VIGILANCIA ON LINE Y SECRETO PERIODISTICO: ANALISIS Y REFLEXIONES SOBRE SU NECESARIA PROTECCIÓN LEGAL

TALLER: VIGILANCIA ON LINE Y SECRETO PERIODISTICO.

Descripción del taller: Desde mediados del S. XX a la fecha en diferentes partes del mundo han tenido lugar diversos conflictos jurídicos a raíz de pedidos judiciales tendientes a que se revele la identidad de la fuente de una información periodística invocándose, como justificación, de ello su vital importancia para la resolución de un caso en particular.

Ante esta situación, con justa razón los periodistas han invocado como impedimento de tal pedido su derecho profesional a preservar el anonimato de su fuente. En Argentina, tal derecho se encuentra garantizado en el último párrafo del art. 43 de la Constitución Nacional donde expresamente reza que "No podrá afectarse el secreto de las fuentes de información periodística". Ahora bien, a partir de las revelaciones de Chelsea Manning y Edward Snowden, se ha tomado conocimiento de cómo las Agencias de inteligencia y Empresas privadas monitorean y vigilan toda clase de actividad on line de cualquier persona, entre quienes se encuentran por supuesto los periodistas. ¿La reserva de la identidad de las fuentes periodísticas merece una protección absoluta o, por el contrario, debe ceder frente a una situación particular en la cual, por ej., se encuentre en juego la seguridad nacional? ¿Debe permitirse a las Agencias de inteligencia que puedan interferir o acceder a cualquier clase de comunicación de los periodistas sin intervención de una autoridad judicial con basamento en la potencial inseguridad? ¿Quién controla a las agencias? ¿Cómo? ¿Sería viable ese control?

El objetivo del taller consistirá en exponer el marco jurídico que brinda protección al periodista para preservar el anonimato de la fuente. Acto seguido analizar diversos casos que han tenido lugar en diversos países de Latinoamérica y del resto del mundo donde se ha vulnerado el derecho del profesional a mantener el secreto de su fuente de información, fundado en que se corría un riesgo contra la seguridad nacional (posibles actos de terrorismo por ej) para finalmente realizar ejercicios prácticos de reflexión y razonamiento grupales con los asistentes.

Público al que va dirigido: licenciados en comunicación social, periodistas, docentes universitarios, abogados, público en general.

Requerimientos especiales del taller: PC, Proyector, micrófono.

Palabras clave: Vigilancia, Secreto periodístico, Intimidad, Comunicación, Expresión.

SEBASTIÁN CASTELLI*
MANUEL ERNESTO LARRONDO**

Online surveillance and journalistic secret. Reflections on the legal protection.

WORKSHOP: ON LINE SURVEILLANCE AND JOURNALISTIC SECRET

Abstract: Since the mid-twentieth century to date, in different parts of the world many legal disputes have occurred as a result of tending court orders that the identity of the source of journalistic information invoked as a justification, it is revealed its vital importance for the resolution of a particular case.

In this situation, journalists rightly had invoked as an impediment in such order his professional right to preserve the anonymity of its source. In Argentina, this right is guaranteed in the last paragraph of art. 43 of the Constitution which expressly states that "it will not affect the secrecy of journalistic information sources." Now, from the revelations of Chelsea Manning and Edward Snowden, it has taken note of how the intelligence agencies and private companies monitor all kinds of online activity of any person, including those who are, of course, journalists. Does the reservation of the identity of journalistic sources deserve absolute protection or, on the contrary, must yield to a particular situation in which, eg., Is in the national security game? You should be allowed to intelligence agencies that may interfere or access any kind of communication of journalists without intervention of a judicial authority with basement in the potential insecurity? Who controls the agencies? How? Would it be feasible that control?

The aim of the workshop will expose the legal framework that protects the journalist to preserve the anonymity of the source. Then analyze various cases that have taken place in several countries in Latin America and around the world where it has infringed the right of professional secrecy of their source of information, based on a risk that ran against national security (eg acts of terrorism) to finally practical exercises and group reflection reasoning with attendees.

Audience it is addressed: graduates in social communication, journalists, university professors, lawyers, public in general.

Keywords: Surveillance, Journalistic secret, Intimacy, Communication, Expression.

Monitoramento on-line e secreto jornalística. Reflexões sobre a protecção jurídica.

WORKSHOP: VIGILÂNCIA ON LINE E SECRETO PERIODISTICO

Resumo: Desde meados do século XX até hoje em diferentes partes do mundo, muitas disputas legais ocorreram como resultado da tendência ordens judiciais que a identidade da fonte da informação jornalística invocada como justificação, é revelado sua importância vital para a resolução de um caso particular.

Nesta situação, os jornalistas, com razão, sido invocadas como um impedimento de tal modo o seu direito profissional para preservar o anonimato de sua fonte. Na Argentina, esse direito é garantido no último parágrafo do art. 43 da Constituição, que expressamente afirma que "não vai afetar o sigilo das fontes de informação jornalísticas." Agora, Monitoramento on-line e secreto jornalística. Reflexões sobre a protecção jurídicaa partir das revelações de Chelsea Manning e Edward Snowden, ele tomou conhecimento de como as agências de inteligência e empresas privadas monitorar e controlar todos os tipos de atividade on-line de qualquer pessoa, incluindo aqueles que são de jornalistas do curso. Será que a reserva da identidade das fontes jornalísticas merecem proteção absoluta ou, pelo contrário, deve ceder a uma situação particular em que, por exemplo, é no jogo a segurança nacional? Você deve ter permissão para agências de inteligência que podem interferir ou acesso a qualquer tipo de comunicação de jornalistas sem a intervenção de uma autoridade judiciária com cave na insegurança potencial? Quem controla as agências? Como? Seria possível que o controle?

O objetivo do workshop irá expor o quadro jurídico que protege o jornalista para preservar o anonimato da fonte. Em seguida, analisar vários casos que ocorreram em vários países da América Latina e em todo o mundo onde ele violou o direito de sigilo profissional de sua fonte de informação, com base em um risco ele correu contra a segurança nacional (possível por exemplo, atos de terrorismo) para, finalmente, exercícios práticos e grupo de reflexão de raciocínio com os participantes.

Audiência é dirigida: graduados em Comunicação Social, jornalistas, professores universitários, advogados, público

Palavras-chave: Vigilância, Segredo jornalístico, Intimidade, Comunicação, Expressão.

INTRODUCCIÓN

Desde la reforma constitucional de 1994, en Argentina se ha debatido y escrito en demasía en torno a los conflictos jurídicos que han tenido lugar frente a pedidos de informes a periodistas y/o empresas de medios de comunicación por parte de la Justicia a fin de que se suministre la identidad de una fuente periodística invocándose como justificación de ello, su vital importancia para la resolución de un caso en particular.

Ante esta situación con justa razón los periodistas han invocado como impedimento de tal pedido la protección constitucional prevista en el último párrafo del Art. 43 de la Norma Fundamental cuando, luego de referirse al Habeas Data, expresamente reza que**"No podrá afectarse el secreto de las fuentes de información periodística."**

La reserva de la identidad de las fuentes periodísticas es y será el eje central en la eterna discusión jurídica respecto a si merece una protección absoluta o si, por el contrario, debe ceder frente a una situación particular en la cual, por ej., esté en juego la vida de un inocente. Los partidarios de la primera postura sostienen que dejar abierta la posibilidad de que un periodista deba identificar su fuente pone en serio riesgo el derecho humano de recibir, investigar y difundir información de toda índole a la opinión pública (Art. 13 de la Convención Americana de Derechos Humanos).

Sin ir más lejos, debe tenerse en cuenta que los profesionales de la prensa arriesgan su vida con el único objetivo de dar a conocer información a la opinión pública. Un ejemplo de ello es el caso de la periodista rusa Anna Politkovskaia cuando a fines de 2006 fue asesinada mientras investigaba el conflicto entre Rusia y Chechenia (ex república soviética). Otro caso es el de Judith Miller, del diario The New York Times, quien estuvo detenida por negarse a testificar sobre sus conversaciones confidenciales con fuentes gubernamentales, en un caso que buscaba determinar quién -del Gobierno de EEUU- filtró la identidad de la agente secreta Valerie Plame, esposa de un ex diplomático ("La SIP pide la puesta en libertad de la periodista Judith Miller" (19 de agosto de 2005). El Mundo. Recuperado de: http://www.elmundo.es/elmundo/-2005/08/18/comunicacion/1124361853.html.

En nuestro país sobran los ejemplos en los cuales la Justicia ha requerido en innumerables ocasiones que los periodistas revelaren sus fuentes ya que así se contribuiría a la resolución de un caso de trascendencia pública. Por ejemplo, el del periodista Thomas Catan del diario Financial Times de Londres que explicaremos en detalle más adelante; o bien el del bodeguero de la Pcia de San Juan que fue entrevistado en 1993 por periodistas mientras se encontraba prófugo por ser sospechoso de haber comercializado vino en damajuana en mal estado, ocasionando la muerte de varias personas por su ingesta. Al leer la crónica, el Fiscal de la causa solicitó que los periodistas revelaren donde estaba el imputado bajo apercibimiento de considerarlos cómplices. El Juez no hizo lugar al pedido justamente sosteniendo que, de acceder, se afectaría el derecho colectivo de la sociedad a ser informada ya que los periodistas perderían todas sus fuentes.

En los casos brevemente reseñados advertimos que ha intervenido formalmente la Justicia analizando la pertinencia o no del pedido de revelación de la fuente periodística en miras a solucionar un caso concreto.

Ahora bien, a partir de las revelaciones realizadas por Chelsea Manning y Edward Snowden se ha tomado conocimiento público, entre otros asuntos, de cómo las Agencias estatales de inteligencia e incluso Empresas privadas monitorean y vigilan toda clase de actividad on line o vía telefonía móvil de cualquier persona, entre quienes se encuentran, por supuesto, los periodistas. Al mismo tiempo, la situación personal tanto de Manning (condenada a 35 años de cárcel en EEUU) como de Snowden (asilado en Rusia, ya que si regresa a EEUU se expone a igual condena que Manning) demuestran el peligro al que se encuentran expuestas aquellas personas que actúen como fuentes periodísticas revelando información vinculada con la vigilancia social estatal o privada.

Por otra parte, debe tenerse en cuenta que, en el ejercicio profesional, el periodista enfrenta en principio muchas situaciones distintas a los de cualquier ciudadano común. Sin embargo, como su trabajo y su vida personal se encuentran en cierta forma subsumidas en el necesario empleo de la tecnología y redes sociales, es claro que ello implica dejar en el camino una enorme y variada cantidad de registros electrónicos y metadatos como por ejemplo: destinos y recepción de llamadas telefónicas, mensajes de texto, conexiones temporales a determinadas antenas de telefonía celular, uso de GPS, intercambio de correos electrónicos y mensajes a través de las plataformas web, entre otros. El uso de todas estas plataformas sin dudas conlleva dejar cientos de registros que, bajo vigilancia masiva estatal o privada, podrían ser usados en perjuicio de sus fuentes de información. De allí que, dependiendo del caso sobre el que el periodista se encuentre trabajando, se infiere que bien podrían o deberían emplear tecnologías de encriptación en sus comunicaciones a fin de evitar, justamente, que tenga lugar la recolección on line de sus datos de contactos o interacción en la web.

Sin dudas el caso de Edward Snowden es sumamente revelador. Luego de haber realizado un análisis de los documentos revelados por el ex dependiente de una Empresa contratista de la Agencia Nacional de Seguridad de EEUU, el diario británico "The Guardian" informó el 19 de Enero de 2015 que en Noviembre de 2009, la British Global Communications Headquarters (GCHQ, la Agencia de Seguridad Británica) interceptó alrededor de 70.000 correos electrónicos incluidos algunas direcciones de empresas periodísticas como la BBC, Reuters, los diarios The Guardian, The New York Times, Le Monde, The Sun, NBC y The Washington Post (Ball J. (19 de Enero de 2015). "GCHQ captured emails of journalists from top international media." The Guardian. Recuperado de: https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post)

Se informó que la Agencia Británica interceptó los correos electrónicos a través de un uso de la fibra óptica como parte de un entrenamiento. Luego compartieron esos correos electrónicos

interceptados en su propia Intranet. El informe periodístico del diario inglés reveló además que el GCHQ entiende que la información sobre la que trabajan los periodistas de investigación es comparable a la actividad que realizan los "terroristas" y "hackers." Concluye el reporte que los documentos de dicha Agencia de Inteligencia sostienen que los *"periodistas y reporteros representan una potencial amenaza a la seguridad."* La idea que se desprende de este reporte es que sería "potencialmente riesgoso" ejercer el derecho humano a recibir, investigar y difundir información. Inaudito.

La vigilancia masiva de la actividad de los periodistas implica, tal como referimos, poder acceder a los metadatos de las comunicaciones. A través de ellos, informa la ONG "Necessary & Proportionate" que se puede crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones. A pesar del gran potencial para la intromisión en vida del individuo y el efecto negativo sobre las asociaciones políticas y otras, las leyes, normas, poderes o autoridades a menudo ofrecen a los metadatos de las comunicaciones un menor nivel de protección y no ponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados (*Necessary and Proportionate Coalition, Necesarios y Proporcionados (Mayo 2014)* https://necessaryandproportionate.org/es/necesarios-proporcionados).

Juan Diego Castañeda (2016) apunta que*"los datos que se recogen son, por ejemplo, el número que recibe una llamada, el tiempo de la llamada, la ubicación geográfica del dispositivo o sus identificadores únicos (IMEI e IMSI) en telefonía móvil o fija, y las direcciones IP en internet. Esto es, en un nivel simple, diferente de la recolección de las comunicaciones en sí mismas y, por tanto, han sido llamados "metadatos", es decir, datos acerca de los datos de comunicación. Esta clasificación puede llevar a concluir erróneamente que los metadatos o los datos de identificación del suscriptor merecen una protección menor a la que está establecida para las comunicaciones en sí mismas. La agregación de datos, en realidad, es más reveladora que el contenido de las comunicaciones. Por esta razón, se ha establecido que la retención de datos es una medida que restringe y afecta los derechos a la intimidad y a la libertad de expresión."*

Ante esta alarmante situación, surgen algunos interrogantes que planteamos como disparadores de este trabajo: ¿La reserva de la identidad de las fuentes periodísticas merece una protección absoluta o, por el contrario, debe ceder frente a una situación particular en la cual, por ej., se encuentre en juego la seguridad nacional? ¿Debe permitirse a las Agencias de inteligencia que puedan interferir o acceder a cualquier clase de dato derivado de una comunicación telefónica o electrónica que realice un periodista sin intervención de una autoridad judicial? ¿Es justificable el fundamento de la vigilancia masiva en miras a proteger la "seguridad nacional"?

El objetivo de este trabajo consistirá en exponer el marco jurídico argentino e internacional que brinda protección al periodista para preservar el anonimato de la fuente. Acto seguido analizaremos diversos casos que han tenido lugar en diversos países de Latinoamérica y del

resto del mundo en los que se intentado avasallar el derecho del periodista a mantener el secreto de su fuente de información de parte de Organos estatales, fundando tal proceder en que habría un peligro inminente o bien se corría un riesgo contra la seguridad nacional (posibles actos de terrorismo por ej).

SECRETO DE LA FUENTE PERIODISTICA. NATURALEZA JURIDICA. TITULARIDAD. PRINCIPIOS REGULATORIOS DE VIGILANCIA EN LAS COMUNICACIONES

Empezaremos el análisis de este punto formulándonos un nuevo interrogante: ¿Quién es el titular del derecho a mantener en reserva la identidad de la fuente? ¿Será la Empresa de medios de comunicación o el periodista?

Titularidad del derecho.

Por empezar, siguiendo a Badeni (2002) "**el secreto profesional es un derecho subjetivo de naturaleza pública que integra la libertad institucional de prensa**. Ese secreto coadyuva a obtener y difundir la información que interesa a la sociedad, ya que tanto en el ámbito privado como público se generan datos y noticias que son revelados bajo la condición expresa de preservarse la reserva de la fuente del informante".

En nuestra opinión, este derecho pertenece con exclusividad a los periodistas y también a quienes ocasionalmente publiquen información en cualquier medio de comunicación (Portal de Internet, redes sociales, por ej.). En concordancia con lo expuesto, afirma Silvana Catucci (1997) que "el titular de esta garantía es el periodista" y Javier De Lucca (1999) expresa por su parte que "no parecen existir razones constitucionales por las cuales el privilegio del secreto, si así quiere llamárselo, no pueda extenderse a toda persona que realiza una actividad periodística en sentido material, aún cuando no lo haga habitualmente o no sea un profesional".

Por el contrario, esta prerrogativa no se extendería **a las empresas propietarias de los "medios" o "multimedios**" en tanto, justamente, no son ellos los titulares de ese derecho público subjetivo.

Es decir, los protegidos por esta garantía son los periodistas comprendidos en el art. 2° del Estatuto del Periodista Profesional (Ley 12908 "Estatuto del Periodista Profesional", Boletín Oficial de la República Argentina Nº15813, Buenos Aires, Argentina, 11 de Julio de 1947) y **toda persona** que publique noticias, opiniones, escritos por medios gráficos, por radio, televisión, Internet u otro mecanismo de divulgación conforme a lo previsto por el art. 14 de la Constitución Nacional y el art. 13 del Pacto de San José de Costa Rica (con jerarquía constitucional en Argentina conforme se desprende del art. 75 inc. 22 de la C.N.).

Sobre este punto, vale la pena traer a colación un fallo judicial de fecha 26/5/06 dictado por la Corte de Apelaciones de California, EEUU, en los autos JASON O'GRADY et al., Petitioners, v. THE SUPERIOR COURT OF SANTA CLARA COUNTY, Respondent; APPLE COMPUTER, INC.,

Real Party in Interest. H028579 (Santa Clara County Super. Ct. No. CV032178 Recuperado de:http://www.internetlibrary.com/pdf/0Grady-Apple-Cal-Crt-App.pdf)

En este caso, la Corte de apelaciones de California decidió que los 'bloggers' –personas que son titulares de un portal en Internet y que en él publican cualquier tipo de información–, al igual que los periodistas tradicionales, tienen derecho a mantener la confidencialidad de sus fuentes.

Los hechos consistieron en que un grupo de 'bloggers' acudió a los tribunales después de que*Apple* – Empresa Americana que desarrolla tecnología en computación hardware – tratara de forzarles a revelar la identidad de la persona -probablemente un empleado de la compañía- que les facilitó los detalles de un proyecto de la empresa denominado 'Asteroid'. Los datos del producto fueron difundidos en varios sitios de Internet.

La sentencia, en síntesis, estableció que los 'bloggers'**no tienen obligación de revelar sus fuentes** y pueden acogerse a las leyes que protegen a los periodistas tradicionales, la **Primera Enmienda** de la Constitución Americana y la **California's Shield Law.**

Este fallo de la justicia norteamericana confirma entonces nuestra postura por cuanto la Constitución Nacional y los Tratados Internacionales de Derechos Humanos que poseen jerarquía constitucional deben ser interpretados en forma amplia y flexible en clara protección a la libertad de expresión del ser humano indistintamente si la acción de recibir, investigar y difundir se realice en forma profesional o amateur.

Ahora bien, en concordancia con la constitucionalista María Angélica Gelli (2005)*"la preservación de las fuentes de información periodística – como la integridad de los derechos que constituyen la libertad expresiva – tienen como finalidad el descubrimiento de la verdad a través de la libre circulación de las noticias obtenidas, éstas muchas veces bajo reserva y que, de otro modo, no se conocerían. El descubrimiento de la verdad de los hechos tiene particular importancia en la investigación de los delitos y en el control del gobierno y de las eventuales ilegalidades que afectan directamente al proceso democrático. En este sentido* ***el privilegio de los periodistas no es un fuero personal****, sino que opera en resguardo de aquellos objetivos y para favorecerlos".*

Es acertada esta posición por cuanto no podría invocarse la protección de esta garantía constitucional como si fuera un fuero personal asimilable a quien desempeña una función pública (Juez, legislador, etc.). Por el contrario, debe remarcarse que se trata de una garantía constitucional de todo ser humano que ejerce profesional u ocasionalmente la tarea de informar por cualquier medio de comunicación, en tanto la acción de recibir, investigar y difundir información es un derecho humano conforme lo prevé el art. 13 del Pacto de San José de Costa Rica. Ello ha sido reafirmado por la Corte Interamericana de Derechos Humanos en la Opinión Consultiva Nº 5 del 13/11/1985 rechazando la Colegiación Obligatoria de Periodistas **(Arts. 13 y 29 de la Convención Americana sobre Derechos Humanos)** (Corte Interamericana de Derechos Humanos (13 de Noviembre de 1985). Opinión Consultiva Nº5. Recuperado de: http://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf).

En síntesis, como primera conclusión de este estudio podemos afirmar entonces que la reserva de identidad de la fuente periodística pertenece al ser humano como tal y no a la Empresa periodística que eventualmente lo emplee.

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

Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones fueron desarrollados a partir de las conceptualizaciones que se han realizado en torno al derecho internacional de los derechos humanos en el entorno digital en un proceso que distintas organizaciones de la sociedad civil lideraron y que contó con la participación de representantes de la industria y expertos en la materia.

De acuerdo a lo que se informa en el sitio web de Necessary & Proportionate*"el proceso de elaboración de estos Principios se inició en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en Diciembre de 2012, Access, EFF y Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericia sobre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en Septiembre de 2013." (Necessary and Proportionate Coalition, Necesarios y Proporcionados (Mayo 2014)* https://necessaryandproportionate.org/es/necesarios-proporcionados)

En ese sentido, los principios que deben regir la aplicación de medidas de vigilancia de las comunicaciones son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo, y derecho a un recurso efectivo.

Siguiendo estos principios, el Relator para libertad de expresión de la OEA, a propósito de las revelaciones sobre el uso de productos y servicios de la empresa italiana Hacking Team por parte de gobiernos alrededor del mundo, expresó que, de acuerdo con los estándares internacionales, el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación. (Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (2015, 21 de julio). Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio Recuperado de: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2)

Veamos entonces brevemente que sostiene cada uno de los Principios reseñados

Principio 1: *Legalidad*

Cualquier limitación a los derechos humanos debe ser prescrita por ley, cumplir con un estándar de claridad y precisión suficiente para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Asimismo exige que esa misma ley sea objeto de revisión periódica.

Principio 2: *Objetivo Legítimo*

Esa misma ley solo debería 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. Por supuesto su aplicación no debería implicar discriminación alguna por cualquier razón o circunstancia.

Principio 3: Necesidad

La ley debe limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo y la justificación de ello debe recaer en el Estado.

Principio 4: *Idoneidad*

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

Principio 5: *Proporcionalidad*

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. Por eso este Principio requiere que el Estado, como mínimo, demuestre que:

1) Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo, y;

2) Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la la Información Protegida, y;

3) Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica. Y;

4) La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado; y

5) Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; y

6) La información será accesada solo por la autoridad especifica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y

7) Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

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. La autoridad debe:

1) Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones.

2) Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y

3) Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

Principio 7: Debido Proceso

El debido proceso exige que, entre otras garantías, toda persona tenga 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.

En nuestra opinión, la última situación prevista en este Principio debería ser la que mayor reglamentación y previsión legal debiera tener ya que podría prestarse a que se cometan abusos que en consecuencia afecten garantías constitucionales.

Principio 8: Notificación del Usuario

Este principio prevé que aquellas personas cuyas comunicaciones están siendo vigiladas deben ser notificados por el Estado 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:

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.

Principio 9: Transparencia

Se exige que los Estados sean transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, debiendo publicar como mínimo informes globales de esta temática.

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.

Principio 11: Integridad de las Comunicaciones y Sistemas

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. El fin es garantizar a las personas su derecho a expresarse anónimamente.

Principio 12: Garantías para la Cooperación Internacional

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 estandar disponible con el mayor nivel de protección para las personas.

Principio 13: Garantías Contra el Acceso Ilegítimo y Derecho a Recurso Efectivo

Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados así como también proteger a los "whistle blowers" (soplones) y medios de reparación a las personas afectadas. Asimismo, deben prever que el material obtenido a través de la Vigilancia de las Comunicaciones ya utilizado debe ser destruido o devuelto a los afectados.

Secreto de la fuente periodística: ¿protección absoluta o relativa?

De igual forma, la doctrina y jurisprudencia han dado sus puntos de vista tanto a favor como en contra de la protección de la reserva de la fuente así como también hay posiciones eclécticas que ameritan que a continuación los tratemos a fin de dilucidar la respuesta a este interrogante.

Doctrina.

PIERINI, LORENCES y TORNABENE (1998) sostienen que "el derecho a no revelar las fuentes es absoluto e incondicional" y agregan que **la reserva de la fuente no debe ceder ante autoridad o reclamo alguno por tener una garantía constitucional absoluta. Los autores mencionados sólo aceptan la excepcionalidad en caso de un delito no ejecutado o que está siendo consumado**, en estos términos: "Aquél que posea una información no deberá, por

decisión de autoridad alguna, aportar datos sobre sus fuentes, pero estará obligado, si se refiere a un delito no cometido aún, a realizar todas las denuncias para evitarlo; o sabiendo de la existencia de un delito que está siendo consumado a realizar la denuncia para evitar la prosecución y reiteración de hechos disvaliosos".

Una opinión distinta es sostenida por otra corriente doctrinaria representada por COLAUTTI (1996) para quien **la veda constitucional no es absoluta pues encuentra su restricción en la facultad de los jueces para ordenar requisas en empresas periodísticas cuando sea imprescindible para encontrar pruebas en un caso criminal**.

EKMEKDJIÁN (1997) agrega que "el secreto a las fuentes de información sólo cede cuando encontrándose el periodista ante la comisión inmediata del delito, éste pudiera lesionar un derecho de jerarquía superior al de la prensa (vgr. la dignidad, la vida, etc.)".

VANOSSI (1988) coincide también con el carácter absoluto del secreto de las fuentes pero cuando se trata de opiniones y datos no relacionados con causas penales. En cambio, cuando sí existe causa penal, distingue entre delitos ya juzgados y eventualmente condenados, y delitos que estén en curso de ejecución. En el primer caso predomina la reserva, en el segundo no, del mismo modo cuando la falta de dato puede llevar a la condena a un inocente.

Por su parte, GOZAÍNI (2001) sostiene que es necesario ponderar el caso en concreto: "En los hechos, nos parece más razonable adoptar un criterio propio y adecuado a las circunstancias y contextos en los que cada información se origina. De este modo, la reserva y confidencialidad de las fuentes es una garantía impermeable, como lo es la libertad de prensa y el derecho a la información. Pero, al mismo tiempo, proporciona un deber inexcusable a los medios de comunicación para que desde una perspectiva ética y moral no difundan aquella información que, siendo disponible, pueda afectar la sensibilidad de las personas. La diferencia entre el*poder* de contar una gran cantidad de información sobre cada individuo y el *deber* de no difundirla sería más que nunca fundamental en este terreno".

Sin embargo, las nuevas tecnologías implementadas por Empresas privadas y por los Gobiernos en ciertas ocasiones implica que las Agencias de inteligencia, Policía o cualquier otra autoridad estatal considere necesario contar con una orden judicial para obtener datos o vigilancia de ciertas comunicaciones.

Así lo explica Martin Shelton (2015) en relación a EEUU, en tanto sostiene que "los registros electrónicos (por ejemplo, los metadatos relacionados a llamadas telefónicas) proporcionan suficiente evidencia para vincular a un periodista con una fuente. Las agencias de Estados Unidos en general, tienen la autoridad para obligar a las personas jurídicas (por ejemplo, compañías de teléfono) para dar a los registros electrónicos del gobierno, incluyendo información sobre las comunicaciones electrónicas en virtud de múltiples autoridades. El gobierno no tiene que pedir a un periodista a revelar información sobre fuentes confidenciales si el gobierno puede en lugar de obtener una orden judicial para obtener los registros, y entregar la citación

a la empresa que gestiona los registros pertinentes. En otros casos, el gobierno recoge la información de inteligencia con potencial."

Agrega Shelton (2015, pág. 44) que en 1967 tuvo lugar el caso del Tribunal Supremo EE.UU., Katz v. Estados Unidos (EE.UU. 389 347), en el cual se examinó la definición legal de una "búsqueda" de la información. El tribunal estableció que la "expectativa razonable de privacidad" prueba para determinar si ciertos tipos de información deben ser protegidos bajo la Cuarta Enmienda. Sin embargo, en el caso criminal Smith v. Maryland (EE.UU. 442 735, 1979), el Tribunal Supremo reafirmó que la policía podría interceptar los registros de llamadas sin una orden judicial, **porque la persona que llama renuncia a cualquier expectativa razonable de privacidad, proporcionando registros de las comunicaciones a un tercero- la compañía telefónica**. El principio de que las personas no tienen ninguna expectativa razonable de privacidad cuando la información de ruta a través de una parte exterior es ahora conocida como la "doctrina de terceros", es un concepto que se ha convertido en la piedra angular para la interpretación moderna de las protecciones de la Cuarta Enmienda de datos de los consumidores en los tribunales (por ejemplo, Kerr, 2012; Newell, 2013; Newell & Tennis, 2013)."

Esta doctrina americana que data de unos casi 40 años estaría vulnerando claramente los principios regulatorios de vigilancia en las comunicaciones referidos anteriormente, tales como el de notificación al usuario, debido proceso, autoridad judicial competente, entre otros.

Jurisprudencia Argentina.

Entre las causas judiciales argentina de mayor relevancia donde se ha producido un conflicto de derechos se destaca aquella que tuvo de protagonista al fallecido ex miembro del ERP (Ejército Revolucionario del Pueblo) "**Gorriarán Merlo**" en la cual **se admitió la posibilidad de que este secreto ceda "cuando razones de orden público de relevante jerarquía así lo aconsejen y cuando ello no vulnere el derecho a no autoincriminarse ni afecte los límites previstos en el art. 28 C.N. (...) Otorgándole un alcance absoluto terminaría afectando intereses del propio estado de derecho que motivara el reconocimiento y necesidad de una prensa libre..."** (Cámara Federal de Apelaciones de San Martín, Sala I, Buenos Aires, Argentina (2 de Mayo de 1996) Revista Jurídica "La Ley" Tomo 1996 C, pág 637).

Particular atención merece prestarse al caso "Thomas Catán" al que hicimos mención al comienzo. El Juez instructor, Dr. Claudio Bonadío, ordenó confeccionar un listado con la totalidad de las llamadas entrantes y salientes registradas entre los días 15 y 29 de agosto de 2002 de la línea telefónica celular del periodista inglés Thomas Catan del diario Financial Times de Londres quien, en un primer momento, fue citado como testigo en esta causa habiéndose negado a revelar la identidad de su fuente ante el pedido del Juez. Recordemos que el periodista fue autor de dos notas en las que reveló la posible existencia del presunto delito de cohecho en el Senado de la Nación a legisladores que dieron su voto para reformar la ley laboral y que el aludido magistrado investigaba (Cámara Federal de Apelaciones en lo Criminal y Correccional, Sala II,

Buenos Aires, Argentina (28 de Octubre de 2002) Causa n° 19.480 caratulada "Incidente de Thomas Catan en autos n° 14.829/2002" Juzg. Federal n° 11 - Secretaría n° 22 Registro nº 20.377, Publicado en Revista Jurídica "LaLey", 1º/11/02).

Frente a la orden judicial, el periodista planteó la nulidad y apeló la medida con fundamento en que ella afectaba el secreto a las fuentes de información periodística protegido en el artículo 43 de la Constitución Nacional.

La sentencia de Cámara resolvió desestimar la orden del Juez de instrucción en tanto entendió que **no había necesidad de que ella sea adoptada teniendo en cuenta que se podía avanzar en la pesquisa mediante otros cursos de investigación que resulten igual de útiles y eficaces sin que el secreto a las fuentes de información periodística resulte afectado**. De hecho, se tuvo en cuenta que, contemporánea e indepedientemente, habían sido dispuestas otras vías que se dirigían a determinar la verdad de la hipótesis delictiva investigada.

Adviértase que la sentencia deja la "puerta abierta" para entender que, dependiendo del caso y del momento, podría eventualmente recurrirse a esa medida, es decir, a requerir el listado de llamadas salientes y entrantes del teléfono del periodista si no hubiera otros caminos de investigación para averiguar la verdad del caso. Esto significa que la mentada inviolabilidad del secreto de la identidad de la fuente periodística, según surge de este fallo, podría ceder dependiendo del caso judicial y del estado en que éste se encuentre.

Así todo, se visualiza que en tal situación se impone que sea un magistrado quien ordene tal proceder y, en ese caso, el periodista debería evaluar si corresponde impugnarla por las vías judiciales pertinentes.

Jurisprudencia de Paraguay

Jorge Rolón Luna, Maricarmen Sequera Buzarquis con las contribuciones de Katitza Rodríguez y David Bogado (2016) refieren un caso judicial que llegó hasta la Corte Suprema de Justicia de Paraguay en el que se validó la intervención de comunicaciones sin contar con una orden de un Juez obteniendo así un conjunto de metadatos. Es importante destacar que si bien en el caso no surge que se vieran involucrados periodistas, la doctrina que emerge del fallo amerita a reflexionar acerca de que –eventualmente- el día de mañana podría validarse la vigilancia de comunicaciones de un comunicador con su fuente.

En concreto, 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.

Los acusados de su secuestro y asesinato de la Sra Cubas habían interpuesto recurso extraordinario de casación, el cual fue rechazado por el Máximo Tribunal. Para tal fin, la Corte Suprema sostuvo

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. Para fundar tal postura, entendió que el derecho a la inviolabilidad del patrimonio documental y la comunicación privada, protege la comunicación en sí, no así los datos relativos de estas comunicaciones (con quién, cuándo, frecuencia, horarios, entre otros).

La crítica concreta a la conclusión a la que arriba la sentencia es que, al no estar regulado por ley, el Tribunal ha validado un accionar estatal ilegítimo de una autoridad estatal (Fiscal) que vulneró el derecho a la intimidad de las comunicaciones en miras de obtener metadatos.

Concluyen Rolón y Sequera Buzarquis (2016) que tampoco se tomó en cuenta la decisión de la Corte Interamericana de Derechos Humanos sobre el caso contencioso en el que se condenó al Brasil 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" (Corte Interamericana de Derechos Humanos (6 de Julio de 2009) (Cecilia Medina Quiroga, Presidenta). Recuperado de: https://web.archive.org/web/20140527113509/http:/www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

CONCLUSIONES FINALES

Hemos analizado a lo largo de este trabajo el marco jurídico nacional e internacional así como también las diversas opiniones doctrinarias y algunos antecedentes jurisprudenciales vinculados con la pertinencia o no de que la protección al secreto periodístico deba o pueda ceder cuando los hechos se relacionan con una investigación penal o bien por razones de "seguridad nacional".

A ésta de por sí conflictiva situación sumamos la problemática referida a la vigilancia en las comunicaciones que realizan ciertos Estados sin contar con una orden judicial expresa, lo cual suelen justificar en base al mentado deber de brindar "seguridad" a la ciudadanía en detrimento del derecho humano a la privacidad en las comunicaciones.

Para concluir, debemos hacer una breve referencia a la investigación desarrollada por John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri y Marion Marschalek (2015) del "Citizen Lab" –de la Universidad de Toronto- titulada "Packrat: Siete Años de un Actor de Amenaza en América del Sur". Se trata de un informe de investigación que describe un uso intensivo de malware, phishing y una campaña activa de desinformación en varios países latinoamericanos, incluyendo Ecuador, Argentina, Paraguay, Venezuela, y Brasil. Entre otros casos, se menciona

que algunos países han hecho uso del sistema FinFisher que posee una funcionalidad similar al de la empresa italiana Hacking Team, la cual provee un sistema que permite interceptar computadores, videollamadas, correos electrónicos, mensajes instantáneos y contraseñas.

El software empleado por este tipo de sistemas 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.

En ese sentido, Shelton (2015) ilustra muy claramente el peligro en el que se encuentran subsumidos los periodistas al ejercer su profesión. Así comenta que entre una de las principales causas de espionaje en 2006, el periodista del diario The New York Times, James Risen publicó su libro Estado de guerra donde detalla las actividades encubiertas del gobierno de EEUU en guerras en el extranjero.

En un capítulo del libro, Risen reveló que en la era de Clinton la Agencia Central de Inteligencia tenía un plan para sabotear el programa de desarrollo nuclear de Irán de modo que cuente con los modelos defectuosos. Sin embargo, su plan fracasó. En 2008 y 2010, al salir el libro, Risen fue citado ante los Tribunales para declarar sobre el caso a fin de quee revelare sus fuentes, a lo cual se negó a través de una larga serie de apelaciones en la Corte. Sin embargo, el Tribunal Supremo rechazó su apelación en junio de 2014, dejando abierta la posibilidad de que Risen pasara un tiempo en la cárcel por negarse a revelar sus fuentes.

A principios de 2015, la batalla legal de Risen llegó a su fin cuando el Departamento de Justicia decidió que no era más necesario contar con su testimonio. En efecto, el Gobierno había podido identificar que su fuente era un ex agente de la CIA llamado Jeffrey Sterling ¿Que había ocurrido? El Gobierno de EEUU había interceptado correos electrónicos entre Risen y Sterling, quien más tarde fue acusado y condenado en virtud de la Ley de Espionaje, la misma ley que fue aplicada a Chelsea Manning y por los mismos cargos que le son imputados a Edward Snowden.

Como periodista, Risen había tenido una considerable protección legal, pero su supuesta fuente no. Mientras que su sentencia fue significativamente más corta que la pena de prisión de 19 a 24 años que los fiscales del gobierno previeron inicialmente, Jeffrey Sterling todavía deberá pasar tres años y medio en una prisión federal.

Sin dudas esta situación latente de vulnerabilidad a la que en particular se encuentran expuestos las fuentes periodísticas en distintos países del mundo genera un peligro cierto de daño irreparable al derecho humano de recibir, investigar y difundir información de conformidad a la protección que brinda el art. 13 del PSJCR y en particular nuestro art. 43 de la CN al proteger expresamente la preservación de la identidad de la fuente periodística.

En coincidencia con la postura adoptada por el Relator para la Libertad de Expresión ante la OEA, sin duda algunael uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en una ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación. Para tal fin, es vital que las legislaciones del mundo incorporen y apliquen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

NOTAS

* castelli.sebastian@gmail.com

** Facultad de Periodismo y Comunicación Social UNLP. larrondomanuel@gmail.com.

REFERENCIAS

Juan Diego Castañeda https://karisma.org.co/es-legitima-la-retencion-de-datos-en-colombia/ pág 10

BADENI, Gregorio. Tratado de Libertad de Prensa, pág. 344, Ed. Lexis Nexis, 2002

CATUCCI, G., Silvana, "Libertad de Prensa. Calumnias e Injurias", p. 99, Ediar, Buenos Aires, 1997

DE LUCCA, Javier Augusto, "El secreto de las fuentes periodísticas en el proceso penal", Ad Hoc, Buenos Aires, 1999

GELLI Maria Angélica, El resaltado nos pertenece; Constitución de la Nación Argentina comentada y anotada, 3º Ed. La Ley, 2005, pág. 515

PIERINI, Alicia, LORENCES, Valentín, TORNABENE, María I., "Hábeas Data. Derecho a la intimidad", Universidad, Bs. As., 1998, pág. 202

COLAUTTI, Carlos E., "Reflexiones preliminares sobre el "Hábeas Data", en L.L. 1996-C-917

De Lucca, Javier Augusto, "El secreto de las fuentes periodísticas en el proceso penal", Ad Hoc, Buenos Aires, 1999

EKMEKDJIÁN, Miguel A., "El derecho al secreto de las fuentes de información", en L.L. 1997-C-666

VANOSSI, Jorge Reinaldo, Disertación pronunciada en el Primer seminario Profesional sobre "Aspectos Jurídicos de la empresa periodística", Buenos Aires, 28 y 29 de junio de 1988 según cita de CATUCCI, Silvana, op. cit.

GOZAÍNI, Osvaldo A. "Hábeas Data. Protección de datos personales". Rubinzal-Culzoni Editores. Buenos Aires, 2001. Pág. 380

SHELTON MARTIN, "The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices. DISSERTATION. Submitted in partial satisfaction of the requirements for the degree of DOCTOR OF PHILOSOPHY in Information and Computer Science https://mshelt.onl/p/shelton_2015.pdf (pág. 43)

Jorge Rolón Luna, Maricarmen Sequera Buzarquis con las contribuciones de Katitza Rodríguez y David Bogado Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay - TEDIC y Electronic Frontier Foundation está disponible bajo Licencia Creative Commons Reconocimiento 4.0 Licencia Internaciona, Marzo 2016 https://www.eff.org/es/country-reports/Paraguay-ES-final pág 23/26

Scott-Railton John, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor", Citizen Lab, Diciembre, 2015, https://citizenlab.org/2015/12/packrat-report/#.Vm81JgRq1v0.twitter