificación y la alteración de moneda previstas en los artículos 227 y 228 del Código Penal".

20 Meléndrez, P. *Escuchas Se Disponen con "Prudencia", Dicen Jueces.* EL PAÍS. 26 Abril del 2014. Disponible en: http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.html [Accedido 30 de Abril, 2015].

21 Código Penal uruguayo: Artículo 296. (Violación de correspondencia escrita): Comete el delito de violación de correspondencia el que, con la intención de informarse de su contenido, abre un pliego epistolar, telefónico o telegráfico, cerrado, que no le estuviera destinado. Este delito se castiga con 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables) de multa. Los que abran, intercepten, destruyan u oculten correspondencia, encomiendas y demás objetos postales con la intención de apropiarse de su contenido o interrumpir el curso normal de los mismos, sufrirán la pena de un año de prisión a cuatro de penitenciaría. Constituye circunstancia agravante de este delitos, en sus dos formas, el que fuera cometido por funcionario público perteneciente a los servicios que en cada caso se tratare.

- Artículo 297. (Interceptación de noticia, telegráfica o telefónica): El que, valiéndose de artificios, intercepta una comunicación telegráfica o telefónica, la impide o la interrumpe, será castigado con multa de 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables).

- Artículo 298. (Revelación del secreto de la correspondencia y de la comunicación epistolar, telegráfica o telefónica): Comete el delito de revelación de correspondencia epistolar, telegráfica o telefónica, siempre que causare perjuicio : (i) El que, sin justa causa, comunica a los demás lo que ha llegado a su conocimiento, por alguno de los medios especificados en los artículos anteriores. (ii) El que, sin justa causa, pública el contenido de un correspondencia, epistolar, telegráfica o telefónica que le estuviere dirigida y que, por su propia naturaleza debiera permanecer secreta. Este delito será castigado con 20 U.R. (veinte unidades reajustables) a 200 U.R. (doscientas unidades reajustables).

- Artículo 299. (Circunstancias agravantes): Constituyen circunstancias agravantes de este delito:

    1. El que fuera cometido por persona adscrita al servicio postal, telegráfico o telefónico.

    2. Que se tratare de correspondencia oficial; Que la revelación se efectuare por medio de la prensa.

22 Ver sentencia del Tribunal de Apelaciones del 1ero 38/2005. Disponible en: http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=81 [Accedido 16 de Septiembre, 2015].

23 Ver declaración de la sociedad civil en Uruguay sobre este punto en: http://www.rga.com.uy [Accedido 16 de Septiembre, 2015].

24 La Unidad indexada equivale a 3 pesos uruguayos (aprox.). 150 Unidades Indexadas equivalen a aproximadamente 450 pesos uruguayos (US$ 16) al cambio al cierre de esta edición (18-7-2015).

25 AGESIC es un organismo que depende de la Presidencia de la República. Tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las Tecnologías de la Información y las Comunicaciones (TIC). Disponible en: http://www.agesic.gub.uy/ [Accedido 16 de Septiembre, 2015].

26 Ley 18.331, *Protección de Datos Personales y Hábeas Data*, 2008. Disponible en: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor [Accedido 16 de Septiembre, 2015].

27 Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay (2014). *El Derecho a la Privacidad en la Era Digital: A/RES/68/167*. Disponible en: http://www.ohchr.org/Documents/Issues/Privacy/Uruguay.pdf [Accedido 16 de Septiembre, 2015].

28 Sentencia 58/209. Proceso de Inconstitucionalidad. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=46058

29 Poder Judicial - República Oriental del Uruguay. Inconstitucionalidad. Disponible en http://www.poderjudicial.gub.uy/historico-de-noticias/140-articulos-explicativos/567-inconstitucionalidad.html [Accedido 8 de Octubre, 2015]

30 El Tribunal indica que: "el inciso 2º del artículo 212 tolera la adopción de la interceptación de comunicaciones de cualquier índole aún respecto de terceros, por lo que no se advierte la razón que lleva a sostener, fundadamente, que el indagado no puede ser alcanzado por tal medida cuando la disposición abarca también a quienes no se encuentran sujetos al proceso penal" (TAC, 2ndo, Sentencia 80/2006. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359).

31 Sentencia 377/2013 Tribunal De Apelaciones Penal 2º T. Disponible en: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37314

32 Un delito en concurrencia significa usar otro delito como medio para cometer el delito principal.

33 Véase un informe inicial sobre la situación en Uruguay. Scrollini, Fabrizio. Uruguay: National Report en Global Information Society Watch, 2014. Disponible en:http://www.giswatch.org/2014-communications-surveillance-digital-age

34 Terra, Gonzalo. *Gobierno compró "El Guardián" para espiar llamadas y correos.* El País, 2013. Disponible en: https://eff.org/r.5fvk [Accedido 16 de Septiembre, 2015].

35 Diario El Observador (2014). *El Guardián espiará desde enero mails y celulares.* [ONLINE] Disponible en:http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757. [Accedido 29 de Septiembre, 2015].

36 Poder Legislativo, Cámara de Senadores. Disponible en http://www.parlamento.gub.uy/indexdb/Distribuidos/ListarDistribuido.asp?URL=/distribuidos/contenido/senado/S20150196.htm&TIPO=CON [Accedido 29 Septiembre, 2015].

37 Declaración conjunta: Vigilancia, seguridad y privacidad: llamamiento para que Uruguay adopte estándares de derechos humanos. Disponible en: http://www.cainfo.org.uy/2014/12/dia-internacional-de-los-derechos-humanos-declaracion-conjunta-vigilancia-seguridad-y-privacidad-llamamiento-para-que-uruguay-adopte-

estandares-de-derechos-humanos/ [Accedido 23 de Octubre del 2015].

38 Diario El País. *Ultiman detalles antes de implementar el Guardián*. http://www.elpais.com.uy/informacion/ultiman-detalles-implementar-sistema-guardian.html [Accedido 29 Septiembre, 2015].

39 De los Santos, F., (2015). ¿Quién vigila a los vigilantes? *La Diaria*. Disponible en: http://ladiaria.com.uy/articulo/2015/3/quien-vigila-a-los-vigilantes/ [Accedido 18 de Septiembre, 2015].

40 Poder Judicial Uruguay (2015). Tribunal Civil 5º Rechaza Apelación Sobre "El Guardián" y Señala Error Estratégico de la Accionante. Disponible en: https://eff.org/r.qayy [Accedido 15 de Marzo, 2015].

41 El documento indica que "en otras jurisdicciones el establecimiento de normativa secreta ha sido duramente cuestionado por establecer procesos jurisdiccionales y administrativos totalmente faltos de transparencia. La idea de norma secreta, como establece el Profesor Kutz de la Universidad de Berkeley, California, es "manifiestamente repugnante". Pueden existir secretos clasificados como tales, pero lo que no puede existir en una democracia es un meta-secreto, es decir, reglamentos, protocolos y normas que sólo el Estado conoce de su existencia.

42 Diario El País. *Los Gobiernos de la Región Potencian Capacidad para Espiar. Noticias Uruguay y el Mundo actualizadas. EL PAÍS Uruguay, 2015*. Disponible en: http://www.elpais.com.uy/informacion/gobiernos-region-potencian-capacidad-espiar.html [Accedido 17 de Septiembre 2015].

43 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, 2014. Disponible en: https://es.necessaryandproportionate.org/text [Accedido 16 de Septiembre, 2015].

44 *Ibíd.*

45 Las autoridades involucradas serían la DINACIE (Dirección Nacional de Inteligencia del Estado) ,el Coordinador Nacional de Inteligencia y algunas dependencias no mapeadas dentro de la estructura de las distintas armas del Estado (Tierra, Aire y Mar).

46 Principios Internacionales, *op. cit.*, Principio de Necesidad.

47 *Bonomi: "El Guardián" da más garantías que el sistema actual.* Diario EL PAIS Uruguay, 2015. Disponible en: http://www.elpais.com.uy/informacion/bonomi-guardian-garantias-sistema-actual.html. [Accedido 19 de Agosto, 2015].

48 Principios Internacionales, *op. cit.*, Principio de Idoneidad.

49 Diario EL PAÍS Uruguay. Polémica por escuchas telefónicas. Penalistas. Alertan "pinchazos" sin orden de juez y grabación de diálogos indagado-abogado. Diario EL PAÍS Uruguay. 04 de Noviembre 2012. Disponible en: http://historico.elpais.com.uy/121104/pnacio-673703/nacional/escuchas-riesgo-en-interpretacion/

50 *Ibíd.*

51 Principios Internacionales, *op. cit.*, Principio de Proporcionalidad.

52 Melendrez, Pablo, *op. cit.*

53 Principios Internacionales, *op. cit.*, Principio de Autoridad Competente.

54 Principios Internacionales, *op. cit.*, Principio de Debido Proceso.

55 Principios Internacionales, *op. cit.*, Principio de Notificación del Usuario.

56 Principios Internacionales, *op. cit.*, Principio de Transparencia.

57 Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay, *op. Cit.*

58 Melendrez P. J*ueces Penales ordenan tres esuchas por día* Diario El País [accedido 10 de Octubre 2015] disponible en http://www.elpais.com.uy/informacion/jueces-penales-ordenan-tres-escuchas.html

59 Principios Internacionales, *op. cit.*, Principio de Supervisión Pública.

60 Principios Internacionales, *op. cit.*, Principio de Integridad de las Comunicaciones y Sistemas.

61 Principios Internacionales, *op. cit.*, Principio de Garantías para la Cooperación Internacional.

62 OEA, Convención Interamericana Sobre Asistencia Mutua en Materia Penal [Inter-American Convention on Mutual Assistance in Criminal Matters], 1992. http://www.oas.org/juridico/english/treaties/a-55.html [Fecha de consulta: 22 de julio, 2015].

63 Principios Internacionales, *op. cit.*, Principio de Garantías contra el Acceso Ilegítimo y el Derecho al Recurso Efectivo.