El derecho a la Intimidad y los límites a la injerencia estatal

Sobre la intervención de comunicaciones y la retención de datos de trafico en el articulado de la ley 25.873

Federico Viegener

Índice

Introducción

En la actualidad los desarrollos tecnológicos gozan de tiempos acelerados y vertiginosos muy distintos a los que se vivían hasta hace tan solo pocos años. Las posibilidades de comunicación entre puntos lejanos asombran por su velocidad, instantaneidad, facilidad de uso y bajo costo. Lamentablemente estos avances permiten su uso con fines dañinos y atentatorios contra la seguridad nacional y el surgimiento de nuevas formas delictivas que se valen de sus potencialidades. Esta veta provoca la preocupación de las autoridades y desencadena en intentos normativos para el control y erradicación de las nuevas actividades criminales.

Lamentablemente en ciertos casos, la precipitación por sancionar un marco legal capaz de hacer frente a las preocupaciones florecidas en torno a estas nuevas modalidades de delinquir, no repara en garantías fundamentales, patrimonio de los ciudadanos.

La sanción de la ley 25.873, instauradora de un sistema técnico destinado a facilitar la intervención de comunicaciones y la retención de datos de tráfico, resulta comprendida en el panorama aludido. Su texto vulnera en dilatada forma el derecho a la intimidad consagrado por nuestro texto constitucional y lamentablemente no fue objeto del siempre necesario y adecuado debate parlamentario.

La presurosa sanción de la ley que será motivo de análisis a lo largo del presente desarrollo, hizo caso omiso de las realidades extranjeras, las cuales necesariamente deben ser bienvenidas a la hora de afrontar una problemática que tuvo nacimiento con anterioridad en tierras foráneas.

La cuestión de la retención de datos de tráfico, plantea una extensa cantidad de cuestionamientos que al día de hoy no han recibido todos ellos una adecuada respuesta por parte de los actores implicados a nivel internacional. La Unión Europea, por su parte, aun no cuenta con una realidad normativa definitiva, y transita por un periodo de búsqueda de armonización de las legislaciones de sus distintos estados miembros. El tema cuenta con interesantes aristas y diversas opiniones, las cuales deben necesariamente trasladarse a nuestro país a la hora de reevaluar la cuestión.

El mantenimiento de la paz social y la seguridad nacional deben necesariamente realizarse en un adecuado marco de respeto de los derechos fundamentales asegurados a los habitantes de la nación en los diferentes textos legales, siendo piedra angular la Constitución Nacional y los Tratados Internacionales ratificados.

Teniendo lo antedicho como idea directriz, serán tratadas a lo largo de las próximas páginas, diversas cuestiones que surgen del articulado de la ley 25.873 y resultan plenamente actuales a nivel global. A modo de anticipo de las conclusiones vertidas, es de subrayar que encontrar un punto medio, balanceado en cuanto al respeto de los derechos individuales y la seguridad

colectiva, es sin duda alguna el objetivo primordial que debe gobernar en un futuro el replanteamiento de lo normado por la ley.

Puntos Preliminares

Sanción de la ley 25.873

El Honorable Congreso de la Nación Argentina sancionó en fecha 17 de diciembre de 2003 la ley 25.873, constante de 4 artículos, incorporando así los artículos 45 bis, 45 ter y 45 quáter a la ley de telecomunicaciones 19.798. En fecha 8 de de Noviembre del año 2004, el Poder Ejecutivo nacional reglamentó la normativa mediante el decreto 1563/04.

En líneas generales la ley prevé la captación y derivación de las comunicaciones que transmiten los prestadores de servicios de telecomunicaciones para su observación remota a requerimiento del poder judicial o del ministerio publico; y el registro y sistematización de los datos filiatorios, domiciliarios y de tráfico de comunicaciones de usuarios y clientes, para su consulta por parte del Poder Judicial o el Ministerio Publico de conformidad con la legislación vigente.

La sanción de dicha ley provocó una gran conmoción mediática y social, que derivó en la suspensión del decreto reglamentario por parte del presidente de la nación, por medio del decreto 357/05 manifestando en los considerándos que razones de publico conocimiento aconsejaban suspender la aplicación del decreto 1563/04, a los fines de permitir un nuevo análisis del tema y de las consecuencias que el mismo implica.

Medios periodísticos y la ciudadanía en general rechazaban lo normado por la ley, la cual a pesar de sus escasos artículos, era considerada un fuerte agravio a la intimidad de los usuarios de servicios de telecomunicaciones.

Numerosas opiniones doctrinarias surgieron referentes a la aquí tratada normativa, opiniones las cuales no coincidían en todos los casos y que de su análisis se llega a conclusiones radicalmente disímiles. Resulta ineludible llevar a cabo un repaso y estudio de estas corrientes de pensamiento para así lograr un real y pleno entendimiento de la cuestión en debate.

Con el fin de que la presente tarea sea lo más organizada posible, nos es necesario como punto de partida realizar una breve referencia al proyecto de ley mentor de la normativa analizada.

El proyecto

El proyecto presentado por el diputado Díaz Bancalari del Partido Justicialista, en fecha 15 de Julio de 2003, constante de 6 artículos, tenía una finalidad específica, consistente en la lucha contra la ola de secuestros extorsivos que se vivió en la república. El mismo tenía como destinatarios a los prestadores de servicios de comunicaciones móviles. A tal respecto, no existe margen de duda alguno considerando el título del proyecto: “Obligación de información de las empresas de prestación de servicios de comunicaciones móviles.”

Remitiéndonos a los fundamentos del diputado Díaz Bancalari, expresados en su proyecto de ley, podemos leer:

"Existe una necesidad actual, derivada de la utilización de nuevos medios comisivos de delitos, entre los que se comprende el uso disfuncional de los recursos derivados de los modernas telecomunicaciones.
Esta realidad que todos conocemos torna imperioso, con el fin de asegurar las "investigaciones" que se realizan para esclarecer estos delitos que utilizan los medios antes mencionados, regular la obligada colaboración sin excepción, de las entidades que tengan a su cargo la explotación de los respectivos servicios.
En este sentido no debe perderse de vista, que una de las herramientas más importantes para las investigaciones, en especial el de los secuestros extorsivos, las constituyen las intervenciones telefónicas.
Así la Dirección de Observaciones Judiciales de la Secretaria de Inteligencia del Estado, ve dificultada la realización de las diligencias encomendadas por los jueces, debido a cierta falta de colaboración o reticencia por parte de las empresas licenciatarias de servicios de telecomunicaciones.
Además entre los inconvenientes, se pueden mencionar la demora en que estas suelen incurrir para identificar a un determinado usuario. (…) Todo lo hasta aquí expuesto torna necesario esta regulación, sin perjuicio del resguardo de elementales garantías de orden procesal, así como también que lo requerimientos de información sean efectuados únicamente por la Dirección de Observaciones Judiciales, de conformidad a la ley 25.250."[1]

Sintetizando el texto del proyecto, a fin de extendernos lo menos posible en este punto, y poniendo en realce sus aspectos fundamentales, podemos concluir que el mismo buscaba la implementación por parte de los prestatarios de servicios de telecomunicaciones de los recursos técnicos necesarios para atender a las solicitudes de la Dirección de Observaciones Judiciales para la captación y derivación de las comunicaciones telefónicas, posibilitando su observación remota.

Planteo inicial de lo normado por la ley 25.873

La ley 25.873 reguló tres aspectos diferentes: I) la obligación de toda empresa de telecomunicaciones de colaborar con una investigación en la justicia y en concreto con los pedidos de informes; II) la obligación de retener ciertos datos de tráfico en materia de comunicaciones por el plazo de 10 años y III) la responsabilidad estatal por los daños que esta

[1] Cámara de Diputados, Expediente 3243-D-2003, Publicado en Tramites Parlamentarios N° 93, 15/07/2003

actividad pueda ocasionar.
Con el fin de tratar adecuadamente y de la forma más ordenada posible los interrogantes que nos plantea la denominada “Ley de escuchas y datos de tráfico”, procederemos a analizar su articulado en forma ordenada. De la lectura de sus artículos surgirán diversos cuestionamientos que deberán ser abordados en conjunto con el análisis de la reglamentación de ley, como así también motivarán el examen de normativas extranjeras y dictámenes de autoridades comunitarias supranacionales.

Articulo 1°: Captación, derivación y observación re mota de comunicaciones

Párrafo 1°

El primer articulo de la norma, el cual reza “Incorporase el articulo 45 bis a la Ley 19.798 con el siguiente texto”, establece en su párrafo inicial: "Todo prestador de servicios de telecomunicaciones deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente.”

Es importante destacar que las obligaciones que impone la ley 25.873 están referidas a los prestadores de telecomunicaciones en general y no sólo restringidas a los prestadores de telefonía o servicios de voz, ya sea telefonía fija o móvil. Recuérdese que la ley 19.798 define como telecomunicación a toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos, entendiéndose como correspondencia de telecomunicaciones a toda comunicación que se efectúe por medios de telecomunicaciones públicos o privados autorizados (Conf. artículo 2°, ley 19.798).
Asimismo, las disposiciones de la ley 25.873 se incorporan como artículos del Capítulo I, del Título III de la ley 19.798, referido a las disposiciones comunes que rigen para los servicios de telecomunicaciones en general, por lo que cabe concluir que estas nuevas normas abarcan todo tipo de telecomunicaciones, ya sea servicios de voz, transmisión de datos, valor agregado, acceso a Internet, etc.[2]

Por su parte, Fernández Delpech, ratificando lo recién apuntado, sostiene que debido a la

[2] Marcos, Gustavo H., Pinedo, Alejandro, Intervención de comunicaciones: Responsabilidad del los prestadores de servicios de telecomunicaciones, La Ley 2004 - A, p.1486

redacción de la norma, la misma es de plena aplicación a los Proveedores de Servicios de Internet. Interpretación basada en las siguientes consideraciones:

- Que la ley 19.798 a que se refiere es la Ley Nacional de Telecomunicaciones
- Que el Dec. 764/2000 que aprobó el Reglamento de Licencias para Servicios de Telecomunicaciones estableció la existencia de una licencia única para la prestación de los servicios de telecomunicaciones. Destacando que en los considerandos del decreto se expresa: "Que el anterior régimen establecía divisiones de servicios que no se correspondían con la evolución real de su prestación en el mundo, observándose, por ejemplo, que se establecían distingos entre el servicio telefónico, los servicios de telecomunicaciones- excepto telefonía- y los servicios de valor agregado. Que dichas distinciones no responden a tendencias cada vez mas actuales toda vez que poco a poco Internet podría transformarse en servicio básico y configurar la red básica, absorbiendo en su prestación a los demás servicios de datos y de telefonía en un periodo relativamente corto"
- Que la Guía orientativa para la solicitud de licencias de la Comisión Nacional de Comunicaciones contempla el otorgamiento de una licencia única que habilita al prestador a brindar al público todo servicio de telecomunicaciones. En su Capitulo III y dentro de la Guía de contenidos de planes técnicos, contempla expresamente el acceso a Internet y los servicios de valor agregado.[3]

Finalmente, como corolario, el decreto 1563/04 (reglamentario de la ley 25.873) pauta que se entenderá por telecomunicación toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, cable eléctrico, atmósfera, radio electricidad, medios ópticos y/u otros medios electromagnéticos, o de cualquier clase existente o a crearse en el futuro.

A la luz de lo expuesto es claro que la ley definitivamente sancionada, amplio considerablemente su ámbito de aplicación con referencia al proyecto de ley. Tal cuestión no esta exenta de críticas.

Llama la atención que no obstante decidir sobre temas tan sensibles para toda la sociedad, como lo son los referidos a la posibilidad de intervención y derivación de las comunicaciones, no tuvo específico trámite previo, ni exposición de motivos, ni tampoco debate parlamentario.

Como ya ha sido analizado, el proyecto presentado por el diputado Díaz Bancalari tuvo un objeto reducido a las comunicaciones móviles. Además dicho proyecto contó con un fundamento claro, que mas allá de disentir o no con él, daba acabada justificación a la propuesta legislativa.

[3] Fernández Delpech, Horacio, Internet: Su problemática Jurídica 2° Ed, Lexis-Nexis, Buenos Aires, 2004 , p.215

Cuando el proyecto pasa a dictamen de la Comisión Nacional de Comunicaciones, recibe un cambio sustancial. Vio modificado su objeto, ampliándose al servicio de telecomunicaciones, sin distingos y sin darse motivos ni fundamentos. Sin duda un cambio de objeto tan radical como el que recibió la norma, viendo importantemente modificado su ámbito de aplicación, requiere de una justificación adecuada que brinde los argumentos necesarios para comprender tal accionar. Llamativamente los justificativos no se dieron, y la modificación subsistió.
Con respecto al la referida falta de debate parlamentario, podemos señalar que la ley fue estudiada en la Cámara de Senadores por iniciativa del Poder Ejecutivo Nacional y tratada sobre tablas, es decir que se voto en general y en particular por la afirmativa. En tal oportunidad el senador Pichetto se refirió al "Régimen para la prestación de servicios de comunicaciones móviles (CD 132/03)" expresando:

"Se trata de una iniciativa del Poder Ejecutivo, ya sancionada por la Cámara de Diputados, que apunta a fortalecer la lucha contra el delito organizado, fundamentalmente en lo que se refiere a la logística para la captación de las líneas telefónicas en secuestros extorsivos. El Estado requiere de esta ley para que las compañías puedan actuar con celeridad en la captación de las líneas.
Este proyecto debe ser complementado, con otras iniciativas de otros señores senadores que tienden a evitar que en la Argentina se dé algo que es típicamente argentino, porque no ocurre en ningún lugar del mundo, esto es, la venta o alquiler de teléfonos celulares usados. En este país se hace cualquier cosa en esta materia. En cualquier esquina de esta ciudad se venden teléfonos celulares usados, lo que ayuda a la organización de las actividades delictivas. De esta manera, en los secuestros extorsivos las bandas pueden tener teléfonos celulares para poder funcionar alegremente en este país generoso.
Con la aprobación de este proyecto estamos dando un primer paso. Están pendientes muchos temas en cuanto a la seguridad. Lo dijeron los senadores Cafiero y Agúndez. El Congreso está en deuda con los temas de la seguridad. Aboquémonos en serio a tratar estas iniciativas. Hagamos una agenda con entidad y responsabilidad, y avancemos.
Creo que con este tema, además de dar una primera respuesta importante, le estamos dando al Estado mismo este instrumento para que las compañías puedan responder con rapidez, a fin de avanzar en las investigaciones contra las bandas organizadas que se dedican a los secuestros extorsivos en el país."

Es claro que el proyecto, a pesar de haber sufrido una considerable modificación, fue tratado por el Senado como si se tratase de una medida únicamente dirigida a los prestadores de servicios de comunicaciones móviles y acotada a la prevención y persecución de secuestros. No se debatió sobre la materia que se legisló.
Si bien podemos considerar que la voluntad real del legislador pudo estar dirigida a las

comunicaciones móviles, o máxime a las comunicaciones telefónicas, la ley se sancionó con términos amplios abarcativos de todo tipo de comunicaciones, un objeto infinitamente más amplio que el previsto en el proyecto original, siendo desde todo punto de vista reprochable e inaceptable.

Lo que si es claro, y no hay posibilidad de otras interpretaciones, es el aprovechamiento que del termino “telecomunicación” realizó el Poder Ejecutivo al reglamentar la ley. Se la definió como toda comunicación actualmente existente y las que se creen en el futuro.

El proyecto que nace con una motivación definida y un ámbito de aplicación determinado, recibe una modificación sin justificación en su sanción por el Congreso de la Nación. Finalmente, valiéndose del tal cambio, la reglamentación del Poder Ejecutivo confirma su amplio campo de aplicación, y no solo para la realidad tecnológica actual, sino también con la intención de perdurar en el tiempo y servir para los futuros desarrollos tecnológicos. Todo lo dicho, bajo la sola justificación que leemos en el decreto reglamentario de combatir el delito, el cual se sirve de los sistemas de comunicación para concretar su accionar delictivo, dándose como ejemplos los secuestros extorsivos y el narcotráfico.

No existe una justificación adecuada que manifieste claramente el por que, la necesidad, la motivación, de dar igual tratamiento interventivo a todos los medios de comunicaciones, amen de no tenerse en cuenta las diversidades de funcionamiento de los mismos, como su complejidad, y diversos grados de afectación de la intimidad de la persona que se obtendría con tal proceder injustificado.

Prosiguiendo con el análisis, resulta necesario debido a su trascendental importancia, afrontar el estudio del que puede considerarse uno de los puntos mas controvertidos de la normativa en análisis, referente a su colisión con el derecho a la intimidad. A fin de dar un adecuado tratamiento a la cuestión y arribar a una conclusión fundada para el planteo traído a discusión, se desarrollará en las próximas líneas el derecho citado, para luego analizar categóricamente la controversia y su respuesta.

Derecho a la Intimidad

Si bien podemos dar muchos conceptos distintos de este derecho, nos limitaremos a definirlo como la facultad que tiene cada persona de disponer de una esfera, espacio privativo o reducto inviolable de libertad individual, el cual no puede ser invadido por terceros, ya sean particulares o el propio Estado, mediante intromisiones de cualquier signo. El reconocimiento de este derecho presupone las condiciones mínimas indispensables para que el hombre pueda desarrollar su persona y su individualidad en inteligencia y libertad. Es el derecho que tiene un

hombre “a ser dejado en la soledad de su espíritu” (“the right to be alone”), según el concepto de Cooley.[4]

Llegando todavía más lejos en la valoración de esta garantía, Werner Goldschmidt ha señalado que el principio mismo de justicia consiste en asegurar a cada cual una esfera de libertad dentro de la cual cada persona sea capaz de desarrollar su personalidad, de convertirse de individuo en persona, de personalizarse.[5]

El ámbito de la intimidad individual está tutelado por la legislación común (Art. 1071 bis, Cód. Civ.). Esa protección encuentra amplio fundamento en el texto del Art. 19 de la ley suprema y en otras normas constitucionales, que importan manifestaciones del concepto general de inviolabilidad de la esfera intima (v. gr. Arts. 14, 17 in fine, 18).[6]

La afectación de la intimidad no solo se produce invadiendo el ámbito real del individuo afectado, sino también a través de la propalación de datos que deforman la realidad. Este derecho se tiene como derecho civil frente a los particulares, pero también como derecho publico subjetivo frente al Estado, para impedir su intromisión en la intimidad de la gente.[7]

La Corte Suprema de Justicia lo considera como derecho personalísimo, y lo define como "el derecho, que cada uno tiene, a decidir por sí mismo en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal"

Además, nuestro más alto Tribunal ha sentenciado: "El derecho a la intimidad protege jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños, significa un peligro real o potencial para la intimidad..."[8]

A nivel supranacional, podemos advertir que el derecho a la intimidad ha sido reconocido de modo universal en diferentes Tratados, Declaraciones y Convenciones, que en algún caso obligan a nuestro país en tanto signatarios del mismo, tal es el caso de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica, ratificado por la Ley 23.054)[9], Declaración Americana de Derechos y Deberes del Hombre[10], Declaración Universal

---

[4] Ekmekdjian, Miguel A., Manual de la Constitución Argentina 4° Edición Actualizada, Depalma, Bs.As., 1 997, p.95

[5] Introducción Filosófica al Derecho, Depalma, 6ª Ed., p.417. Allí el jusfilófoso también expresa: "La justicia protege la libertad del individuo de transformarse de hombre en persona. Desde este punto de vista existen en cada grupo dos partidos que pueden ser apellidados, con alguna imprecisión, como el partido de los hombres y el partido de las personas. El partido de los hombres se compone de los individuos que carecen del espacio de libertad necesario para convertirse en personas; mientras que el partido de las personas comprende a los individuos que disfrutan de él."

[6] Zarini, Helio Juan, Derecho Constitucional, Astrea, Bs. As., 1992, p.381

[7] Quiroga Lavié, Humberto, Constitución de la Nación Argentina Comentada Segunda Edición Actualizada, Zavalia, Bs. As., 1997, p116

[8] CSJN, “Ponzetti De Balbín, Indalia c/ Editorial Atlántida S.A.", 11-12-1984

[9] **Art. 11. Inc. 2** "...nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia,

de Derechos Humanos[11], Pacto Internacional de Derechos Civiles y Políticos[12]

Planteo de inconstitucionalidad de lo normado, de cara a la invasión de la esfera intima de los ciudadanos

Como ya ha sido esbozado, con sustento en el derecho a la intimidad, se han hecho fuertes criticas por considerar violatoria del mismo a la ley en examen, las cuales en diferentes términos han expresado su repudio.

Una de las tantas, la cual podemos considerar por su planteo sintetizadora de las demás, sostiene: ¿No se invade entonces la intimidad, cuando los servicios de telecomunicaciones a los que la comunidad toda se encuentra suscripta son "monitoreados" y "derivados" hacia la Dirección de Observaciones Judiciales de la Secretaría de Inteligencia de la Presidencia de la Nación, para su uso discrecional tanto del Poder Judicial o el Ministerio Público, cuanto por las fuerzas de seguridad?; o dicho de otro modo, ¿cómo se puede sostener que los ciudadanos puedan no poseer un sector o ámbito de vida privada fuera de toda intromisión? ¿Cómo se materializaría la garantía constitucional que protege la intimidad y privacidad si todo lo que expresamos, por cualquier medio que fuera, quedará almacenado dentro del gran "CPU del Estado" para su uso absolutamente discrecional?[13]

Cierto sector de la doctrina ha dado respuesta a tal cuestionamiento, sosteniendo que tal invasión no es real, y que la motivación normativa encuentra sustento en la legislación vigente. Así se ha dicho que, de conformidad con nuestro sistema constitucional, tanto para acceder al contenido de una comunicación como para acceder a la información asociada a ella se requiere orden de juez competente. Esto surge del Art. 18 de la Constitución Nacional, y de los Arts. 5, 21 y 22 de la ley 25.520 de inteligencia nacional[14]. Expresamente se aclara en su Art. 5 que

---

en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.", **Inc. 3.** "...toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

[10] **Art. IX.** Toda persona tiene el derecho a la inviolabilidad de su domicilio. **Art. X.** Toda persona tiene el derecho a la inviolabilidad y circulación de su correspondencia.

[11] **Art. 12**. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

[12] **Art.17.1**. Nadie ser 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.

[13] Nobile, Lisandro E, Nuevas formas de intromisión en la vida privada, ADLA 2005-C, 3589

[14] **Art.5.** Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario. **Art.21.** Créase en el ámbito de la Secretaría de Inteligencia la Dirección de Observaciones Judiciales (DOJ) que será el único órgano del

toda clase de comunicación -telefónica, por Internet, y por cualquier otro medio- está amparada por la privacidad y sólo con orden de juez competente se podrá proceder a su interceptación. Esta interpretación se refuerza, porque la ley de datos de tráfico (ley 25.873, Art. 1° y 2°) requiere expresamente que la colaboración de las empresas de telecomunicaciones y la sistematización de datos de tráfico tenga lugar "de conformidad con la legislación vigente". Por último, el Código Procesal Penal requiere para incautar estos datos una orden fundada de juez (Art. 236 CPP), salvo las reformas de la ley 25.760 respecto de las facultades fiscales en casos de secuestros). La única forma de obtener el contenido de una comunicación digital es entonces con una orden judicial. Toda otra interpretación sería inconstitucional.[15]
La tesis comentada, poniendo en realce la referencia que hace en su texto la ley 25.873 a “la legislación vigente”, sostiene que con tal frase se pone de manifiesto que la voluntad del legislador no ha sido la de atribuir nuevas competencias estatales, en especial a los organismos de inteligencia, o de disminuir las exigencias habilitantes que legitiman la intervención de las autoridades públicas allí mencionadas (Poder Judicial o Ministerio Público) que surgen del ordenamiento jurídico que actualmente regula la materia. Subrayándose de tal manera la necesidad de orden judicial para la procedencia de la intervención telefónica.

Teniéndose por planteado el cuestionamiento al texto legal, y habiéndose delineado brevemente la tesis que propugna la inexistencia de sustento de la crítica y a fin de poder dar una acabada y justificada respuesta al cuestionamiento que en este punto nos atañe, nos resulta ineludible entrar en consideración de una cuestión que data de antaño y la cual es merecedora de una respuesta en la actualidad y de manera definitiva. Nos referimos al secreto de las comunicaciones y la posibilidad de intervención de las mismas en la normativa argentina vigente.

Secreto de las comunicaciones

El derecho al secreto de las comunicaciones (extraído del secreto de la correspondencia epistolar en aplicación del Art.18 de la Constitución Nacional) protege implícitamente la libertad

---

Estado encargado de ejecutar las interceptaciones de cualquier tipo autorizadas u ordenadas por la autoridad judicial competente.

Art.22. Las órdenes judiciales para la interceptación de las comunicaciones telefónicas serán remitidas a la Dirección de Observaciones Judiciales (DOJ) mediante oficio firmado por el juez, con instrucciones precisas y detalladas para orientar dicha tarea. El juez deberá remitir otro oficio sintético, indicando exclusivamente los números a ser intervenidos, para que la DOJ lo adjunte al pedido que remitirá a la empresa de servicios telefónicos responsable de ejecutar la derivación de la comunicación. Los oficios que remite la DOJ y sus delegaciones del interior a las empresas de servicios telefónicos, deberán ser firmados por el titular de la Dirección o de la delegación solicitante.

[15] Palazzi, Pablo A., La controversia sobre la retención de datos de trafico en Internet, La Ley, columna de opinión, 28/04/2005, p.1

de las comunicaciones y, además de modo expreso, su secreto.[16] De manera que la protección constitucional se proyecta sobre el proceso de comunicación mismo, cualquiera sea la técnica de transmisión utilizada y con independencia de que el contenido del mensaje transmitido o intentado transmitir - conversaciones, informaciones, datos, imágenes, fotos, etc. -, pertenezca o no al ámbito personal, lo intimo o lo reservado.[17] Se garantiza a los interlocutores la confidencialidad de la comunicación, con lo cual el contenido de la misma se mantiene ajeno al conocimiento de terceros y reservado solo al conocimiento de los participes.

La Constitución Nacional no prevé una protección de todos los tipos de comunicaciones, reduciéndose a la epistolar. Lamentablemente, cuando fue objeto de reforma en el año 1994, el constituyente desaprovecho la oportunidad de actualizar el texto del artículo 18, teniendo en consideración las innovaciones telecomunicacionales que se generaron en las últimas décadas.

A pesar del silencio de nuestra carta magna, en el desarrollo normativo argentino nos encontramos con piezas legislativas que si hacen referencia directa a las telecomunicaciones. La Ley Nacional de Telecomunicaciones 19.798 establece en su articulo 18 la inviolabilidad de las telecomunicaciones, mientras que en el Art. 19 dilucida el significado de dicha inviolabilidad expresando que importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos.[18]

La Ley 25.520 de Inteligencia Nacional en su articulo 5° establece también este derecho: “las comunicaciones telefónicas, postales, de telégrafo o facsimil, o cualquier otro sistema de envió de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al publico, son inviolables en todo el ámbito de la Republica Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario”.

Como se ha dicho, la Constitución Nacional establece la inviolabilidad únicamente de la correspondencia epistolar a nivel comunicacional, ignorándose un vasto catalogo de medios actualmente existentes. Primeramente debemos tener en cuenta que al momento de su sanción obviamente los mismos no existían y la redacción de un precepto en términos más amplios que permitiera a posteriori abarcar las nuevas tecnologías es algo que seguramente se

---

[16] Carbone Carlos A., Grabaciones, escuchas telefónicas y filmaciones como medios de prueba. Derecho constitucional de utilizar los medios de prueba pertinentes. Rubinzal-Culzoni, Buenos Aires, 2005, p.190.

[17] Tribunal Europeo de Derecho Humanos (TEDH), sent. del 6-9-78, caso “Klass y otros”, consid. 68

[18] **Art. 18.** La correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente. **Art. 19.** La inviolabilidad de la correspondencia de telecomunicaciones importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos.

escapaba de la idea de los redactores. Consideremos que eran otras épocas en las cuales las innovaciones tenían otros tiempos, muy diferentes a los precipitados de hoy en día.
Sin embargo, y correctamente, es unánime en la doctrina el hecho de extender la protección constitucional, aplicándose por vía analógica a los nuevos medios de comunicación. Puede validamente sostenerse que cualquier tipo de comunicación goza de las mismas garantías que la correspondencia epistolar y que toda injerencia en ellos es inadmisible, exceptuándose los casos en los que sean cumplidas las exigencias constitucionales previstas para la ocupación de la correspondencia epistolar.
A esta aplicación analógica del articulo 18 de la Constitución nacional se llega juntamente con lo normado en su articulo 33, que consagra la vigencia de los derechos no enumerados en el catalogo constitucional positivo pero que nacen de la forma republicana de gobierno.[19]

La exigencia constitucional de ley reglamentaria de la intervención de las comunicaciones

Teniendo en claro que el articulo 18 por extensión de sus preceptos es aplicable a toda comunicación, mas allá de la correspondencia epistolar, debemos considerar el fragmento de su texto que estipula que “una ley determinara en que casos y con que justificativos podrá procederse a su allanamiento y ocupación”.[20]
Al día de hoy tal normativa no ha sido dictada, y desde que el procedimiento técnico es posible, las intervenciones telefónicas tienen lugar por medio de orden judicial.
Cierto sector de la doctrina se ha conformado con señalar que los derechos no son absolutos, pudiéndose restringirse el derecho en cuestión en virtud de una orden judicial si se están investigando delitos por estar en este caso en juego el orden público.
En el mismo sentido, se sostiene que la exigencia del dictado de una ley que establezca los casos y con que justificativos se podría allanar u ocupar la correspondencia, verbigracia, restringir la inviolabilidad de las comunicaciones telefónicas, puede cumplirse con el propio

[19] Cuando el Art. 33 de la CN expresa que “las declaraciones, derechos y garantías que enumera la Constitución, no serán entendidas como negación de otros derechos y garantías no enumerados; pero que nacen de la soberanía del pueblo y de la forma republicana de gobierno.”, está haciendo una declaración fundamental en el sentido de que todo el sistema de la Constitución está estructurado sobre las ideas democráticas de que los derechos se reconocen a las personas, no como gracia de un príncipe, sino antes bien, como integrantes de un pueblo “soberano” que, como lo declama el preámbulo, ha dado mandato a sus representantes para que dicten una Constitución que les asegure los beneficios de la libertad. La inviolabilidad de las comunicaciones telefónicas la entiende incluida en el Art. 18 CN por vía del Art. 33 CN. Maier, Jaime B, Derecho Procesal penal, 2° Ed, Del Puerto, Buenos Aires. 1995, p.6 94

[20] **Art. 18.** “Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. **El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación (…)”**.

texto constitucional que ampara las restricciones al derecho fundamental al secreto de las comunicaciones, y por tanto, como es la ley fundamental del Estado seria de aplicación inmediata.[21]

Contrariamente a lo expuesto, debe considerarse que si la constitución establece un derecho fundamental, sin posibilidad de su limitación, obviamente seria de cumplimiento imposible, y esa limitación seria la piedra angular de su construcción jurídica, lo que permitiría la orden judicial. Pero si no se sanciona una ley que desarrolle los principios constitucionales de limitación, sobre todo respetando los límites de la proporcionalidad, no puede convalidarse la restricción porque no puede caer en la esfera de la discreción judicial.[22]

Tomando como referencia lo acaecido en Brasil, es de señalar que la doctrina brasileña estaba conteste en la necesidad imperiosa de contar con un "diploma legal especifico" en materia de derechos fundamentales cuando se trate de restringirlos por propia invitación constitucional que remite a una "ley" y también para terminar con tantos abusos que en el campo de las intervenciones telefónicas se cometían diariamente. [23]

Retomando la situación de nuestro país, podemos decir sin lugar a dudas que la carencia de reglamentación necesita el dictado de una ley específica que cubra el requisito constitucional acabadamente. Es una ley que reviste trascendental importancia debido a su función de ponderación de valores e intereses que entran en conflicto a la hora de ordenar la medida en el marco de un proceso en el cual se ponen en juego el interés público y el interés individual.

Desde una interpretación literal cabria inferir que los constituyentes entendieron que esa ley específica era una ley dispuesta por el Congreso, la que se encargaría de establecer los requisitos y condiciones para limitar esos derechos.[24]

Así en el panorama legislativo actual nos encontramos con la Ley Nacional de Telecomunicaciones 19.798 sancionada en el año 1972. La misma si bien establece en su articulo 18 que la interceptación solo procederá a requerimiento de juez competente y en su articulo 19 brinda un catalogo de acciones prohibidas en protección de la inviolabilidad de las telecomunicaciones, no podemos considerar cumpla los requisitos establecidos por el Art. 18 de la CN. En el mismo sentido recién apuntado, la Ley 25.520 de Inteligencia Nacional, la cual ya ha sido citada en su articulado pertinente, no consuma el mandato constitucional. Igualmente es de destacar que su Art. 19 prevé que la autorización para la intervención será concedida por un plazo no mayor de sesenta días prolongable por otros sesenta como máximo cuando ello fuera imprescindible para completar la investigación en curso. A lo cual es de sumar el hecho de establecerse en su articulado la destrucción de lo grabado cuando no se

---

[21] De Llera Suarez Barcena, Eduardo, El régimen jurídico ordinario de las observaciones telefónicas en el proceso penal, Revista Judicial, 1986, N°3, p.11.

[22] López Barja de Quiroga, Jacobo, Las escuchas telefónicas y la prueba ilegalmente obtenida, Akal, 1989, p.156

[23] Gomez, Luis Flavio y Cervini, Raul, Interceptacao telefonica, Revista dos Tribunais, Sao Paulo, 1997, p.84

[24] González Calderón, José, Derecho Constitucional, Lajouane, Bs. As, 1931, t. II, p.132

diera iniciación a la causa.

Por su parte, a nivel codificación procesal, hallamos la previsión en el artículo 236 del CPPN.[25]

En definitiva, es claro que hasta ahora la ley que establezca en que casos y con que justificativos se podrá realizar la intervención de la comunicación no existe. Toda la normativa señalada no establece los casos, los delitos, con que fundamentos y de acuerdo a que proceder se efectuará.

Resulta ineludible dar cumplimiento a la exigencia constitucional de dictar la ley que reglamente las intervenciones. Asimismo es indudable que la misma debe provenir del Congreso de la Nación dada la entidad del derecho a restringir. Por lo cual pereciera adecuado la sanción de la misma con la posterior adhesión provincial, a fin de lograr un texto único de vigencia en todo el país, lo cual permite un tratamiento absolutamente claro de la cuestión y sin diferencias de matices en cada provincia. Esta ley finalmente establecería: a) cual es la autoridad competente para ordenar la interceptación de las comunicaciones, b) en que casos puede hacerlo, c) con que justificativos, d) las formas mínimas según las cuales debe ejecutarse la interceptación, e) la duración de la medida y su consecuente posibilidad de prorroga, f) el destino de lo grabado tras la investigación, etc.

Respuesta final concerniente a la inconstitucionalidad primeramente planteada

Lo normado por el artículo 1° de la ley 25.873 es desde todo punto de vista reprochable e inaceptable. Su breve redacción se inserta en una realidad normativa referente a las telecomunicaciones que no es la debida, atento a la falta de sanción de la ley reglamentaria de la intervención de las mismas. Tal legislación debe ser dictada de cara a la evolución de las telecomunicaciones y sus repercusiones cada día mayores en todos los ámbitos de la vida ciudadana. Dicha ley deberá afrontar la redacción de preceptos que regulen acabadamente las necesidades actuales, como así prever que su texto pueda sobrellevar desafíos a futuro de la mejor manera posible, mas allá de tener en cuenta que los desarrollos tecnológicos muchas veces sorprenden al mas instruido en la materia y resulta de una gran dificultad poder adelantarse a tales innovaciones a nivel de previsión legislativa.

La finalidad del artículo 1° de la ley 25.873, de establecer una sistema que posibilite la captación y derivación de las comunicaciones que transmiten los prestadores, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público las 24 horas del día y los 365 días del año (en su intento por luchar contra la delincuencia), terminaría por establecer un sistema del cual los servicios de inteligencia podrían valerse para concretar una vigilancia continua de los usuarios, avasallando las garantías constitucionales en absoluto

[25] **Art. 236.** El juez podrá ordenar, mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedirlas o conocerlas.

silencio. Si bien la normativa en apariencia cree resguardar estas garantías al establecerse que el procedimiento se hará de acuerdo a la normativa vigente y a requerimiento del Poder Judicial o en su defecto del Ministerio Publico, nada quita que el día de mañana y de una manera ciertamente posible, se utilicen los recursos en forma secreta, lo cual por su simpleza de concreción alerta y preocupa en demasía.

Son conocidas las directivas que el presidente de los estados Unidos George W. Bush dirigió a la National Security Agency (NSA) para espiar llamadas telefónicas y mensajes de correo electrónico, aun en violación de las leyes de su país, y con la justificación de luchar contra el terrorismo. En el mismo sentido, se ha alertado sobre el software de la Federal Bureau of Investigation (FBI) denominado "Carnívoro"[26]. Dicho programa se instala en el servidor que tramita la conexión del sospechoso y del cual no hay garantías que limite la vigilancia al correo del sospechoso y no de todos los usuarios del servidor.

Con la implementación de lo normado por la ley 25.873 el secreto de las comunicaciones se vería gravemente vulnerado. En cierta manera podríamos terminar viviendo en una sociedad *Orwelliana,* en donde nuestra vida intima es continuamente vigilada, pero no a través de *telepantallas*[27] instaladas en nuestras casas, lugares de trabajo, lugares públicos o medios de transporte, sino mediante los sistemas de comunicación que estamos habituados a utilizar. Nuestras computadoras, teléfonos fijos y celulares, en definitiva instrumentos de los cuales nos valemos diariamente y estamos altamente acostumbrados a manejar, no reparando en mayores precauciones en tal accionar, serian el medio de vigilancia silencioso con el cual el Estado en su lucha contra la actividad delictiva se valdría para tener un conocimiento más allá del necesario para tal fin. Se abordaría directamente nuestra zona de intimidad, esa esfera en la cual cada individuo se desarrolla y vive exento de un control foráneo a la misma.

En el siglo XIX, Sir Thomas Erskine May, constitucionalista británico, expresó: *"Próximo en importancia a la libertad personal es la inmunidad de sospecha y celosa observación, los*

---

[26] El 17 de Septiembre de 2001, el Instituto de Investigación Tecnológica de Illinois presentó un informe sobre este programa en el que dudaba sobre las exigencias de seguridad y sensatez del sistema. Entre los autores del citado informe se encuentran Steven M. Bellovin y Matt Blaze de Laboratorios AT&T, David J. Farber de la Universidad de Pennsylvania, Peter Neumann de SRI International y Eugene Spafford del Centro para la Educación e Investigación en Seguridad de la Información de la Universidad de Purdue.

[27] "A la espalda de Winston, la voz de la telepantalla seguía murmurando datos sobre el hierro y el cumplimiento del noveno Plan Trienal. La telepantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior a un susurro, era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído. Por supuesto. No había manera de saber si le contemplaban a uno en un momento dado. Lo único posible era figurarse la frecuencia y el plan que empleaba la Policía del Pensamiento para controlar un hilo privado. Incluso se concebía que los vigilaran a todos a la vez, pero desde luego podían intervenir su línea de usted cada vez que se les antojara. Tenía usted que vivir - y en esto el hábito se convertía en un instinto - con la seguridad de que cualquier sonido emitido por usted sería registrado y escuchado por alguien y que, excepto en la oscuridad, todos sus movimientos serían observados." Extracto de la Novela de George Orwell, 1984, Colección Literaria Universal, 2005, p.9

hombres en ese caso pueden disfrutar sin restricciones de su libertad e ir y venir como les plazca, pero si sus pasos son seguidos por espías e informantes, sus palabras utilizadas para formular incriminaciones, sus compañías observadas como conspiradoras, quien podrá decir que son libres". Hoy en día los espías ya no son personas a las cuales podemos percibir y prestar atención, son por el contrario productos de la innovación tecnológica que funcionan en silencio y de los cuales es posible aprovecharse en forma indiscriminada, atentando contra fundamentales garantías constitucionales.

Sin dudas la actitud del legislador de querer enfrentarse a problemáticas actuales que atentan contra la seguridad en nuestra sociedad es una actitud positiva y que debe existir necesariamente, pero asimismo es preciso que en tal proceder se guarden debidamente las garantías constitucionales y no se creen medios que puedan dar a abusos amen de la real voluntad del legislador. No debe olvidarse la advertencia formulada por la Corte Europea de Derechos Humanos relativa a los peligros de restringir las libertades ciudadanas bajo la desproporcionada invocación de consideraciones de seguridad.[28]

Notas de la ampliación de objeto abarcando Internet

Como se ha señalado, el texto de la normativa ha visto ampliado su objeto haciéndose referencia a las telecomunicaciones, abarcándose de tal manera a las realizadas en Internet.

Amen de todos los argumentos dados en contra de la sanción de una normativa que avale una intervención generalizada de las comunicaciones por parte del Estado, creando una especie de gran computadora controladora del ámbito privativo de nuestras vidas, debemos subrayar que la norma no ha reparado en dos aspectos fundamentales necesarios para su concreción: su medio de producción procesal y el procedimiento técnico de realización de la medida.

Viabilidad procesal de la medida

Como es sabido, los medios de prueba constituyen la actividad desarrollada por el juez, las partes y terceros, dentro del proceso, con el fin de traer al mismo fuentes de prueba; esa actividad es realizada de acuerdo a lo indicado en cada ordenamiento procesal. Por su parte las fuentes de prueba son las personas, las cosas cuya existencia es previa al proceso e independientes del mismo, que tienen conocimiento o representan hechos que interesan en el proceso.

[28] Pronunciamiento del 6 de Septiembre de 1978, Series A-N°28, en el caso Klass y otros c/Alemania, la C orte Europea de Derechos Humanos decidió que los Estados no deben "en el nombre de la lucha contra el espionaje y terrorismo adoptar cualquier medida que estimen apropiada".

Un cuestionamiento que ha sido debatido cabalmente por la doctrina es el referente a la enumeración taxativa o enunciativa de los medios probatorios, y como consecuencia el principio de la libertad probatoria.

Si uno se embarca en la ruta del *numerus clausus* podría chocar en muchas legislaciones con una pared que le impida realizar una determinada probanza por no estar contemplada en el rito procesal y produciendo su ilegalidad al ser arrimada al proceso.

Por el contrario, si estas legislaciones fueran interpretadas a la luz de una enumeración enunciativa, el problema de la ilicitud desaparecería, debiendo solo velar por que los medios no contemplados no violen los derechos fundamentales de la defensa en juicio y el debido proceso.

Actualmente, ninguna legislación puede hacer frente a los desarrollos tecnológicos y ser abarcativa del amplio catálogo de fuentes de prueba. Consideremos la fotografía digital, las grabaciones, las filmaciones, los documentos electrónicos, la firma digital, por nombrar algunos, y vaya saber cuales vendrán en los próximos años. Este es el verdadero problema del derecho procesal actual, más allá de la taxatividad o no de los medios de prueba, evaluar debido al progreso tecnológico, la forma de acercar las pruebas al proceso.

El articulo 378 del Código Procesal Civil y Comercial de la Nación (CPCCN) dispone: “La prueba deberá producirse por los medios previstos expresamente por la ley y por los que el juez disponga, a pedido de parte o de oficio, siempre que no afecten la moral, la libertad personal de los litigantes o de terceros, o no estén expresamente prohibidos para el caso”.

Del citado precepto surge que los medios de prueba son ilimitados, la ley prevé algunos pero indica que los no previstos se diligenciaran aplicando por analogía las disposiciones de los que sean semejantes o, en su defecto, en la forma que establezca el juez.[29]

El Código Procesal Penal de la Nación (CPPN) en el titulo sobre Disposiciones generales para la instrucción, Art. 206 establece que no regirán en la instrucción las limitaciones establecidas por las leyes civiles respecto de la prueba, con excepción de las relativas al estado civil de las personas. Disposición que permite interpretar que tampoco existe limitación de los medios de prueba.

A nivel provincial, a modo de ejemplo, En los Códigos Procesales Penales de las provincias de Río Negro[30] y Santa Fe[31] nos encontramos con idéntica redacción a la del Código de la Nación, arribándose a la misma conclusión antes expuesta.

Más claro resulta el CPP de la provincia de Buenos Aires, que en su artículo 209 reza: “Todos los hechos y circunstancias relacionados con el objeto del proceso pueden ser acreditados por

---

[29] Arazzi, Roland, Derecho Procesal Civil y Comercial, Rubinzal Culzoni Editores, Bs. As. 1999, Tomo I, p.335

[30] **CPP Art. 197:** No regirán en la instrucción las limitaciones establecidas por las leyes civiles respecto de la prueba, con excepción de las relativas al estado civil de las personas

[31] **CPP Art. 209:** En la investigación no regirán las limitaciones establecidas por las leyes civiles respecto de la prueba, salvo las relativas al estado civil de las personas.

cualquiera de los medios de prueba establecidos en este Código (…) Además de los medios de prueba establecidos en este Código, se podrán utilizar otros siempre que no supriman garantías constitucionales de las personas o afecten el sistema institucional".

De lo expuesto puede concluirse que en nuestro derecho, tanto para el proceso civil, comercial, como para el proceso penal, existe una consagración del principio de la libertad de prueba referente a los medios.

En el mismo sentido, el principio de la no taxatividad de los medios de prueba es reiteradamente sustentado por la jurisprudencia, por cuanto se sostiene que es un principio inconmovible del sistema penal probatorio vigente en el Código Procesal Penal, de modo que considerar abierta la enumeración que la ley hace de ellos implica que la presencia de algún medio probatorio que no tenga regulación especifica no obsta a su admisión si resulta pertinente para comprobar el objeto de prueba.[32]

La razón del imperio de la regla de la libertad probatoria no es otra que el reconocimiento de que el fin asignado al proceso - teniendo una especial relevancia en el proceso penal - no puede ser alcanzado si quien debe cumplir con esa meta no goza de tal amplitud en la esfera probatoria. Dicho en otros términos: el juez para alcanzar la verdad real, para desentrañar el suceso histórico que constituye el objeto de su proceso, debe contar con medios suficientes para desplazarse por el ámbito de los hechos, y para determinarlos sin condicionamientos que esterilicen su labor.

Por supuesto, esta facultad no es ilimitada, lo que sería contrario al espíritu de un Estado de Derecho. Existen ciertamente restricciones tanto en referencia al objeto, como a los medios de prueba. Así, y en relación al primer límite, la prueba debe recaer sólo sobre hechos o circunstancias que estén relacionadas con la hipótesis que originó el proceso (principio de pertinencia). En referencia a lo segundo no se pueden utilizar medios de prueba que afecten la moral, expresamente prohibidos (v.gr utilización de cartas sustraídas), o que sean incompatibles con nuestro sistema procesal (v.gr. indagatoria prestada bajo juramento); o que no estén reconocidos por la ciencia como idóneos para provocar conocimiento (v.gr. adivinación).

A nivel nacional, El Código Procesal Penal de la Nación establece en su artículo 236 que el juez podrá ordenar mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedirlas o conocerlas. De la lectura del citado precepto, surge claramente que su texto hace extensible la posibilidad de intervención de las comunicaciones a otros medios que nos sean telefónicos, por lo cual, y

[32] CNFed.CCorr. de Cap.Fed., in re "Cingolani y otros s/Procesamiento", res. 15.010 del 19-2-97

dejándose de lado el análisis referente a la libertad de medios probatorios, la autorización para la realización de la medida encuentra sustento en la misma normativa.

A nivel ordenamiento civil, nos encontramos con otra realidad. Si bien es cierto que existe un silencio del Código Civil como así también en los ritos con respecto a la cuestión de las intervenciones de comunicaciones, no puede interpretarse que tal ausencia signifique su prohibición. Recordemos que la limitación al derecho fundamental a la correspondencia epístolar y telefónica que surge del articulo 18 no hace una referencia directa al sistema penal, a lo que se suma el hecho de que la Ley de Telecomunicaciones en su articulo 18 prevé la limitación al secreto mediando orden de juez competente y el articulo 5° de la ley 25.520 a su vez establece que las comunicaciones telefónicas son inviolables excepto cuando mediare orden o dispensa judicial.

Es claro que la ley procesal penal no es la única que podría tener la necesidad de reglamentar la garantía, pues también en los procedimientos civiles y comerciales podrían presentarse casos en los que podría eventualmente justificarse como necesario y razonable el recurso a la injerencia en las telecomunicaciones.[33]

En este estado de las cosas, y debido a la ausencia de ley reglamentaria al articulo 18 en su parte referente a la intervención de las comunicaciones, el juez competente en materia no penal y a nivel nacional, como así también los jueces provinciales con competencia en diversas materias a los cuales no les asista la facultad interventiva expresa en las normativas procesales provinciales, podrían echar mano, mediante el instituto de la libertad probatoria, a la intervención de las comunicaciones. Obviamente la intervención se debería decretar adecuadamente sustentada y observando el debido respeto a las garantías procesales y constitucionales, vigilando la no infracción de las mismas con el fin de que la medida no devenga en inutilizable, debiendo ser excluida por su trasgresión a la doctrina del fruto del árbol venenoso[34]. Haciendo eco de la misma, diversos fallos nacionales han hablado de la necesidad de salvaguardar los derechos del individuo que emanan de la Constitución, de modo de privilegiar el respeto a su dignidad y a los derechos esenciales que de allí derivan. Paralelamente se ha afirmado que en la comparación de los valores en juego - el respeto a las

---

[33] García Luis M., La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal penal de la Nación: un cheque en blanco para espiar nuestra vida privada; Cuadernos de Doctrina y Jurisprudencia Penal, Ad-Hoc, Bs. As., 1995, N°6, p.419

[34] Doctrina originada en los Estados Unidos de Norteamérica, donde recibió el nombre de *fruit of the poisonous tree.* Su génesis se remonta al caso"Silverthorne Lumbre Co. V. United States", 251 US385 (1920) en el que Corte estadounidense decidió que el Estado no podía intimar a una persona a que entregara documentación, cuya existencia había sido descubierta por la policía a través de un allanamiento ilegal. Posteriormente, en "Nardote v. United States", 308 US388 (1939), ese tribunal hizo uso por primera vez de la expresión "fruto del árbol venenoso", al resolver que no solo debía excluirse como prueba en contra de un procesado grabaciones de sus conversaciones efectuadas sin orden judicial, sino igualmente otras evidencias a las que se había llegado aprovechando la información que surgía de tales grabaciones.

garantías individuales por un lado, y el interés de la sociedad en que los delitos sean investigados por otro - debe acordarse primacía a los primeros por tratarse de dictados de la Ley Suprema[35]. La garantía del debido proceso y la que consagra el principio de que nadie puede ser penado sin un juicio previo fundado en ley se verían naturalmente menoscabadas si se permite que se utilice en contra de un individuo pruebas obtenidas en violación a sus derechos básicos[36].

La ausencia de normativa especifica referente a la intervención de comunicaciones y el entendimiento del termino comunicación en su sentido literal y por tanto abarcativo de todo tipo de comunicaciones, (no solo las telefónicas), encontrándose por tal razón dentro de su catalogo las desarrolladas por Internet, viabilizan a nivel procesal la posibilidad de decretar la medida.

Procedimiento técnico

Internet puede definirse en termino simples como una red de computadoras localizadas en diferentes lugares del mundo interconectadas entre si mediante líneas de comunicación de alta velocidad, permitiendo el intercambio y acceso a una cantidad grandiosa de información.

El Federal Networking Council (FNC) de los Estados Unidos en Octubre de 1995 ha definido a Internet de la siguiente forma: “Internet se refiere al sistema global de información que; 1) Esta lógicamente unido por un espacio global único de dirección basado en el protocolo de Internet TCP/IP o sus extensiones/continuaciones subsecuentes, 2) Es capaz de soportar comunicaciones usando la serie de protocolos de transmisión Control Protocol/Internet Protocol (TCP/IP y sus extensiones/continuaciones subsecuentes, y/u otros protocolos IP compatibles; y 3) ofrece o hace accesibles, ya sea publica o privadamente, servicios de alto nivel soportados en las comunicaciones e infraestructura relacionada descripta aquí.” [37]

El servicio de Internet es prestado por los denominados proveedores de servicio (ISP), los cuales normalmente, dejando de lado los servidores gratuitos, por medio del pago de un abono mensual y otorgando en consecuencia un nombre de usuario y contraseña, permiten la navegación por la Red. El acceso a la misma es diferente según el tipo de servicio que se contrate, así nos encontramos con el mas “antiguo” conocido como *Dial-Up*, el cual utiliza como medio de enlace el cableado telefónico; el Cable Módem, que se vale de la red de televisión por cable; *ADSL*, el cual también funciona por medio del cableado telefónico, pero a velocidades mucho mayores mediante el uso de una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales. Para disponer de *ADSL*, es necesaria la instalación de un filtro que se encarga de separar la señal telefónica convencional

[35] Caso “G.E” Cam. Fed. La Plata, Sala II, 25/09/1984, ED 112, p.363

[36] Caso “P.G”, CN Crim.Corr., Sala III, 6/07/1982, ED 101, p.252

[37] Informe del 24-10-1995 del Federal Networking Council (FNC) de los Estados Unidos

de la que usaremos para conectarnos con Internet. Finalmente, nos encontramos con las conexiones por antena o por vía satelital, que se valen de ondas enviadas y recibidas por aparatos de transmisión trabajando en forma inalámbrica uno de otros.

Sea cualquiera de los recién mencionados, el servicio con el que cuenta el usuario, la conexión siempre se realiza por medio de la vinculación de la computadora personal con el servidor del proveedor. La operación consiste en una serie de procedimientos técnicos que permiten la intercomunicación de ambos actores e identifican a la terminal, permitiéndole la conexión a Internet. Al realizarse esta identificación y permitir la conexión del usuario se le asigna al mismo un numero que lo identifica en la red, denominado numero IP. El mismo consiste en un identificador registrado (para evitar duplicados) conocido como Direcciones IP Públicas, para un ordenador o dispositivo en una red de TCP/IP[38].El formato es una dirección de 32 bits (4 bytes), que se representa usualmente por cuatro cifras (de 0 a 255) decimales separadas por puntos. (v.gr. 255.255.255.100).

El mismo es en contadas ocasiones de tipo fijo (Direccionamiento IP estático), lo cual significa que siempre se tiene el mismo y cuando quiera que uno se conecte el número permanecerá inmutable. Pero, en la amplia mayoría de los casos ese numero IP, especie de DNI de la maquina en la Red, es variable (Direccionamiento IP dinámico), siendo asignado al ínternauta cada vez que se conecta.

Ahora bien, ¿como es posible lograr la “intervención” de la comunicación vía Internet que la persona realiza cuando no posee un numero que la identifique en todos los casos?, no se trata de una línea telefónica, la cual es identificada con un numero concreto, inmutable y que esta asociada a su titular. Y ampliando mas el interrogante, ¿que debemos entender en el vasto catalogo de acciones desarrollables en Internet como comunicación? Si se pudiera efectivamente intervenir la computadora se tendría un total control de lo que en la misma se realiza, verbigracia, charlas por Messenger u otros programas de mensajería instantánea, comunicaciones desarrolladas por telefonía IP[39], intercambio de archivos con otros usuarios, sitios Web visitados, conexiones establecidas para la descarga de archivos, etc.

---

[38] Protocolo de red. Consiste en el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red. En su forma más simple, un protocolo se puede definir como las reglas que gobiernan la semántica (significado de lo que se comunica), la sintaxis (forma en que se expresa) y la sincronización (quién y cuándo transmite) de la comunicación.

[39] Telefonía basada en la tecnología VoIP (Voice over IP- voz sobre IP), la cual permite la transmisión de la voz a través de redes IP en forma de paquetes de datos, habilitando la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando una PC, Gateways y teléfonos estándares. Esta tecnología digitaliza la voz y la comprime en paquetes de datos que se reconvierten de nuevo en voz en el punto de destino. Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

Retomando el punto en desarrollo, poder lograr la intervención de la comunicación en Internet significaría establecer un Standard en las conexiones a Internet, IPs fijos para todos los usuarios, *software* limitado y prohibición de bloquear puertos de comunicación en las computadoras o utilización de cualquier tipo de programa *firewall*.

Asimismo es de destacar, que dicha reglamentación que torne operativa la interceptación, dejaría las puertas abiertas a un total acceso y control de la información asentada en el soporte físico de la PC (Disco Rígido), como así también de la información asentada en los dispositivos de almacenamiento móviles introducidos en ese momento en la computadora. Lo cual sin duda alguna excede el objeto de la medida.

Con el establecimiento de un Standard de conexión, se atentarían contra un sinfín de derechos garantidos por nuestra normativa vigente, ya sea el derecho a la libertad de contratar, libertad de comercio, libertad de elección de los consumidores, el derecho a la propiedad y obviamente el derecho a la intimidad, resultando mecanismos propios de un régimen autoritario y muy alejado de los valores de una sociedad que vive en democracia.

Recordemos que la palabra democracia tiene dos contenidos: uno formal y otro sustancial. El primero se relaciona efectivamente con que órganos del estado existen y como y entre quienes se eligen los magistrados, que posición ocupan y que relaciones guardan entre si. En este aspecto, la democracia es una forma de gobierno en la que, dicho esto muy sencillamente, el acceso al poder esta abierto a la generalidad.[40]

El segundo se refiere a determinados patrones de conducta que deben seguir quienes mandan y quienes obedecen: lo que ha dado en llamarse el “estilo de vida democrático”. La democracia como forma de Estado implica, según Pericles, el apego cotidiano de esa generalidad a determinados valores. Los romanos, por ejemplo, acuñarían a este respecto un afortunado aforismo; vivir honestamente, no dañar al prójimo y tratar justamente a todos.[41]

El Estado, actualmente considerado como un instrumento del que se vale la sociedad para el aseguramiento de la convivencia, ocupa una posición fundamental garantizándole al hombre el amparo de sus derechos individuales.

Por eso mismo, es también la fuente de todas las reglas relativas a las relaciones de los individuos con el Estado: este está obligado a proteger los derechos individuales y solo puede limitarlos en la medida en que esta limitación sea razonable y necesaria para asegurar la protección de los derechos de todos.[42]

Hoy en día la concepción de la democracia vas mas allá de los términos estrictamente políticos, se tiende a concebirla de una forma mas concreta y sustantiva: la democracia significa para el hombre derechos individuales, elecciones personales, estilo de vida. La libertad implica, por una parte, reclamos sustanciales, derechos y opciones reales para los individuos particulares,

[40] Graña, Eduardo, Álvarez, César, Principios de Teoría del Estado y de la Constitución, Ad-Hoc, Bs. As., p.174

[41] Honeste vivere, alterum non laederes, ius suum quique tribuere

[42] Duguit, Leon. Las transformaciones del derecho publico, Francisco Beltran, Madrid, 1915, p. 45

pero también, como lo más importante, que ninguna mayoría puede ni debe tocar la zona de derechos.[43]

Cualquier intento de concreción de una normativa limitativa de los medios de acceso a Internet como la anteriormente señalada, resultaría un atentado directo a las libertades que el hombre actualmente disfruta en nuestra sociedad, lo cual es sin duda alguna absolutamente inconcebible e inaceptable.

Párrafo 2°

El párrafo segundo, del artículo 1° en análisis, establece que deberán los prestadores de servicios de telecomunicaciones soportar los costos derivados de la obligación puesta en cabeza de los mismos en el párrafo inicial y dar cumplimiento a la misma a toda hora y todos los días del año.

Aquí nos encontramos con la que es posiblemente una razón determinante que coadyuvo a la suspensión de la ley 25.873 por la trascendental negativa de los prestadores de servicios de telecomunicaciones a su acatamiento. El factor económico.

El Decreto 1563/2004, reglamentario de la ley en cuestión, en su articulo 2° inciso B) establece que cuando, por el tipo de tecnología o estructura de redes seleccionado u otras razones técnicas, resulte necesario utilizar herramientas o recursos técnicos, inclusive software o hardware específicos, para la interceptación y derivación de las comunicaciones, las compañías licenciatarias de servicios de telecomunicaciones deberán disponer de estos recursos desde el mismo momento en que el equipamiento o tecnología comience a ser utilizado. Complementariamente, el inciso I) pauta: “Asimismo, los operadores deben poner a disposición los medios técnicos y humanos necesarios para que esa información pueda ser recibida en tiempo real y en condiciones de ser interpretada por el órgano del Estado encargado de ejecutar las interceptaciones, salvedad hecha, en su caso, de una comunicación que se encuentre en curso, al momento mismo de la efectivización de la interceptación.”

Finalmente el inciso O), del mismo artículo 2°, instituye: “Los prestadores de servicios de comunicaciones, deberán soportar los costos de todo equipamiento, elemento tecnológico (software o hardware), vinculación, línea o trama, nueva o existente, necesaria para la captación de las comunicaciones y conexión efectiva entre sus centrales y el lugar de observación remota, y la obtención de los datos asociados en las condiciones establecidas en la presente norma. Asimismo, deberán tomar a su cargo los costos de equipamiento, personal, insumos y todo otro gasto que resulte necesario para el cumplimiento de las obligaciones establecidas en la ley conforme al presente decreto, incluyéndose los servicios que se presten al órgano encargado de ejecutar la interceptación para transportar las telecomunicaciones, y

[43] Friedman, Lawrence M., La republica de las opciones infinitas, Grupo Editor Latinoamericano, Bs. As., 1992, p.32

los del tendido de cualquier vínculo con dicho propósito, como asimismo la totalidad de los servicios o actividades que fueran necesarios para el cumplimiento de las tareas que impone para la materia la normativa aplicable.”

Sin olvidar las conclusiones dadas antecedentemente, contrarias a la implementación por parte del estado de un sistema que posibilite la captación y derivación de las comunicaciones que transmiten los prestadores de comunicaciones para su observación remota, cabe realizar ciertas precisiones.

A través de lo normado, el Estado se vale de los recursos técnicos y la infraestructura de los prestadores de comunicaciones con el fin de aprovecharlos en su lucha contra la delincuencia, estableciendo asimismo la obligación de los prestadores de soportar en forma exclusiva los costos necesarios para la ejecución definitiva de lo normado.

Resulta claro del texto y espíritu de la ley y decreto reglamentario que las obligaciones impuestas a los prestadores de telecomunicaciones no constituyen "cargas" propias de la prestación de los servicios de telecomunicaciones como por ejemplo la obligación de interconectar sus redes. Además, también es de considerar que los usuarios de los servicios de telecomunicaciones no obtienen ningún servicio o prestación adicional, que por tanto permita trasladar a sus abonos por servicio, el recupero de las inversiones necesarias para la implementación del sistema realizadas por los prestadores.

En virtud de nuestro texto constitucional, la propiedad tiene la característica de inviolabilidad, por tanto nadie puede ser privado de la misma sino excepcionalmente. En tal sentido, si bien es motivo de consenso que el estado puede excepcionalmente afectar la propiedad privada para lograr fines de interés general, dicha afectación debe tener una adecuada reparación. Conjuntamente, no debe olvidarse que el sentido asignado al término propiedad en el derecho constitucional, excede considerablemente al que posee en el derecho civil, comprendiendo de tal manera todos los intereses apreciables que el hombre puede poseer fuera de si mismo, de su vida y de su libertad.

Por tanto, al disponer la normativa en estudio, que los costos derivados de la obligación impuesta, deberán ser soportados por los prestadores de comunicaciones, vulnera y afecta injustificadamente el derecho de los mismos a la propiedad.

En el mismo sentido, surge del articulo 16 de la Constitución Nacional que la igualdad es la base del impuesto y de las cargas públicas. De esta manera queda determinado que los costos derivados de una política pública tendiente al logro del bienestar general no pueden ser distribuidos de forma desigual o desproporcionada entre sus beneficiarios.

Por lo expuesto, es de concluir que si en definitiva lo que se busca es la protección de la comunidad de ciertas amenazas delictivas, no es posible imponer a los prestadores de telecomunicaciones la total asunción de los costos resultantes de la implementación de los requisitos técnicos. Resulta ineludible que el Estado en su propósito de lucha contra la

delincuencia, en forma generalizada y con más razón cuando signifique la implementación de modernos y gravosos sistemas, financie los costos con los impuestos que el Tesoro Nacional percibe en forma equitativa y proporcional de toda la población, de manera de no afectar injustificadamente la propiedad privada.

Párrafo 3°

Finalmente el párrafo tercero se limita a establecer que será tarea del Poder Ejecutivo reglamentar las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Publico.

El Decreto 1563/2004, cumple con la tarea encomendada por el texto legislativo, encontrándonos en el mismo con las regulaciones de las condiciones técnicas y de seguridad antes apuntadas en el Art. 2 Incisos B), E), I) y J). Los mismos exceden el ámbito del presente análisis, razón por la cual se omitirá adentrar en su exposición.

Articulo 2º: Registro y sistematización de datos de tráfico

Incorpórase el artículo 45 ter a la Ley 19.798 con el siguiente texto: "Los prestadores de servicios de telecomunicaciones deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años."

Sin lugar a dudas el hecho de almacenar datos referentes a las telecomunicaciones puede generar cuestionamientos y en cierta manera recelo y hasta temor por parte de los usuarios. Cierta sensación de vigilancia puede ocupar a la persona al saber que es almacenada información relativa a sus comunicaciones. Resulta necesario desentrañar ciertos aspectos de la cuestión para que exista un real entendimiento de la misma. En primer lugar el análisis de la realidad normativa extranjera sobre la cuestión; en segundo, el examen de los datos objeto de almacenamiento por los prestadores; y como tercer punto, el plazo de guarda de los mismos y su consecuente costo.

1.- Derecho Comparado

Estado Unidos

En el año 1994 fue aprobada la *"Communications Assistance for Law Enforcement Act"*, dirigida a las empresas de telecomunicaciones, a las que se obligó a prestar una serie de colaboraciones a los fines de aislar e interceptar datos de tráfico y contenido de comunicaciones telefónicas, siempre que existiera orden judicial. Asimismo es de señalar que la misma no era de aplicación a los Proveedores de Servicio de Internet.
En virtud de los atentados del 11 de Septiembre de 2001, el Congreso de Estados Unidos aprobó la H.R.3162, llamada Acta Patriótica, el 24 de octubre de 2001. La misma otorga amplios poderes especiales al FBI y a las agencias de inteligencia nacional para poder monitorear el tráfico de correo electrónico

España:

El articulo 12 de la ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico del 11 de julio de 2002 establece que los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicio de alojamiento de datos deberán retener los datos de conexión y trafico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de información por un periodo máximo de doce meses.
Se instituye allí que los referidos datos serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario de la transmisión de la información y que los prestadores de servicio de alojamiento de datos deberán retener solo aquellos imprescindibles para identificar el origen de los datos alojados y el momento en que se inicio la prestación del servicio, señalándose que en ningún caso la obligación de retención de datos afectara el secreto de las comunicaciones.
Asimismo, se dispone que los datos, se conservaran para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y defensa nacional, poniéndose a disposición de los jueces o tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerza y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.
Se ha justificado esta normativa española en el texto de la Directiva 97/66/CE[44] y la Propuesta de Directiva de la UE relativa al tratamiento de datos personales y a la protección de la

[44] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Diario Oficial N° L 024 de 30/01/1998 P.0001 – 0008.

intimidad en el sector de las comunicaciones electrónicas en donde se "faculta a los estados para estableces excepciones a las normas de destrucción de datos de trafico (…) para proteger la seguridad y defensa nacional".[45]

Inglaterra

Pese a una gran oposición de numerosas organizaciones, fue aprobada la normativa titulada "*The Regulations of Investigatory Powers"*, de aplicación a los proveedores de servicio de Internet. En su Parte I - Capitulo II (Acquisition and Disclosure of Comunnication Data) obliga a retener datos de tráfico de todo tipo de telecomunicaciones. La Parte III de la norma inglesa obliga a los proveedores que utilizan algún tipo de encriptado a entregar a pedido oficial las claves del mismo para poder acceder a la comunicación codificada.
La retención de datos de tráfico se justifica por: Los intereses de la seguridad nacional; La prevención e investigación de crímenes y la prevención de desordenes; Los intereses económicos del Reino Unido; Recaudar todo impuesto, tasa, contribución o cualquier tipo de obligación impositiva: Prevenir cualquier tipo de daño o injuria a una persona, o para mitigar los efectos de los mismos; O para cualquier otro propósito.
La *Anti-Terrorism Crime and Security Act* del año 2001, en su Parte 11, también prevé la retención de datos de comunicaciones. La misma fue sancionada en términos de protección de la seguridad nacional y la lucha contra el delito. La norma se funda sobre la base de un Código de práctica de retención, instrumentado por la Secretaria de Estado, el denominado *"Home Office Voluntary Code of Practice. Retention of Comunication data under Part 11: Anti-terrorism, Crime & Security Act 2001"*. En el mismo se establecen las obligaciones de los prestadores, la información a retener y los periodos de guarda.

Italia

El Código de protección de datos personales (Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, Nro. 196), dispone en su artículo 132 la conservación de los datos de tráfico de comunicaciones. Establece que deberán ser conservados los datos relativos a las comunicaciones telefónicas, aun cuando la comunicación no haya tenido respuesta por el destinatario, por un periodo de 24 meses y con la finalidad de luchar contra el delito. Con respecto al "traffico telemático" la obligación se fija por un periodo de 6 meses.
El Decreto 144/2005 de "Misure urgente per il contrasto del terrorismo internazionale", del 27 de Julio de 2005, regula en sus artículos 6 y 7 nuevas normas para los datos de tráfico de comunicaciones. Suspende a partir de su entrada en vigencia, todas las disposiciones que

[45] Fernández Delpech, Ob.Cit., p.213

consienten la eliminación de datos de tráfico de comunicaciones, determinando que la información almacenada deberá conservarse hasta el 31 de diciembre de 2007.

Regulación de datos de tráfico en la Unión Europea:

Directiva 2002/58/CE

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, fue sancionada con la finalidad de derogar y sustituir la Directiva 97/66/CE a fin de adaptar la normativa europea al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas disponibles al público sea el mismo, con independencia de las tecnologías utilizadas.[46]

La Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea. Específicamente hace alusión a los derechos enunciados en los artículos 7 y 8 de dicha Carta[47] y a la confidencialidad de las comunicaciones, de conformidad con los instrumentos internacionales relativos a los derechos humanos, especialmente el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y las constituciones de los Estados miembros.

En su artículo 2 inc B) define a los datos de tráfico como “cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma”. La definición aparece vaga y poco delimitada. En el considerando 15 de la Directiva podemos leer: “Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una

[46] De acuerdo con lo establecido en los Tratados de Roma, una directiva es una decisión colectiva obligatoria aprobada por los Estados miembros. Obliga a todos o parte de los Estados miembros en cuanto al objetivo a alcanzar, pero les permite elegir la forma y los medios para conseguir tales objetivos. Las directivas, no son de aplicabilidad directa en los ordenamientos jurídicos internos, sino que obligan a los Estados a aplicar una serie de medidas, lo cual conllevará a una transposición de las mismas al Derecho nacional de cada uno.

[47] **Art.7.-** Respeto de la vida privada y familiar: “Toda persona tiene derecho a la protección de su vida privada y familiar, de su domicilio y de sus comunicaciones”. **Art. 8.1.-** Protección de los datos de carácter personal: “Toda persona tiene derecho a la protección de sus datos de carácter personal que la conciernan. **2.-**Estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. **3.-** El respeto de estas normas quedara sujeto al control de una autoridad independiente.”

comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación." Su tono es más bien ejemplificativo y no termina de demarcar concretamente y con exactitud a que datos se hace referencia.

Por su parte el Artículo 5 inc.1 establece la garantía de confidencialidad de los datos de trafico, prohibiendo el almacenamiento, intervención o vigilancia de los mismos, salvo el almacenamiento técnico necesario para la conducción de la comunicación o que exista autorización en virtud del apartado 1 del articulo 15.[48]

En el mismo sentido el Art. 6.1 fija el deber de eliminar o hacer anónimos dichos datos cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, sin perjuicio de la posibilidad de tratarlos para la facturación de los abonados (inc 2.), para la promoción comercial de servicios siempre y cuando el usuario haya dado su consentimiento (inc 3), y la detección de fraudes (inc 5).

Finalmente, el ya mencionado articulo 15.1, determina la posibilidad a modo de excepción, de efectuar la retención de datos de trafico, cumplimentando una serie de garantías y con una finalidad limitada a la seguridad nacional: El mismo establece: "Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8[49] y en el artículo 9[50] de la presente Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva

---

[48] **Art. 5.-** Confidencialidad de las comunicaciones **1.-** Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.

[49] **Art.8.-** Presentación y restricción de la identificación de la línea de origen y de la línea conectada

[50] **Art.9.-** Datos de localización distintos de los datos de tráfico.

95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea."

Directiva 2006/24/CE

La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, fue sancionada con el objeto de modificar la Directiva 2002/58/CE. Su finalidad puede encontrarse en la lucha contra el terrorismo y el crimen organizado[51], dado que se considera que la conservación de datos resulta un elemento crucial para tal objetivo. Igualmente, responde a la necesidad de adoptar disposiciones armonizadoras a nivel de la UE sobre retención de datos.[52]

Así, en su artículo 1° punto 1 es posible leer: "La presente directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación,

[51] Considerando: **7.-** Las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 destacan que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada. **8.-** La Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004, encargó al Consejo que examinara medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones. **10.-** El 13 de julio de 2005, el Consejo reafirmó en su declaración de condena de los atentados terroristas de Londres la necesidad de adoptar cuanto antes medidas comunes sobre conservación de datos de telecomunicaciones.

[52] Considerando: **5.-** Varios Estados miembros han adoptado legislación que prevé la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos. Estas disposiciones de las normativas nacionales varían considerablemente. **6.-** Las diferencias legales y técnicas entre disposiciones nacionales sobre conservación de datos con fines de prevención, investigación, detección y enjuiciamiento de delitos crean obstáculos en el mercado interior de las comunicaciones electrónicas; los prestadores de servicios deben cumplir requisitos diferentes en cuanto a los tipos de datos de tráfico y de localización que deben conservarse, así como en cuanto a las condiciones y los períodos de conservación.

detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro."

El punto 2, dictamina que la presente Directiva será de aplicación a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No siendo aplicada al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas. Por tanto, esta obligación de conservación de los datos configura una excepción a los arts. 5, 6 y 9 de la Directiva 2002/58/CE.[53]

El objeto de conservación viene dado por el artículo 2.2 en el cual se establece que los datos que son objeto de conservación son los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o al usuario registrado. A su vez el artículo 5 establece en forma detallada las categorías de datos que deben conservarse, estableciéndose que serán los datos necesarios para: 1) rastrear e identificar el origen de una comunicación; 2) identificar el destino de una comunicación; 3) identificar la fecha, hora y duración de una comunicación; 4) identificar el tipo de comunicación; 5) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; 6) identificar la localización del equipo de comunicación móvil. Dentro de cada de uno de los subgrupos de datos, se hace referencia precisa a su significado con respecto a la telefonía fija y móvil, acceso a Internet, Correo Electrónico y telefonía por Internet.

Con respecto al periodo de conservación de los datos, el artículo 5 regla que será por un periodo de tiempo que no sea inferior a 6 meses ni superior a 2 años a partir de la fecha de la comunicación. Llamativamente no se distingue al establecer dichos plazos, entre los diferentes tipos de datos.

El artículo 7 determina que los Estados miembros velarán por que los proveedores de servicios de comunicaciones cumplan en lo que respecta a la conservación de datos con la Directiva, y pauta una serie de principios mínimos en materia de seguridad de los datos.

Por su parte el Art. 9 instruye la necesidad de que los Estados miembros nombren una autoridad pública responsable de controlar la aplicación de la Directiva en relación con la seguridad de los datos conservados. Dichas autoridades, que actuarán con plena independencia, pueden ser las Agencias de protección de datos ya existentes en virtud del artículo 28 de la Directiva 95/46/CE.[54]

---

[53] **Art. 3.1-**Obligación de conservar datos. Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.

[54] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Directiva entró en vigor el 3 de mayo del 2006, previendo su artículo 15.1 que deberá transponerse por los Estados miembros a más tardar el 15 de septiembre de 2007. En virtud del punto 3 del citado artículo se faculta a los Estados miembros a decidir, en el momento de adopción de la Directiva, aplazar hasta el 15 de marzo de 2009 la aplicación de la misma en lo que se refiere a la conservación de los datos de comunicaciones a través de Internet (acceso a Internet, telefonía por Internet y el correo electrónico). Han optado por tal posibilidad Alemania, Bélgica, Austria, Chipre, Eslovenia, Estonia, Finlandia, Grecia, Letonia, Lituania, Luxemburgo, los Países Bajos, Polonia, República Checa, el Reino Unido y Suecia

Críticas formuladas al texto de la Directiva 2006/24/CE

La aprobación de la Directiva 2006/24/CE ha sido enérgicamente criticada desde de su mismo proyecto[55]. Dichas reprobaciones vinieron por parte del Comité Económico y Social, del Parlamento, del Grupo de trabajo del Artículo 29[56] y del Supervisor Europeo de Protección de Datos, siendo el principal argumento de objeción a la Propuesta el considerar que no se amparaban suficientemente los Derechos fundamentales en juego.

El 26 de septiembre de 2005, el Supervisor Europeo de Protección de Datos (SEPD) aprobó su Dictamen sobre la propuesta de directiva del parlamento y del Consejo. [57]
En dicha ocasión manifestó que reconoce la importancia que tiene para los servicios policiales de los Estados miembros contar con todos los instrumentos jurídicos necesarios, en especial en la lucha contra el terrorismo y otros tipos de delincuencia grave. Asimismo, sostuvo que una disponibilidad adecuada de determinados datos de tráfico y de localización de los servicios electrónicos públicos puede ser un instrumento decisivo para dichos servicios policiales y puede contribuir a la seguridad física de las personas. Pero al mismo tiempo, teniendo en consideración el evidente impacto que la normativa tendría en la protección de datos personales, sostuvo cierta falta de convencimiento sobre la necesidad y proporcionalidad de la medida. Consideró que la misma requería de un análisis completo a fin de establecer mayores salvaguardias y que una simple referencia al marco jurídico vigente en relación con la

[55] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE. (SEC (2005) 1131). Bruselas, 21/9/2005, COM (2005) 438 final 2005/0182 (COD).

[56] Grupo creado en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

[57] Dictamen del Supervisor Europeo de Protección de Datos, adoptado el 26 de septiembre de 2005 (2005/C 298/01), sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE.

protección de datos no es suficiente. En síntesis, el SEPD reconoció que las circunstancias cambian, pero que en dicho momento no estaba convencido de la necesidad de la retención de datos de tráfico y de localización a efectos policiales, según lo establecido en la propuesta.

Por su parte, el Grupo del Artículo 29 en su Dictamen sobre la Propuesta de Directiva adoptado el 21 de octubre de 2005, declaró en primer lugar que los enfrentaba a una decisión histórica.[58] En una línea similar a la del SEPD, indicó que el terrorismo plantea a nuestra sociedad un desafío real y apremiante, debiendo los Gobiernos responder a este desafío de una manera que responda con eficacia a la necesidad de sus ciudadanos de vivir en paz y seguridad, sin socavar sus derechos humanos individuales, incluido el derecho a la confidencialidad de los datos, que constituyen una piedra angular de nuestra sociedad democrática.
Demandó que la justificación para la conservación obligatoria y general de los datos debe demostrarse claramente y apoyarse con pruebas y que las finalidades de la conservación de datos deben exponerse claramente en la Directiva en el contexto de la lucha contra el terrorismo y la delincuencia organizada, en vez de contra los "delitos graves" indeterminados.
Como punto final, bajo el titulo de “Otras garantías específicas”, el Grupo indicó veinte cuestiones que debían necesariamente abordarse, prestando especial atención a los requisitos aplicables a los destinatarios y al tratamiento posterior de los datos, a la importancia de las autorizaciones y controles, a las medidas aplicables a los prestadores de servicios también en términos de seguridad y de separación lógica de los datos, a la determinación de las categorías de datos en cuestión y su actualización, y a la necesidad de excluir datos relativos al contenido.

El 19 de enero 2006, el Comité Económico y Social Europeo (CESE) aprobó su dictamen relativo a la Propuesta con noventa y dos votos a favor, diecisiete en contra y diecisiete abstenciones[59]. En el punto 1.1 manifestó su extrañeza y preocupación por la presentación de una propuesta de normativa de tal índole, considerando su contenido desproporcionado y atentatorio de lo derechos fundamentales. Del mismo modo denunció que el tratamiento dado a los derechos humanos, especialmente al derecho a la intimidad, no era realizado adecuadamente, pudiendo colisionar en determinados aspectos.
En otro orden de ideas, apuntó que se corre el riesgo de socavar la confianza de los usuarios de las comunicaciones electrónicas y disminuir su disposición a utilizar las TIC (tecnologías de

[58] Dictamen 4/2005, adoptado el 21 de octubre de 2005 (1868/05/ES. WP 113), sobre la Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE.

[59] Dictamen del Comité Económico y Social Europeo, de 19 de enero 2006, sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE.

la información y la comunicación), implicando el riesgo de que el futuro desarrollo de la sociedad de la información se vea frenado a largo plazo.
El CESE concluyó y recomendó la necesidad de revisar sustancialmente la propuesta por considerar que la misma no respetaba en su totalidad los derechos fundamentales, ni las reglas de acceso, uso o intercambio de los datos.

Finalmente, El 25 de marzo 2006, con posterioridad a la aprobación de la Directiva, el Grupo del Artículo 29 emitió el Dictamen 3/2006[60]. En el mismo, dicho grupo declaró que las consideraciones y las preocupaciones recogidas en el Dictamen emitido anteriormente mantenían toda su validez., siendo de suma importancia que la Directiva vaya acompañada y sea aplicada en cada Estado miembro a través de medidas destinadas a limitar el impacto sobre la intimidad.
Consideró que para transponer las disposiciones de la Directiva de una manera uniforme y cumplir con los requisitos del artículo 8 del Convenio europeo sobre derechos humanos[61], los Estados miembros deberían aplicar una serie de garantías adecuadas y específicas, tales como: Especificación de propósito, limitación de acceso, minimización de los datos y medidas de seguridad, entre otras.

En breves líneas y sin perjuicio de las mayores precisiones que se efectuaran a continuación, es de señalar que se sostiene que la redacción de la Directiva contiene una serie de imprecisiones que la hacen criticable: indeterminación de los delitos que permitirán usar los datos, insuficiencia de las medidas de seguridad establecidas, indefinición del procedimiento para tener acceso a los datos y finalmente, silencio respecto a quién soportará los costos que significan las medidas a adoptar.

Delitos

Con respecto a la determinación de los delitos que son abarcados en el ámbito de la directiva, es motivo de crítica la incertidumbre presente en el texto definitivo de la misma, en

[60] Dictamen 3/2006, adoptado el 25 de marzo de 2006 (654/06/ES. WP 119) sobre la Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, adoptada por el Consejo el 21 de febrero de 2006.

[61] **Art.8.** Derecho al respeto a la vida privada y familiar. **1.** Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. **2.** No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

contradicción con lo que acontecía en la Propuesta. El Art. 1.1. de la Propuesta de Directiva al hacer referencia a "delitos graves" especificaba el terrorismo y la delincuencia organizada.
En el mismo sentido, el Grupo del Artículo 29 señaló que "los datos sólo deberán conservarse con el fin específico de luchar contra el terrorismo y la delincuencia organizada, en vez de considerarse cualesquiera otras infracciones graves indeterminadas."[62]
En este punto, y en paralelo con la crítica que se hace a la indeterminación de los delitos, es necesario e ineludible señalar otra de las más importantes objeciones planteadas al texto de la Directiva. Se sostiene que las medidas adoptadas son excesivamente vulneradoras de los derechos fundamentales de los ciudadanos, y que en la actualidad existen otros medios técnicos que satisfacen la misma finalidad y de una manera considerada menos invasora.
En esta línea planteada, se hace referencia al denominado *Quick freeze*[63], sistema en el cual el almacenamiento de *data* no es generalizado, sino que responde a casos determinados y justificados por solicitud de las autoridades policiales. El acceso a los datos almacenados de conformidad con la solicitud, solo podrá efectuarse mediante orden judicial emitida a tal respecto.

Acceso a los datos

Como ha sido dicho, el artículo 4 de la Directiva determina que los datos conservados solamente serán proporcionados a las autoridades nacionales competentes, agregando que solo procederá en casos específicos y de conformidad con la legislación nacional.
El reproche del que ha sido objeto la Directiva en este punto, se refiere a la excesiva generalidad del término "autoridades nacionales competentes". Es opinión del SEPD y del Grupo del Artículo 29 la forzosa necesidad de que las legislaciones nacionales oportunamente dictadas en virtud de la transposición de la Directiva, identifiquen en forma manifiesta cuáles serán las autoridades legitimadas para acceder a los datos.
El Grupo del Artículo 29 (WP 113) especificó que el acceso a los datos deberá, en principio, autorizarse debidamente en cada caso por una autoridad judicial, sin perjuicio de los países donde exista la posibilidad específica de acceso autorizado por ley, bajo supervisión independiente. En su caso, las autorizaciones deberán especificar los datos particulares requeridos para los casos concretos. De igual forma marco la necesidad de registrar todo acceso a los datos.
El SEPD en su dictamen (2005/C 298/01), indicó serias previsiones a tener en cuenta en referencia al acceso a los datos: La imposibilidad de accesos a fines de prospección de datos o de operaciones de búsqueda aleatoria de información y la necesidad de regular en forma clara

[62] Grupo sobre protección de datos del Art. 29, WP 113, p.9.

[63] Procedimiento considerado por el Grupo del Artículo 29 (WP 113, p. 7).

el intercambio de datos con las autoridades de otros Estados miembros (Punto 32); la insuficiencia de precisión de las limitaciones para el acceso y la utilización posterior de los datos, siendo necesarias salvaguardias adicionales (Punto 50); La necesidad de añadir una disposición en el texto, para asegurar que los individuos distintos de las autoridades competentes no tengan acceso a los datos (Punto 52); especificar en debida forma que los datos sólo pueden proporcionarse cuando sea necesario en relación con una infracción penal concreta (Punto 53); establecer que el acceso en casos específicos deberá estar supeditado al control judicial en los Estados miembros (Punto 56).

Por su parte, el Dictamen del CESE (2006/C 69/04) señaló en la misma dirección, que no resultaban previstas normas que impidan un eventual acceso de los proveedores y otros interesados a los datos almacenados, debiéndose prever que todo acceso a dichos datos deberá realizarse, solo en casos específicos y bajo control judicial. (Punto 2.4.9)

A pesar de las consideraciones recibidas, el texto definitivo de la Directiva simplemente recibió el agregado de un párrafo en su articulo 4, que establece que cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del derecho de la Unión o del derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos.

Plazo de conservación

La Directiva en su Art. 6 establece una guarda de los datos por un periodo de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación, sin realizar distinciones entre las diferentes categorías de datos. Contrariamente a lo señalado, el Art. 7 de la Propuesta establecía un plazo general de un año de conservación y con respecto a los datos que tengan lugar entera o principalmente a través del protocolo de Internet, de seis meses.

El Dictamen del CESE consideró que el plazo de un año previsto en la Propuesta resultaba demasiado largo, ya que la Comisión no acreditaba suficientemente la necesidad de retención por esos periodos. Señaló como prudencial un plazo unificado de seis meses, con las medidas de seguridad y confidencialidad adecuadas (Punto 2.4.8).

Costos

El artículo 10 de la Propuesta, expresamente establecía que los Estados miembros asegurarían que los proveedores de servicios de comunicación electrónica de acceso público o de una red

de comunicaciones pública, serían reembolsados por los costes adicionales en que demuestren haber incurrido para cumplir con las obligaciones que la Directiva les imponía.

El SEPD marcó que una normativa adecuada debe contener incentivos para que los proveedores inviertan en la infraestructura técnica, hablándose de una indemnización. (Punto 36).

El Grupo del Artículo 29 observó que los gastos adicionales que soporten los proveedores de comunicaciones electrónicas deberían ser compensados por los Estados miembros. Subrayando la importancia de la cuestión en virtud de tener una relación directa con el nivel de protección de los datos como en la esfera económica de los ciudadanos, a los que podrían cargarse parte de los gastos de los proveedores (WP 113, p.11-12).

En discrepancia con lo hasta aquí planteado, el Comité Económico y Social se manifestó sorprendido por el hecho de regular la Propuesta los “costos adicionales” en su articulo 10. Sostuvo que dichos costos deberían contemplarse como una carga que a los operadores correspondía asumir por el mero hecho de estar en el mercado sin que el erario público, y por ende todos los ciudadanos, tengan que soportarla (Puntos 2.4.11 - 2.4.14).

Finalmente, en el texto definitivo adoptado, la problemática de la carga de los costos no recibe respuesta alguna, debido a que se omitió realizar todo tipo de referencia a la cuestión. Por lo tanto es factible interpretar que ante el silencio de la Directiva, corresponderá a los Estados a la hora de trasladar la normativa a sus legislaciones, establecer individualmente que medidas adoptaran con respecto a la cuestión de la asunción de la inversión.

Es de destacar que la razón que determinó la sanción de la Directiva, fue la idea de lograr la armonización de las normativas de países europeos ya sancionadas en materia de retención de datos de tráfico. Por tal motivo, resulta llamativo que una cuestión trascendental como es la determinación de la repartición de los costos de implementación y funcionamiento del sistema, haya sido dejada al arbitrio de cada país.

Medidas futuras

El artículo 12 de la Directiva, bajo el titulo “medidas futuras”, ha dado lugar a una significativa preocupación. Su texto establece que “Todo Estado miembro que deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6 podrá adoptar las medidas que se impongan. El Estado miembro en cuestión informará inmediatamente a la Comisión y a los demás Estados miembros sobre las medidas adoptadas de conformidad con el presente artículo e indicará las razones que le llevan a adoptarlas.”(Art. 12.1). Agregando el punto 2, que “en un plazo de seis meses tras la notificación, la Comisión aprobará o rechazará las medidas nacionales en cuestión después de haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el

funcionamiento del mercado interior. En caso de que la Comisión no adopte ninguna decisión en dicho plazo se considerará que las medidas nacionales han sido aprobadas."
De acuerdo a lo normado, se confieren a los Estados ciertas facultades permisivas de traspasar los límites impuestos por la Directiva. El cuestionamiento surge en torno a la falta de precisión de la redacción en cuanto a cual es el momento desde el cual son ejecutivas las modificaciones realizadas, si desde el momento mismo de sanción de las mismas o por el contrario con posterioridad a su aprobación (positiva o por omisión).
Asimismo, la utilización del precepto "circunstancias especiales" es demasiado amplio y podría dar lugar a abusos por parte de los gobiernos nacionales.

2.- Datos objeto de almacenamiento

En el artículo 2° de la ley 25.873 se establece, como ha sido dicho, el deber de almacenamiento de los datos de tráfico de las comunicaciones cursadas y de los datos filiatorios y domiciliarios de los clientes y usuarios. Con respecto a la obligación de almacenamiento de los datos filiatorios y domiciliarios, es muy posible que la misma encuentre problemas de aplicación por diversos factores. En la realidad comercial actual, a nivel telefonía celular existe la posibilidad de adquirir "Chips" telefónicos en el mercado por sumas muy bajas y en forma totalmente anónima. Por lo tanto, una persona propietaria de un solo equipo celular, podría adquirir varios de los aludidos chips, utilizándolos para hacer un par de llamados, y luego cambiarlo, obteniendo de esta manera un nuevo número. Por tanto, la data almacenada en referencia a los llamados realizados sería de ningún valor, por no existir una real e inconmovible vinculación de la línea con un titular. Con respecto a las comunicaciones cursadas por Internet, es factible señalar dos factores que pueden perjudicar la medida de retención. Por un lado la gran cantidad de Cybers que brindan acceso al público en general a Internet y por otro lado la tecnología de Internet inalámbrico (Wi-Fi). Mediante la misma, cualquier persona con una computadora portátil (Notebook), puede ingresar a Internet, sin identificarse, simplemente estando dentro de la zona de cobertura del servidor Wi-Fi. El mismo esta disponible en gran cantidad de universidades, locales comerciales, bancos, oficinas, etc. En ciertos casos siquiera es requisito entrar a tales establecimientos, debido a que la zona de cobertura excede los límites de la edificación, pudiendo accederse por ejemplo desde el banco de una plaza cercana.
Con respecto a los datos de tráfico, la ley no contiene, lo cual es preocupante, definición de que debe entenderse por ellos.
La Resolución 40/2004 de la Secretaria de Comunicaciones clarifica un poco la cuestión. La misma fue sancionada con anterioridad al decreto 1563/04, razón por la cual en su texto instituye "que, sin perjuicio de lo que oportunamente establezca el Poder Ejecutivo en relación con la propuesta legislativa aprobada en fecha 17 de diciembre de 2003 (Ley 25.873), resulta

procedente establecer una inmediata tutela sobre los mencionados registros.” El articulo 3 de la resolución define a la información asociada como toda aquella que permita individualizar el origen y destino de las telecomunicaciones, tales como registros de tráfico, identificación y ubicación del equipo utilizado y todo otro elemento que permita establecer técnicamente su existencia y características.
Finalmente, cuando fue sancionado el decreto reglamentario 1563/04, el panorama no resulto ser mucho más alentador. Su Art. 3º punto A) menciona la ubicación geográfica del abonado; mientras que el punto D) hace referencia a “la demás información asociada a las telecomunicaciones”.

Muy diferente es la realidad europea, en la cual mediante la Directiva ya vista, se dispone que los datos objeto de conservación son los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o al usuario registrado. El artículo 5 se encarga de establecer en forma detallada las categorías de datos que deben conservarse, instituyéndose que serán los datos necesarios para: 1) rastrear e identificar el origen de una comunicación; 2) identificar el destino de una comunicación; 3) identificar la fecha, hora y duración de una comunicación; 4) identificar el tipo de comunicación; 5) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; 6) identificar la localización del equipo de comunicación móvil. Conjuntamente, dentro de cada de uno de los subgrupos de datos, se hace referencia precisa a su significado con respecto a la telefonía fija y móvil, acceso a Internet, Correo Electrónico y telefonía por Internet.

Una cuestión que llama la atención en la antes mencionada resolución 40/2004 de la Secretaría de Comunicaciones, es lo dispuesto en su Art. 1. Textualmente reza que “los Prestadores de Servicios de Telefonía Local, Larga Distancia Nacional e Internacional, del Servicio de Radiocomunicaciones Móviles (SRMC), del Servicio de Telefonía Móvil (STM), del Servicio de Comunicaciones Personales (PCS) y del Servicio Radioeléctrico de Concentración de Enlaces (SRCE), deberán tomar los recaudos necesarios para conservar inalterados los datos filiatorios de sus clientes y registros de tráfico de telecomunicaciones existentes desde el 1º de enero de 1989.”
La resolución sobrepasa lo establecido por la ley 25.873 y añade que los prestadores deberán tomar los recaudos necesarios para conservar inalterados los datos filiatorios de sus clientes y registros de tráfico de telecomunicaciones existentes desde el 1° de enero de 1989. La obligación podría resultar de cumplimiento imposible, ya que lo mas probable es que los prestadores no cuenten con dichos datos almacenados, en virtud de no existir una obligación semejante, por lo que los prestadores simplemente se limitaban (y lo siguen haciendo), a

almacenar la información necesaria para la facturación de sus servicios[64]. La resolución 40/2004 excede injustificadamente lo normado por la ley 25.873 y es de señalar que su redacción no fue concebida en el texto del decreto 1563/04 suspendido.

3.- Periodo de guarda y su consecuente costo

La normativa argentina en análisis, prevé que el almacenamiento de la *data* debe realizarse por un plazo de 10 años, muy superior al reglamentado en otros países como ha sido visto.
La implementación de un sistema informático capaz de almacenar tal cantidad de datos requiere una gran inversión. A grandes rasgos es posible intentar un cálculo aproximativo de la misma.
En primer lugar, es necesario soporte físico de almacenamiento (Discos Rígidos). En informática la unidad de medida de datos que se utiliza es el Byte. Un Byte esta compuesto por 8 bits, y es la unidad mínima de almacenamiento, con la cual se representa un caracter (v.gr A, B, 1, etc). 1024 Bytes constituyen un Kilobyte, el cual generalmente se abrevia como KB. Las PC de IBM más antiguas, por ejemplo, tenían una capacidad máxima de 640 KB, alrededor de 640 000 caracteres de datos. A su vez, 1024 KB constituyen un Megabyte (MB), la cual es la unidad más típica actualmente, usándose para especificar la capacidad de la memoria RAM, de las memorias de tarjetas gráficas, de los CD-ROM, o el tamaño de los programas y de archivos grandes. A la hora de hablar de Discos Rígidos, la misma ya ha quedado obsoleta, siendo lo habitual hablar de Gigabytes (GB), el cual esta formado por 1024 MB. Finalmente, y aclarando que existen unidades mayores pero que superan lo necesario para el presente desarrollo, está el Terabyte (TB), su nombre viene del griego τέρας, que significa monstruo. Un TB es equivalente a 1024 Gigabytes.

Teniendo ya en claro como se maneja en informática las unidades que marcan el almacenamiento de la información, es necesario analizar que capacidad se necesita a la hora de registrar los datos de comunicación.
De la lectura conjunta de las normativas extranjeras, surge que la data almacenada consiste en identificación del origen, identificación del destinatario, fecha, hora y duración de la comunicación y el dispositivo utilizado. Lo cual se traduce en una llamada telefónica en: El número de teléfono de quien disca, el número de teléfono del destinatario de la llamada, la fecha en la cual se realizo y su duración. Lo mismo con respecto a los SMS. A nivel Internet

[64] La técnica se conoce como “recuento” (en inglés “comptage” o “pen register”), y consiste en el empleo de un mecanismo que registra los números marcados desde un determinado aparato telefónico, la fecha, hora y duración de la llamada. Se sostiene que no existe obstáculo legal a que tales registros sean llevados por los prestadores en virtud de responder a una necesidad de asegurar la exactitud de los importes facturados, como así también el resguardo contra quejas por el servicio.

consiste en: IP asignado a la persona en el momento de conexión, IP al cual se conecto, fecha, hora y duración de la conexión.
Tal información, la cual seria asentada en una “línea”, requiere una capacidad que podemos considerar satisfecha con 1 KB por línea.

En el plano de las comunicaciones telefónicas el problema del costo de almacenamiento de la *data* no se vislumbra con tanta gravedad como en Internet, pero también es considerable, sobre todo en el plano de las comunicaciones móviles.
En junio de 2003 existían 8.693.700 líneas de telefonía básica instaladas en la Argentina. En el mismo mes había 6.762.000 teléfonos celulares en servicio según datos aportados por la Comisión Nacional de Comunicaciones. Ya en el año 2005, el parque de líneas de telefonía celular superó las líneas fijas al llegar a los 13,5 millones - aunque este número se reduciría a unos 11 millones, si se restan líneas que no están en uso, pero no fueron dadas de baja -, según la firma Prince & Cooke.
Paralelamente con el incremento de las líneas de telefónica celular, se incrementó el envío de mensajes de texto (SMS). Según datos de la consultora Convergencia Research, en octubre de 2005 se transmitieron 400 millones de SMS, contra los 20.000 mensajes mensuales en 2002. A finales del año 2006, de acuerdo a datos revelados por un estudio de la consultora Prince & Cook, se enviaban un promedio de 5.300 millones de SMS por mes.
Según datos publicados por el Diario La Nación en su suplemento Tecnología el 22 de Enero del 2007, el Instituto Nacional de Estadística y Censos (Indec), informó que en el país hay 30 millones de líneas de teléfonos móviles, duplicándose de esta manera la cantidad de líneas con respecto al 2005. Al mismo tiempo, la cantidad de líneas fijas se mantiene estable (8,6 millones) aumentado el uso de VoIP. Según Prince&Cooke, el 22% de los navegantes locales usa algún servicio de telefonía IP.

A pesar de los números recién vistos, es claro que una persona promedio realiza un número acotado de llamados diarios y envíos de SMS en relación con las “comunicaciones” que se realizan online. Cuando el usuario se conecta con el servidor le es asignado un numero IP, el cual quedaría registrado en la base de datos de tal usuario, a fin de a continuación almacenarse los datos de trafico cursados durante ducha conexión. Durante la navegación es común revisar la cuenta de correo electrónico, acceder a páginas Web y desarrollar charlas a través de programas de mensajería instantánea, y todo al mismo tiempo. Cada una de estas acciones del usuario, significan una línea de datos que es almacenada.
A fin de realizar un cálculo estimativo de costos, consideremos que cada usuario por día de navegación realiza entre todas las acciones antedichas, una total de 100 “comunicaciones”, las cuales se traducen en 100 KB. Ahora debemos determinar la cantidad de usuarios.

En el año 2003, existían 918.000 usuarios con acceso propio a Internet en Argentina. 714.877 cuentas eran de tipo dial up (el 78% de las cuentas totales). El resto (202.568) que significan el 22%, eran de banda ancha. De éstas, casi 121 mil accesos ADSL; 73 mil correspondían a cablemodem y el resto a Internet inalámbrico y accesos compartidos.
En el año 2005, fueron vendidas 684.483 computadoras, muy por encima de las 425.986 unidades de 2003. La banda ancha, por su parte, registró cerca de 500.000 accesos en uso, según Carrier y Asociados. A lo cual hay que sumarle otros 6 a 8 millones de navegantes argentinos, dependiendo de las fuentes.
Durante el año 2006 se vendieron 1,3 millones de PC, según un estudio de la consultora Trends Consulting. Esto es un 27,8% más que en 2005. Según Carrier y Asociados, las ventas llegaron a 1,5 millones de equipos. Diferencias de medición aparte, dan cuerpo a un parque instalado de equipos que ronda los 6 millones de PC, según cálculos de la consultora Prince & Cooke.
En el caso específico de Internet, la banda ancha siguió sumando usuarios. Según Carrier y Asociados, hay aproximadamente 1,5 millones de accesos de este tipo en el país, de los cuales el 88% está en los hogares. Siendo el 62% del total por ADSL. Esto coincide con los cálculos de Prince& Cooke, que supone 1,59 millones de conexiones de banda ancha. Esta consultora, sin embargo afirma que hay 13 millones de usuarios de Internet en el país, contra los 10,5 millones que calcula Carrier.

Retomando el cálculo y partiendo de la base de los 100 KB de almacenamiento que en suposición significarían la navegación de un usuario, se traducirían en un mes de navegación en un total de 3.000 KB, es decir 2,93 MB. Por tanto en un año, su nivel de ocupación en el sistema de almacenamiento de datos de tráfico instalado por el servidor, seria de 35,16 MB. Este número es pequeño, pero teniendo en cuenta los 10 años de almacenamiento que se preveían en la ley 25.873 y los 13 millones de usuarios de Internet existentes en Argentina, nos da un total de 4.570.800.000 MB, los cuales constituyen 4359 Terabytes. En pocas palabras, una tonelada de información.
Esa inmensidad de data, la cual requiere una gran cantidad de unidades de almacenamiento, conlleva consecuentemente un gran costo de inversión. Un disco rígido de tocología SCSI[65], la cual es utilizada en este tipo de tareas, con una capacidad de 146 GB, tiene un costo de alrededor de 800 dólares dependiendo del fabricante. Por tanto, para poder soportar la cantidad de información producida por el trafico de comunicaciones, solo a nivel Internet, serian necesarias 30.573 unidades de almacenamiento de este tipo, significando alrededor de 73 millones y medio de pesos.

[65] ***S**mall **C**omputer **S**ystem **I**nterface*, es una interfaz estándar para la transferencia de datos entre distintos dispositivos del bus de la computadora.

Pero la cuestión no encuentra punto final en ese gasto, los discos rígidos, organizados en Raids[66], necesitarían placas controladoras para su comunicación con el "ordenador", asimismo el sistema estaría constituido por procesadores, cableados, sistemas de refrigeración, Racks[67] donde asentar el hardware y posiblemente dispositivos de caching[68]. Con lo cual es claro que la inversión no solo se limita al soporte físico necesario en forma directa para el almacenamiento, sino de un gran número de dispositivos los cuales son de un costo elevado.

Si bien es cierto que el costo total que ha sido estimado no debe ser soportado en su totalidad por un solo prestador (Telefonía-Internet), en virtud de la amplia gama que existen prestando sus servicios en el país, cada uno de ellos debería afrontar una gran inversión para poder sobrellevar la implementación del registro de datos de tráfico. A tal respecto, haciendo extensivo a este punto lo ya dicho en relación a la inversión puesta en cabeza de los prestadores para la ejecución de las intervenciones telefónicas en tiempo inmediato (página 27), resulta claro que las obligaciones impuestas a los prestadores de telecomunicaciones no constituyen "cargas" propias de la prestación de los servicios de telecomunicaciones.

Consideraciones finales sobre las normativas de retención de datos de tráfico

En primer lugar es de señalar que resulta muy diferente el trato que recibió el tema de la retención de datos de tráfico de comunicaciones en la Unión Europea, en comparación con nuestro país. En la UE, el proyecto transitó por diferentes organismos supranacionales, recibiendo dictámenes de los mismos y viéndose señaladas diversas falencias de cara a la protección de fundamentales garantías ciudadanas, reconocidas por los textos legales europeos. Igualmente, a pesar de la preocupación vertida por dichos organismos en relación al trascendental significado de una medida destinada a la recopilación en forma masiva de datos de tráfico, como así también a las variadas críticas señaladas por los mismos, la directiva fue definitivamente adoptada. En nuestro país, la cuestión recibió sanción sin debate parlamentario, en relación a un proyecto de ley destinado, según sus fundamentos, a

[66] ***R**edundan**t** **A**rray of **I**ndependent **D**isks,* sistema de almacenamiento informático que usa múltiples discos duros entre los que distribuye o replica los datos. En el nivel más simple, RAID combina múltiples discos en una sola unidad lógica, determinando entonces que el sistema operativo en vez de reconocer varias unidades lógicas, reconozca solo una.

[67] Bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Consiste en un simple armazón metálico con un ancho normalizado de 19 pulgadas. El mismo cuenta con guías horizontales donde es posible instalar el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón.

[68] Dispositivos informáticos que permiten la duplicación de datos para acelerar el acceso a los mismos. Cuando se accede por primera vez a un dato, se hace una copia en el caché, los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

perfeccionar los procedimientos de intervención y derivación de comunicaciones telefónicas con motivo de combatir los secuestros extorsivos exclusivamente. No se hizo referencia alguna al hecho de legislar la retención de datos de tráfico de comunicaciones.

En el mismo sentido, surge de la comparación a simple vista que la extensión de la norma argentina es realmente muy breve en relación a la europea y no presenta justificativos, los cuales están presentes en el texto de su suspendido decreto reglamentario, y brillan por su brevedad.

Actualmente, el decreto reglamentario de la ley 25.873 se encuentra suspendido y existe un número considerable de proyectos de ley presentados por diputados nacionales, destinados a la derogación de la de la mentada ley.[69] A tal respecto, es de señalar que sin lugar a dudas la derogación debe llevarse cabo, y en forma paralela resulta necesario emprender una nueva consideración de la cuestión. La derogación de la norma no debe llevar aparejado el olvido del tema, sino todo lo contrario. Nos encontramos ante la posibilidad de aprovechar todos los debates, criticas, proyectos y consideraciones, acontecidos en otras naciones y utilizarlos de cara a la implementación de un sistema que permita fortalecer la seguridad nacional y la lucha contra la delincuencia en armonía con las garantías constitucionales.

El almacenamiento de datos de tráfico de comunicaciones generalizado y por un periodo de diez años atenta indiscriminadamente contra la intimidad de las personas, permitiendo determinar sus relaciones personales, sus ideas políticas, su situación y relaciones económicas, sus creencias religiosas, sus inclinaciones sexuales, sus gustos, y un sinfín más de aspectos reservados de los individuos. Asimismo, se crea un estado de sospecha universal, y del cual no siempre sus conclusiones resultan acertadas. A modo de ejemplo, llamados realizados en forma equivocada a un número relacionado con de una banda de criminales; la visita a páginas de Internet referentes a temas como terrorismo, armamento, xenofobia; E-mails recibidos de direcciones vinculadas con organizaciones terroristas que uno desconoce, crearían la presunción de una conexión con las amenazas mencionadas y vulnerarían uno de los principios básicos del ordenamiento jurídico: La presunción de inocencia.

En un orden menor de preocupación, pero no menos importante, es de señalar que se corre el riesgo de de socavar la confianza de los usuarios de las comunicaciones electrónicas y disminuir de esta forma la utilización de las tecnologías de comunicación. Esta pérdida de confianza por parte de los consumidores implica poner en riesgo el desarrollo de la sociedad de la información.

---

[69] **Proyecto de ley 1849-D-2005**, Diputados, Publicado en Trámite Parlamentario nº 30 Fecha: 13/04/2005 - **Proyecto de ley 1863-D-2005**, Diputados Publicado en Trámite Parlamentario nº 30 Fecha: 13/04/2005 - **Proyecto de ley 1870-D-2005**, Diputados, Publicado en Trámite Parlamentario nº 30 Fecha: 13/04/2005 - **Proyecto de ley 2610-D-2005**, Diputados, Publicado en Trámite Parlamentario nº 46 Fecha: 05/05/2005 - **Proyecto de ley 0344-D-2007**, Diputados, Publicado en Trámite Parlamentario nº 6 Fecha: 08/03/2007 - **Proyecto de ley 1006-D-2007**, Diputados, Publicado en Trámite Parlamentario nº 18 Fecha: 26/03/2007

Ahora bien, ciertos puntos son de trascendental importancia y merecen que sean realizadas ciertas precisiones sobre los mismos.

En relación al tiempo de almacenamiento de los datos, sin duda alguna establecerlo en diez años resulta insensato, pero tampoco parece ser una solución adecuada establecerlo entre seis meses y dos años como lo hace la Directiva 2006/24/CE.

Como ha sido dicho, resulta inaceptable crear un registro generalizado de información de comunicaciones, que cree un estado de sospecha extensivo a todos los ciudadanos. En la actualidad, el Servicio de Inteligencia del Estado y las autoridades policiales y de seguridad, determinan a través de sus funcionarios que líneas telefónicas deben ser intervenidas o que individuos deben ser investigados y vigilados, y un sinfín más de acciones preventivas. Por tanto la retención de datos de tráfico de comunicaciones debe verse como una herramienta más puesta a disposición de tales organismos. Los mismos, ante una investigación en curso o sospechas fundadas podrán solicitar en forma directa al prestador de servicios de comunicaciones el inicio de la retención de datos. La nota fundamental del procedimiento reside en que si bien la orden de retención de datos viene dada por fuerzas de seguridad, les esta impedido el acceso a la información almacenada, y solo podrán lograrlo mediante una orden judicial emitida al respecto. Si la orden no se lograra en un tiempo prudencial desde la solicitud del almacenamiento, los proveedores de comunicaciones procederán a la destrucción de los archivos. El procedimiento comentado es denominado *Quick freeze* y fue propuesto por el Grupo de Protección de datos del Art. 29, al debatirse la cuestión en Europa. De esta manera, los servicios de inteligencia y demás organismos de seguridad no ven perjudicado su accionar por verse limitados en el tiempo, dependiendo de una orden judicial que habilite la retención, y la intimidad de la ciudadanía se ve debidamente protegida por circunscribirse el procedimiento solo a casos concretos y debidamente fundados.

Conjuntamente, y en forma ciertamente relevante, los costos de implementación se reducen al mínimo. Almacenar datos de comunicaciones ante solicitudes concretas, no requiere la implementación de grandes “servidores” y evade el consecuente gasto millonario en hardware y mantenimiento anual del sistema.

Con respecto a la determinación de los datos objeto de almacenamiento, la cual sin duda alguna debe encontrarse en el texto mismo de la ley y no en su reglamentación, cobra vital importancia lo desarrollado al analizar la Directiva 2006/24/CE. Deberá precisarse al igual que en la normativa europea, en forma detallada, las categorías de datos que deben conservarse, haciéndose una debida referencia en relación al tipo de comunicación que se trate, es decir con respecto a la telefonía fija y móvil, acceso a Internet, Correo Electrónico y telefonía por Internet.

Por último, con respecto a los delitos que pueden suscitar la solicitud de la medida, cabe realizar una interpretación restrictiva y destinarse a la lucha contra el terrorismo, secuestros, amenazas de vida, y otras formas delictivas que representen una seria amenaza. El el texto de

la ley deberá ser claro y preciso y hacer una referencia directa a delitos comprendidos sin utilizar formas genéricas como “delitos graves” u otras que permitan dejar a la libre interpretación de los magistrados cual es su contenido. Debe tenerse en cuenta que la utilización generalizada de esta herramienta terminaría por desnaturalizarla, sirviendo para la persecución de formas delictivas que no ameritan la retención de datos de tráfico de comunicaciones para su eventual investigación.
En definitiva una actitud conciente del legislador, coadyuvada por la participación de asociaciones destinadas a la protección de los datos personales y la defensa de las garantías constitucionales, en la creación de una norma clara y garante de las libertades individuales, fructificaría en la sanción de una ley positiva y sobre todo equilibrada para la lucha contra la amenaza delictiva.

Ahora bien, como ha sido dicho, con la limitación del almacenamiento de datos de trafico a casos concretos mediante el uso de la técnica *Quik freeze*, como se propugna, el derecho a la intimidad encontraría una adecuada protección en balance con la necesidad estatal de luchar contra peligrosas formas delictivas. La preocupación que surge es que pueda existir un abuso, por parte del estado a nivel vigilancia o por parte de los prestadores de comunicaciones, por usar los datos con otros fines no previstos en la legislación y provechosos para sus intereses. Decididamente la normativa a sancionar debe atender adecuadamente a estos factores y contar con mecanismos que disuadan tales prácticas, y que en caso de producirse reciban una apropiada sanción.
Existe en el derecho extranjero una figura que resultaría provechosa para el fin comentado, la cual ha sido objeto de diversos debates y opiniones contrarias, y hasta ha formado parte proyectos de reforma de la legislación argentina: El daño punitivo.[70]
El mismo puede definirse como sumas de dinero que los tribunales mandan a pagar a la víctima de ciertos ilícitos, que se suman a las indemnizaciones por daños realmente experimentados por el damnificado, que están destinados a punir graves inconductas del demandado y a prevenir hechos similares en el futuro[71]
Constituyen prestaciones dinerarias o de otra naturaleza que el tribunal jurisdiccional o arbitral ordena pagar a la víctima de un acto o hecho antijurídico o a un tercero (que puede ser o no el Estado) que el tribunal determine que pueden agregarse a los restantes rubros indemnizatorios (o no) en relación a los daños realmente experimentados por el damnificado, teniendo como base elementos tales como los beneficios obtenidos por el dañador, el dolo, lo repugnante de la

[70] Institución anglosajona denominada *“punitive damages”, “penal damages”, “smart money”, “exemplary damages”, “non compensatory damages”, “aggravated damages”, “aditional damages”, “punitory damages” o “vindictive damages”*. Su primer precedente jurisprudencial se da en la causa “Hucke v. Money” del año 1763, en la cual se juzgara un caso de abuso de poder público contra un viajero.

[71] Pizarro, Ramón Daniel, Daño moral, Hammurabi, 2000, p.374.

conducta y otras circunstancias valoradas en el caso concreto, cuya finalidad es sancionatoria y preventiva.[72]

Los daños punitivos generan dos efectos principales, uno inmediato, al sancionar al dañador, y otro mediato, como elemento disuasivo, al prevenir la reiteración de acontecimientos similares. Asimismo, también tienden a evitar el enriquecimiento ilegítimo.

En reiteradas ocasiones la doctrina nacional ha indicado la importante labor preventiva que este tipo de sanciones pueden cumplir en gran cantidad de casos, entre otros: a) daños al ambiente; b) agravios al honor y a la fama, irrogados mediante medios masivos de comunicación, o también las invasiones injustificadas a la intimidad personal o familiar; c) menoscabos de la integridad o de la salud causados por productos elaborados; d) daños derivados de la mala praxis profesional médica; e) accidentes sufridos por los operarios de la construcción por omisión de las debidas medidas de seguridad de parte de las empresas constructoras; f) perjuicios derivados de la publicidad engañosa.

En la actualidad, y en forma lamentable, resulta que en considerables ocasiones, la única manera de evitar la reiteración de una conducta lesiva de derechos, es la aplicación de sanciones económicas. Las mismas al ser de una magnitud tal, que las caracteriza como sanciones ejemplares, no solo repercuten en la persona del autor de la misma, sino también llaman la atención en forma generalizada, previniendo el futuro acontecer de hechos de similar naturaleza.

La figura que aquí se trata, excede el ámbito de la normativa de retención de datos de tráfico, consistiendo en una institución que para su funcionamiento requiere de su inclusión en el Código Civil. Debe tenerse en cuenta que la condena judicial al pago de daños punitivos, en el estado actual de la legislación argentina en la cual no poseen un adecuado soporte normativo, significaría incurrir en una clara hipótesis de inconstitucionalidad.

En el pasado se han dado proyectos de reforma de la legislación civil y comercial argentina, propugnando su unificación, y en los cuales el daño punitivo lograba su inclusión. Uno de ellos es el proyecto de unificación del año 1.998 elaborado por la Comisión Honoraria designada por decreto del Poder Ejecutivo Nacional Nº 685/95.

El articulo 1587 de dicho proyecto establecía*: "Multa civil. El tribunal tiene atribuciones para aplicar una multa civil a quien actúa con grave indiferencia respecto de los derechos ajenos o de los intereses de incidencia colectiva. Su monto se fija tomando en consideración las circunstancias del caso, en especial los beneficios que aquél obtuvo o pudo haber obtenido con su conducta, y tiene el destino que le asigne el tribunal por resolución fundada."*

[72] Molina Sandoval, Carlos A., Elementos para una conceptualización adecuada de los daños punitivos a partir de un área de aplicación. ED 205-988.

Posteriormente, la redacción del proyecto de unificación de 1998 aprobada por la Comisión de Diputados el 1 de noviembre de 2001, fue la siguiente:

"Artículo 1559: Atribuciones del Juez. Medidas preventivas. Multa civil. Condenación conminatoria. El Juez tiene atribuciones para:

1. *Disponer, conforme a las circunstancias, medidas tendientes a evitar la producción de daño futuro.*
2. *Para aplicar una multa civil a quien actúa con grave indiferencia respecto de los derechos ajenos cuando afecte o pudiere afectar intereses de incidencia colectiva. Su monto se fija tomando en consideración las circunstancias del caso, en especial los beneficios que aquél obtuvo o pudo haber obtenido con su conducta.*

   La multa se destinará al Fondo de garantía para víctimas con el objeto de cubrir las indemnizaciones fijadas por sentencias contra deudores insolventes que se creen en las respectivas jurisdicciones. El Juez podrá destinar a la víctima del caso un porcentaje de la multa no mayor al treinta por ciento.

   La multa solo puede imponerse una sola vez por los mismos hechos. A tal fin, el Poder Ejecutivo centralizará en un registro especial la información sobre las multas que se impongan por los distintos Jueces del país, informe que deberán pedir los Jueces antes de resolver sobre su imposición.
3. *Imponer, a petición de parte y en beneficio de ésta, condenaciones pecuniarias, que pueden ser progresivas, a quien no cumple los deberes jurídicos impuestos en una resolución judicial. Son graduadas teniendo en cuenta la situación patrimonial del destinatario, y pueden ser reajustadas, o dejadas sin efecto, si éste desiste de su resistencia y justifica total o parcialmente su proceder. Son ejecutables.".*

La Corte Suprema de Justicia en el año 1992, en el caso "Servini de Cubría", en el cual fueron debatidos aspectos de la responsabilidad periodística, advirtió la necesidad de que el juez pondere algo mas que el perjuicio efectivamente causado, debiendo examinarse además si, aun afrontando el pago de tales daños, subsiste para el responsable alguna ventaja económica directamente relacionada con la difusión de la noticia, caso en el cual deberá ampliarse proporcionalmente el monto de la condena para impedir todo injusto enriquecimiento.[73]

En las Jornadas Nacionales de Derecho Civil, llevadas a cabo entre los días 23 al 25 de septiembre de 1.999 en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral (Santa Fe), en su Comisión N° 10 abordar on el tema, pronunciándose por la

[73] CSJN, Fallos 148:291

conveniencia de implementar en la nueva legislación unificada el instituto de la multa civil, con carácter de penas privadas legales, para sancionar graves inconductas mediante la imposición al responsable de una suma de dinero.

Se recomendó que su imposición quede limitada a casos de particular gravedad, caracterizables como los evidenciadores de un singular menosprecio del dañador por los derechos del damnificado o los intereses de incidencia colectiva, o cuando media en el autor del daño un propósito lucrativo. Asimismo se hizo hincapié en que deben ir ajenas a un reproche subjetivo inherente a la conducta del sancionado - resultarían inaplicables en supuestos de factor objetivo de atribución - y en cuanto al destino de la pena, se voto por mayoría que debe ser librado por la ley a la prudente determinación judicial por resolución fundada.

Se acordó que solo pueden aplicarse a requerimiento de parte, y que pueden ser sujetos pasivos tanto las personas físicas como jurídicas, públicas o privadas, agregándose que por su naturaleza sancionatoria no debería autorizarse su asegurabilidad.

A pesar de las reiteradas y variadas opiniones doctrinarias dadas a favor de la inclusión normativa del daño punitivo, no faltan quienes no están de acuerdo y ven en el instituto más inconvenientes que beneficios. Así se han señalado: a) Su cuantía es discrecional, y por tanto evidencia impredicibilidad respecto de su entidad, incidiendo en los costos empresariales; b) Producen un enriquecimiento sin causa en la victima; c) Se diluyen los efectos si la responsabilidad es asegurable, d) Es una institución mas vinculada con el Derecho Penal que al Derecho Civil; e) Otorga al juez facultades excesivas, que lindan con la arbitrariedad.

La extensión de las indemnizaciones es un tema que no solo preocupa a los autores nacionales, sino también a doctrinarios de países donde el instituto se encuentra acogido normativamente. En el caso extranjero, el núcleo de la preocupación reside en las elevadas cifras que llegan a alcanzar las multas establecidas por los jurados en el concepto que nos ocupa. Estas objeciones, no parecen constituir obstáculo alguno para la adopción de la figura, en virtud de que en nuestro país su fijación sería por parte de un juez. Hoy en día el magistrado ya se encuentra encomendado a tomar decisiones sobre el patrimonio de las personas y a la fijación de montos resarcitorios en concepto de daños morales, sin perjuicio de lo que las partes alegan. Con respecto a su incidencia en los costos empresariales, cabe advertir que un argumento económico no debe prevalecer sobre las razones de justicia: “el análisis económico del derecho debe ser sometido por el jurista a la critica axiológica, partiendo de los valores fundamentales humanidad y dignidad y atendiendo a la justicia, equidad, seguridad, orden y paz social”, por lo que “los criterios de eficiencia y de maximización de la riqueza, son insuficientes por si solos para fundar soluciones jurídicas”[74]. Además, ha sido

[74] XIII Jornadas de Derecho Civil, Buenos Aires, 1991.

señalado que en los países donde actualmente son de aplicación los *punitive damages*, las economías y el nivel de inversiones no han sufrido merma alguna, sino todo lo contrario.[75]

Con respecto al destino de los fondos, el texto definitivamente aprobado por la Comisión de Diputados, aparece como una solución adecuada a la cuestión. El mismo establece que la multa fijada se destinará al "Fondo de garantía para víctimas" con el objeto de cubrir las indemnizaciones fijadas por sentencias contra deudores insolventes que se creen en las respectivas jurisdicciones, pudiendo el juez destinar a la víctima del caso un porcentaje no mayor al treinta por ciento.

Mosset Iturraspe, quien mas allá de señalar interrogantes y dudas sobre la implantación del instituto, expresó su adhesión firme y convencida a la misma, reparó sobre el destino de la multa civil. En su opinión los diferentes tribunales podrían destinarlo a la agricultura, medioambiente, educación, hospitales, fomento de la cibernética, o justamente, incorporar al ordenamiento argentino los "fondos de garantía", destinados a cubrir a las victimas de accidentes anónimos o de autores no identificados o bien a las victimas de agentes insolventes.[76]

En referencia a la posibilidad de asegurabilidad, la misma debería ser prohibida, en virtud de desnaturalizar el instituto. Si lo que se busca con la imposición de una multa civil es sancionar en forma ejemplar al infractor, la posibilidad de tercerizar la asunción del monto fijado en tal concepto en una compañía aseguradora, vulneraria tal fin. La definitiva legislación del daño punitivo debe hacer referencia concreta a la cobertura por seguros, imposibilitando su existencia, a fin de que la finalidad del instituto adoptado sea cabalmente cumplida.

En definitiva, es de concluir que la inclusión en nuestro ordenamiento positivo de la figura de los *punitive damages*, resulta por demás beneficiosa. No solo servirá para frenar acciones disvaliosas por parte del estado en referencia al almacenamiento de datos de trafico, o de las empresas de comunicaciones encargadas de realizarlos, sino también de tantas otras circunstancias actuales que merecen una debida protección, y que en el orden actual de las cosas, aun no terminan de verse tuteladas adecuadamente.

Confidencialidad de la información asentada?

En la lectura del decreto reglamentario nos encontramos un articulo que causo ciertas controversias, nos referimos al Art. 2 inciso d), el cual establece: "Los prestadores de servicios de telecomunicaciones deberán mantener la confidencialidad de las actividades técnicas y administrativas que deban realizar a fin de cumplir con los requerimientos que se le efectúen en

[75] Piaggio, Anibal Norberto; Compani, M. Fabiana; Cabrera, Delma y Vetrano, Alejando Javier, Las condenaciones punitivas y el proyecto de Código Civil de 1998, R.C. y S., año II, marzo - abril, 2000, p.28

[76] Mosset Iturraspe, Jorge, La Multa Civil o Daño Punitivo. Comentario al proyecto de reforma al Código Civil de 1998. La Ley, 2000 B, p.1277

el marco de la presente norma, y deberán guardar secreto aun respecto de la existencia misma de los requerimientos que les sean efectuados. Serán aplicables con relación a lo aquí dispuesto las normas penales que tutelan el secreto."

Se ha planteado el interrogante de que si por mandato constitucional toda persona tiene derecho a tomar conocimiento de los datos a ella referidos, contenidos en bancos de datos privados destinados a proveer informes y el Decreto 1563/04 obliga a los prestadores de servicios de telecomunicaciones a crear un registro que contenga una cantidad de información relativa a cada individuo - banco de datos privados, evidentemente- y a "...guardar secreto aun respecto de la existencia misma de los requerimientos que sean efectuados, bajo apercibimiento de serle aplicables sanciones de carácter penal" ¿no se estaría vulnerando el Art. 43, párrafo 3° de nuestra Constitución Nacional?

Si bien debemos tener en cuenta que tal articulo reglamenta el artículo 45 Bis de la Ley Nº 19.798 referente a captación y derivación de las comunicaciones, por lo que aparentemente no seria de aplicación al articulo 45 Ter, el cual si se refiere a la registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones, cabe preguntarnos si tal prerrogativa se hace extensiva a las bases de datos y por tal motivo la vulneración al articulo 43 de la CN es real.

Primero, y de manera esencial, debemos determinar el panorama legislativo a nivel nacional.

Habeas Data

Etimológicamente, la locución latina "habeas data" proviene de "habeas", segunda persona del subjuntivo de habeo ... habere, significa aquí "téngase en su posesión", que es una de las acepciones del verbo, y "data" que es el acusativo plural de datum, que los diccionarios más modernos definen como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos. Entonces, "habeas data" significa "que tengas los registros, los datos".[77]

Para la mayoría de la doctrina, éste resulta ser un amparo especializado, cuya misión consiste en brindar protección inmediata y efectiva a los derechos fundamentales afectados por las prácticas de almacenamiento, procesamiento, y suministro de datos.[78]

El Habeas data, antes de la reforma de la Constitución nacional de 1994, contaba con acogimiento en el constitucionalismo provincial y en el derecho comparado. Con la mentada reforma se inserto en el tercer párrafo del artículo 43 de la Carta magna, el cual reza:

"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados,

[77] Othon Sidou, J.M., "Las nuevas figuras del derecho procesal constitucional brasileño: mandamiento de ejecución y habeas data"; LA LEY, 1992-E, p.1016.

[78] Pucinelli, Oscar Raúl, Habeas data: aportes para una eventual reglamentación, ED 161, p.913.

destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística”

Es de notar que el artículo 43 no utiliza la expresión Habeas Data. Esta particularidad viene dada por motivo de que la declaración de la necesidad de reforma de la CN no hizo referencia al instituto del Habeas Data. La misma solo faculto a realizar enmiendas con el objeto de insertar el amparo y el habeas corpus. Por tal motivo el constituyente encauso la inclusión del habeas data mediante la acción de amparo.

El Habeas Data tiene seis objetivos: acceder a la información; conocer su finalidad; rectificarla; actualizarla; suprimirla y asegurar su confidencialidad.

En consecuencia, el texto constitucional prevé la facultad del registro, en consecuencia de conocer los datos propios y verificar el motivo por los cuales ellos han sido recabados. Si estos datos fueren falsos, o almacenados con fines discriminatorios, el afectado podrá solicitar su rectificación, actualización, supresión o confidencialización.

Con respecto a la legitimación, se encuentra activamente legitimada para promover esta acción toda persona física o jurídica, pública o privada, a quien el dato de que se trate afecte en su derecho subjetivo o en su interés legítimo o difuso.

La legitimación pasiva, según la Carta Magna, queda configurada con relación a "registros o bancos de datos públicos, o los privados destinados a proveer informes".

De acuerdo a lo ya dicho, y siguiendo acierto sector de la doctrina, podemos diferenciar ciertas clases de habeas data teniendo en cuenta su objeto y finalidades. Así nos encontramos con:

- El Habeas Data informativo, para recabar: que datos personales se encuentran registrados; con que finalidad se han obtenido y se hallan registrados; de que fuente se han obtenido los datos.
- El Habeas Data rectificador, para: corregir datos archivados que son falsos o inexactos, actualizar o adicionar datos atrasados o incompletos
- El habeas Data de preservación para: excluir datos archivados que integran la información personal denominada “información sensible”, reservar en la confidencialidad ciertos datos archivados que hacen a informaciones legalmente acumuladas, pero innecesarias y sustraídas al acceso de terceros, o susceptibles de originar daño a la persona si son conocidas por terceros.
- El habeas Data mixto, que tiende a más de una finalidad de las antes expuestas.

El texto constitucional establece como única excepción a la viabilidad del instituto en análisis las fuentes de información periodística. La exclusión de otros ámbitos de secreto profesional, considerando que también son ámbitos de la intimidad de la persona, ha sido criticado, señalándose el secreto del abogado, del medico, de los contadores, por ejemplo, en relación a

los datos que los mismo poseen de sus clientes. Pero mas allá de tal reproche, y en un nivel de relevancia mucho mayor, debemos considerar la información registrada por organismo de inteligencia del Estado, dada la importancia que tales bases de datos poseen para el aparato estatal y su necesidad de mantenerlos confidenciales.

Puccinelli[79], entiende que siempre y en todos los casos, debe haber derecho de acceso, se trate del organismo o medio de comunicación que fuere ya que solo se tratara de verificar datos propios del registrado, lo cual implica una operación sencilla. Lo que podrá variar son las facultades de los registrados de acuerdo a la finalidad por la cual se han registrado los datos.

Por su parte, Bidart Campos[80], quien si bien declara como ámbito no cubierto por el habeas data la defensa y seguridad del estado, señala que ambos términos reclaman precauciones para no desmandar su sentido y alcance, y para impedir que se convierta en un Standard al que el estado acuda para violar los bienes jurídicos protegidos a los que el habeas data presta tutela.

Ley de Protección de Datos Personales - 25.326

La ley de protección de datos personales 25.326, publicada en el Boletín Oficial de fecha 2 de noviembre del 2000, vino a reglamentar el instituto del hábeas data para la protección del derecho a la intimidad y privacidad de los datos personales.

A modo de síntesis inicial podemos decir que la misma regula la protección del derecho a la intimidad y privacidad de los datos personales y también, la manera en que deben ser tratados esos datos personales, estableciendo, entre otras, las condiciones de seguridad exigidas para la gestión de los Bancos de Datos Personales, y la responsabilidad que le cabe a los responsables y usuarios de los mismos por su accionar, es sobre este último aspecto que desarrollaremos algunas reflexiones.

En su articulo 1° se establece: " La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43 párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".

Mediante el articulado de la ley se da una efectiva consagración al derecho a la

[79] Puccinelli, Oscar Raul, Ob. Cit.

[80] Bidart campos, Germán J., Manual de la Constitución Reformada, EDIAR, 2002, Tomo II, p.391

autodeterminación informativa. Consiste en un derecho disponible por el individuo que encuentra de esta forma una vía de acceso a información que le concierne, e inmediatamente, la potestad de resolver, por sí mismo -con algunas pocas limitaciones- si quiere que esos datos se transmitan a otros, se conserven bajo reserva o confidencialidad, o se supriman por afectar la sensibilidad de la persona.[81]

Respuesta al cuestionamiento inicial

De la lectura conjunta de los normado por la Constitución Nacional, la ley de datos personales, como así también la reglamentación de esta ultima (1558/2001), podemos sacar conclusiones esenciales a la hora de determinar cual es el trato que debe tener la información almacenada por los prestadores de servicios de telecomunicaciones de cara a los normado por la ley 25.873.

Partiendo de la base que por datos personales que cuentan con protección de la normativa recién especificada se entiende a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, estamos habilitados a sostener que la información almacenada por los prestadores en referencia a sus clientes, encuentra lugar dentro de tal axioma.

Consideremos que las bases de datos cuentan con datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos.

La información es recabada por los prestadores de servicios de telecomunicaciones y puesta a disposición del Poder Judicial o el Ministerio Público, lo cual nos lleva a considerar que si bien la información tiene una finalidad publica encarada a la persecución y lucha contra la actividad delictiva, la naturaleza de la misma no deja de ser privada. Por lo cual y teniendo en consideración las opiniones doctrinarias que propugnan la confidencialidad de datos que hagan a la seguridad del estado, estamos en condición de argumentar, sin hacer un juicio de valor de las mismas, que son de ninguna aplicación en este punto, por el mentado carácter privado de las bases de datos.

Entonces, si bien de la ubicación del articulo 2° i nc. d) del decreto 1563/2004, y de su ambigua redacción, se dificulta la tarea de determinar si la real intención del ejecutivo al reglamentar la ley 25873 fue establecer la confidencialidad de las bases de datos relativas al trafico de comunicaciones de los usuarios de estos servicios, surge claro de nuestra situación legislativa que tal normar resultaría inobjetablemente inconstitucional. La Constitución Nacional en su

[81] Conway, Graciela M., Las medidas de seguridad en los bancos de datos, La Ley 2002-D, p.1237.

articulo 43 párrafo 3°, la ley de protección de dat os personales (25.326)[82], como así también su decreto reglamentario (1558/2001), establecen claramente el derecho que asiste a toda persona para conocer la información relativa a su persona asentada en registros y sus finalidades. Razón por la cual, la posible voluntad estatal de fijar la confidencialidad de los registros en esta obra tratados no encontraría sustento legal de ningún tipo.

Articulo 3°: Responsabilidad por daños derivados de los procedimientos

Incorpórase el artículo 45 quáter a la Ley 19.798 con el siguiente texto: "El Estado Nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros, de la observación remota de las comunicaciones y de la utilización de la información de los datos filiatorios y domiciliarios y tráfico de comunicaciones de clientes y usuarios, provista por los prestadores de servicios de telecomunicaciones."

Cuando la ley dispone que el Estado Nacional asume la responsabilidad por los daños que pudieran derivar a terceros por los procedimientos normados, en realidad no hace mas que en cierta manera ratificar en forma específica, la responsabilidad que por su actuar le compete.
Si buen durante varios siglos reinó el principio de la irresponsabilidad del estado en virtud de su soberanía, durante el siglo XIX la misma encontró punto final. En la actualidad, con base en la concepción francesa, la responsabilidad del Estado por actos y hechos administrativos se apoya en la idea de falta, concebida como el funcionamiento irregular o defectuoso de la función administrativa, debiendo apreciarse la misma no en relación a la culpa del agente sino de acuerdo a las leyes y reglamentos que rigen la función (el servicio) y el daño causado al administrado. [83]
La obligación de reparar tiene como fundamento el principio de la corrección del desequilibrio causado al administrado que soporta un daño, desigualdad que requiere una justa restitución

[82] **Art. 13**: Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita." **Art. 14.1**: El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. **2.** El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. **3.** El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. **4.** El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

[83] Benoit, Francis Paul, Droit Administraitif, Toulouse, 1968, p.712

que, si bien se gradúa de un modo distinto según que provenga de la actuación legitima o ilegitima del estado, responde a la necesidad esencial de reparar la injusticia que provoca la violación de la igualdad, de impedir la subsistencia del desequilibrio. La obligación de resarcir el perjuicio cometido no nace del daño, sino de la alteración del principio de igualdad, aun cuando se requiera la ocurrencia de un daño.[84]

Se trata, de un principio reconocido por el Derecho Constitucional argentino, que estatuye que la igualdad es la base de las cargas públicas (Art. 16 de la Constitución nacional).

Por tanto, si en el caso concreto el daño acaecido por un particular fuera imputable al Estado en virtud de su actuar, y reuniera los requisitos establecidos por la Corte Suprema de Justicia de la nación para fijar su responsabilidad por actos ilegítimos[85], o excepcionalmente legítimos, el mismo tiene la obligación de repararlos mas allá de lo establecido en la normativa y en virtud de substanciales principios sentados por la Constitución Nacional y la jurisprudencia de la CSJN.

Como punto final es de señalar que, la deficiente redacción del precepto no puede derivar, en entender que se ha pretendido "socializar" -con cargo al Tesoro Público- las consecuencias patrimoniales que pudieran derivarse de los daños causados a terceros por el hecho propio de las empresas de telecomunicaciones, responsabilidad ésta respecto a la cual la ley nada innova y que, por lo tanto, sólo será enjuiciable por el Poder Judicial de la Nación bajo el prisma de las normas y principios que rigen la responsabilidad civil, siendo insusceptible de ser reglamentada por el Poder Ejecutivo Nacional bajo pena de conculcar el Principio de División de Poderes.[86]

Nuevos proyectos de ley

La innegable inconstitucionalidad del texto de la ley 25.873, como así también el hecho de haberse visto suspendido el decreto reglamentario de la misma, derivaron en nuevos proyectos de ley destinados a concretar lo que se buscaba normar. Asimismo, pero con posterioridad a los proyectos que se analizarán, es de señalar que la justicia contencioso administrativa federal falló en los autos Halabi c/ Poder Ejecutivo Nacional, a favor de la pretensión de la parte actora, decretando la inconstitucionalidad de los artículos 1 y 2 de la Ley 25.873 y del Decreto 1563/04

[84] Cassagne, Juan Carlos, Derecho Administrativo, Lexis Nexis, Buenos Aires, 2002, p.490

[85] La responsabilidad extracontractual por los hechos y actos ilegítimos del Estado que causan daño sobre el patrimonio o la persona fue reconocida en el caso “S.A. Tomas Devoto c/ Gobierno Nacional s/ daños y perjuicios” fallado el 22 de Septiembre de 1933 por la Corte Suprema de Justicia de la Nación.

[86] Aguilar Valdez, Oscar R, Algunas pautas para clarificar un importante debate. Acerca de la llamada "Ley de Escuchas" 25.873, La Ley 2005-C, p. 944

reglamentario de la misma.[87]

El proyecto de ley de los diputados Tirinello y Piccinini (Expediente 1856-D-2005, Trámites Parlamentarios N° 30 del 13/04/2005), titulado "Der echo a la privacidad en materia de telecomunicaciones" prevé la modificación de la ley 19.798 y su modificatoria 25.873, como así también la derogación del decreto 1563/04.
En primer lugar prevé la sustitución del artículo 45 bis de la ley Nacional de Telecomunicaciones (19.798) introducido por la ley 25.873, referente la captación y derivación de las comunicaciones. Textualmente dispone:

"Artículo 45 bis: La observación remota de las telecomunicaciones sólo podrá efectuarse mediante orden emanada de juez competente, en el marco de procesos judiciales por delitos de acción pública, mediante resolución fundada.
En dicha orden se fijará el plazo de duración de la observación, que en ningún caso podrá extenderse por más de 30 (treinta) días corridos. Esta medida podrá prorrogarse cuantas veces fuera necesario, en todos los casos mediante resolución fundada.
No se podrá almacenar ninguna información obtenida por este medio que no guarde relación directa e inmediata con el objeto del proceso judicial en que se hubiere ordenado.
La información obtenida por medio de la observación remota de comunicaciones sólo podrá ser utilizada dentro del proceso judicial en que se hubiese ordenado."

Sin duda alguna la redacción del citado precepto es superadora de la ley 25.873, pero no queda a salvo de ciertas críticas. En primer, utiliza el término telecomunicaciones, con lo que como ya ha sido explicado, determina un campo de aplicación amplio y abarcativo más allá de las comunicaciones telefónicas, con todos los inconvenientes que trae aparejado. En segundo término, omite hacer referencia a la Dirección de Observaciones Judiciales, único órgano del Estado encargado de ejecutar las interceptaciones, que si bien su competencia viene dada por la ley 25.520 (Inteligencia nacional), su inclusión en el texto de ley 19.798 sumaría al conocimiento generalizado de tal cuestión, por ser esta la normativa reguladora de las telecomunicaciones. Finalmente es de señalar, que si bien el texto propuesto resulta positivo al normar en que procesos la medida es loable de ser decretada, su plazo de duración y la posibilidad de prorroga, omite otros tantos aspectos necesarios, los cuales en definitiva deben ser parte de ley reglamentaria de comunicaciones, en virtud de lo normado por el artículo 18 de la Constitución Nacional.

[87] Halabi, Ernesto c/ Poder Ejecutivo Nacional, Juzgado Nacional de 1ª Instancia en lo Contencioso Administrativo Federal Nro.10, 14/06/2005, La Ley 2005-F, p.319
- Halabi, Ernesto c/ Poder Ejecutivo Nacional, Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal Sala II - 29/11/2005, La Ley 2006-B, p.398

Con respecto a la obligación de retener datos de tráfico, la misma no tiene cabida en el proyecto bajo análisis, propugnándose la derogación de dicho artículo añadido a la ley 19.798 y sustituyéndolo por otro en el cual se suman exigencias para la intervención de comunicaciones. Así determina que: La observación remota de las comunicaciones sólo podrá ser ordenada cuando fuere imposible obtener la prueba requerida por otro medio probatorio; Sólo podrá afectar a las comunicaciones que emitan y/o reciban en sus domicilios particulares, lugares de trabajo y/o equipos o terminales móviles el imputado en causa penal por delito de acción pública, la víctima y/o los familiares de ésta; y que en el caso de que la observación remota se haga respecto de las comunicaciones que emitan y/o reciban la víctima y/o los familiares de ésta, se requerirá el consentimiento de los interesados.
Es de reiterar en este punto, lo dicho en el párrafo anterior *in fine.*

Por ultimo, es de señalar que en los fundamentos que acompañan al proyecto de ley, los diputados Tirinello y Piccinini argumentan que la sensación de inseguridad tan hábilmente instalada en la actualidad sirve como excusa para el avasallamiento de numerosos derechos, en especial, las garantías procesales y carcelarias. Que el imperialismo (eufemísticamente llamado “globalización”) necesita controlar todo y nada puede estar fuera de él, ya que si se lo está, se torna sospechoso. Se hace referencia en tal sentido a la Patriot Act, sancionada en los Estados Unidos, la cual crea un Estado “omnipresente, omnipotente y omnisciente” y entendiendo que por ese mismo camino avanzan los artículos 45 bis, 45 ter y 45 quáter incorporados por la ley 25.873, determinando que todos somos sospechosos de todo, siendo eso es suficiente para que nuestras comunicaciones sean interceptadas.
Por último, señalan en sus fundamentos, que si bien es necesario prever la posibilidad de ordenar escuchas telefónicas en el marco de causas penales, ella debe serlo en términos claros y restrictivos, atento las impredecibles consecuencias que podrían derivar de su ejercicio.

Prosiguiendo con el examen de los nuevos proyectos, nos encontramos con el presentado por los diputados Bossa y Ritondo (Expediente 1863-D-2005, Trámites Parlamentarios N° 30 del 13/04/2005), titulado “Nueva propuesta de sistema de escuchas telefónicas respetuoso de las garantías constitucionales”. El mismo, en similar sentido que el proyecto antes comentado, prevé la derogación de la ley 25.873 y su decreto reglamentario, y la modificación de la ley 19.798.
En primer lugar, el inciso A) del proyecto establece: *“Los prestadores de servicios de telecomunicaciones que brinden servicios de telefonía fija y/o móvil deberán cooperar con el Estado nacional, en la medida de sus posibilidades tecnológicas, en la captación y derivación de las comunicaciones que se transmiten por sus redes para su observación remota a*

requerimiento del Poder Judicial por razones de preservación de la seguridad pública, de conformidad con la ley 25.520. Quedan excluidos de esta obligación aquellos prestadores que brinden servicios de Internet o de transmisión de datos en general, incluidos los servicios de mensajes de correo electrónico, de mensajes cortos o navegación en páginas WAP (SMS-GPRS) en la telefonía móvil"

De la lectura del citado precepto surge que la intención, reside en limitar el deber de colaboración para las intervenciones solo a los prestadores de telefonía fija y móvil, excluyéndose los servicios de Internet, como así también el envío de mensajes de texto y navegación de páginas WAP vía telefonía celular. Asimismo, se establece que la cooperación se encuentra limitada a las posibilidades tecnológicas con las que cuentan los prestadores. Llamativamente, a pesar de esta disposición, el inciso b) del proyecto pauta que los prestadores mencionados deberán soportar los costos derivados de la obligación precedente. Por tanto, si en primer lugar se establece que la obligación deberá ser cumplida en relación a las posibilidades tecnológicas de cada prestador, y no se manda a la implementación de ninguna tecnología en particular. ¿Qué costos son los que deben soportar los prestadores?, ¿La referencia correcta sería a las posibilidades económicas en vez de tecnológicas en el inciso A)?

Dentro de esta confusión que causa la redacción, poco vale la segunda parte del incido B) que determina que en los casos en los cuales el costo de la adquisición del equipamiento y redes de comunicaciones necesarios para la implementación y mantenimiento del sistema de interceptación de llamadas, exceda las razonables pautas de colaboración entre los prestadores y el Estado nacional, la autoridad de aplicación podrá establecer que parte de los mismos sean descontados de la tasa de control, fiscalización y verificación establecida por el artículo 11 del decreto 1.185/90 (Telecomunicaciones).

Por su parte el inciso C) referente a la retención de datos de trafico de comunicaciones, pauta que la misma debe realizarse por espacio de cinco años, y que los datos a conservar surgirán conforme al Plan Fundamental de Numeración y el Plan Fundamental de Señalización Nacional que establezcan la autoridad de aplicación.

No se dan justificativos de la conservación de datos por un periodo de cinco años y erróneamente se delega la determinación de los datos a retener, los cuales necesariamente deben ser establecidos en forma clara y precisa en el texto mismo de la ley.

En definitiva, este proyecto que expone lograr un balance adecuado en cuanto a la protección del derecho a la intimidad, la seguridad, la competencia empresaria y la incorporación de tecnología, ostenta un texto confuso, no justifica adecuadamente los términos de su normar, como así tampoco el plazo de retención de datos de tráfico y delega la determinación de los mismos.

Finalmente, el proyecto de la diputada Negre de Alonso (Expediente 0808-S-2005, Diarios de Asuntos entrados N° 43 del 13/04/2005), bajo el tít ulo “Modificación de la ley 19.798”, se limita a reproducir el texto de la ley 25.873 realizando una sola modificación a sus términos y reduciendo la conservación de los datos de tráfico a cinco años.

Sustituye en los 3 incisos incluidos al artículo 45 de la ley 19.798, la palabra telecomunicaciones por telefonía. Así en el artículo 45 bis donde se establece “Todo prestador de servicios de telecomunicaciones” resulta en “Todo prestador de servicios de telefonía”, en el artículo 45 ter: “Los prestadores de servicios de telecomunicaciones” es sustituido por “Los prestadores de servicios de telefonía”; aconteciendo lo mismo en el texto del artículo 45 ter.

En definitiva, las obligaciones puestas en cabeza de todos los prestadores de telecomunicaciones, pasan a ser privativas de los prestadores de servicios de telefonía. En cierta manera, resulta de la modificación una aproximación mayor al texto del proyecto del diputado Díaz Bancalari, oportunamente comentado. Sin embargo, no es de olvidarse que el mismo no contenía referencias a la retención de datos de tráfico, estaba dirigido a los prestadores de servicios de comunicaciones móviles y se circunscribía a la lucha contra los secuestros extorsivos.

Surge claramente de los fundamentos del proyecto, que el propósito de la diputada es limitar el alcance de la ley 25.873 de cara al significado dado a la palabra “telecomunicación” en la ley 19.798, sustituyendo así dicho término por el de telefonía. Asimismo expresa que tal propósito viene dado en virtud del proyecto que sirvió de base a la sanción de la ley, y del cual la redacción final se aparto considerablemente.

Con respecto a la conservación de los datos de tráfico simplemente señala que debe reducirse de diez años a cinco, pero sin dar ningún tipo de argumento, o realizar análisis del impacto económico de tal medida.

Conclusiones Finales

A modo de colofón, resulta ineludible en este punto final, reiterar ciertas conclusiones y propuestas dadas a lo largo del presente desarrollo.

Con respecto a la intervención de comunicaciones dispuesta por el artículo primero de la ley analizada, es de remarcar que la sanción del texto definitivamente adoptado se hizo sobre una modificación sustancial del proyecto originario, derivando en un campo de aplicación amplio y abarcativo de todo tipo de comunicaciones. No existió una exposición de motivos adecuada y no contó con el siempre necesario y debido debate parlamentario. No se debatió sobre la materia que se legisló.

Por lo tanto, como ha sido dicho oportunamente, si bien podemos considerar que la voluntad real del legislador pudo estar dirigida a las comunicaciones móviles, o máxime a las

comunicaciones telefónicas, la sanción definitiva de la ley utilizo términos amplios que desencadenaron en una aplicación generalizada a todo tipo de comunicaciones en forma injustificada

Conjuntamente, resulta forzoso concluir que lo normado por el artículo 1° de la ley 25.873 es desde todo punto de vista reprochable e inaceptable. Su texto se inserta en una realidad normativa referente a las telecomunicaciones que no es la debida, atento a la falta de sanción de la ley reglamentaria de la intervención de las mismas, en cumplimiento del mandato constitucional del Art. 18 de nuestra Carta Magna.

Resulta ineludible la sanción de dicha ley de cara a lo que representa la evolución de las telecomunicaciones y sus consecuentes repercusiones cada día mayores en todos los ámbitos de la vida ciudadana. Dicha ley deberá establecer definitivamente un catálogo taxativo de situaciones que permitan la intervención de comunicaciones, la duración de la medida, la posibilidad de prorroga, la autoridad de aplicación y el destino de lo grabado.

El tema de la retención de datos de tráfico resulta por demás complejo y como ha sido expuesto, suscita diversidad de opiniones a nivel mundial. En la Unión Europea, la cuestión transita por un periodo de armonización de las legislaciones internas de cada estado miembro, en búsqueda de un adecuado equilibrio entre los derechos individuales y la seguridad nacional.

Lamentablemente, en nuestro país el tema recibió un trato absolutamente distinto. La cuestión recibió sanción sin debate parlamentario y sin hacerse referencia alguna al hecho de legislar la retención de datos de tráfico de comunicaciones.

Asimismo, la legislación de la retención de datos de tráfico viene dada a través de un solo y breve artículo, y un par más en el decreto reglamentario de la ley. Realmente contrastante de cara a la Directiva 2006/24/CE de la Unión Europea y a las normativas que con anterioridad ciertos Estados ya habían sancionado en referencia a este procedimiento técnico.

En el mismo sentido, es de reiterar que la determinación de almacenar la información por un periodo de diez años atenta indiscriminadamente contra la intimidad de las personas, conlleva a la generación de un estado de sospecha generalizado y se corre el riesgo de socavar la confianza de los usuarios de las comunicaciones electrónicas, disminuyendo de esta forma la utilización de las tecnologías de comunicación.

A pesar de todas las falencias señaladas, resulta ineludible, lejos de propugnar por una derogación de la ley 25.873 que conlleve a un olvido del asunto, considerar que nuestro país se encuentra ante una magnifica posibilidad: Aprovechar las experiencias extranjeras, evaluar sus textos adoptados y aprovecharlos con la finalidad de concebir una ley superadora de las foráneas y respetuosa de los derechos y garantías establecidos por la Constitución Nacional.

Desde aquí se propone que la retención de datos de tráfico sea entendida como una herramienta más puesta a disposición de los organismos y fuerzas de seguridad. Lo antedicho tiene por efecto, el hecho de no realizarse un almacenamiento generalizado de información,

sino por el contrario efectuarse solo ante una investigación en curso o sospechas fundadas. El procedimiento consistiría en una solicitud realizada en forma directa, por el organismo de seguridad, al prestador de servicios de comunicaciones, quien daría comienzo a la retención de datos. La nota fundamental de la propuesta reside en que si bien la orden de retención de datos viene dada por fuerzas de seguridad, les esta impedido el acceso a la información almacenada, y solo podrán lograrlo mediante una orden judicial emitida al respecto. Si la orden no se lograra en un tiempo prudencial desde la solicitud del almacenamiento, los proveedores de comunicaciones procederán a la destrucción de los archivos.

Gracias a este proceder, los servicios de inteligencia y demás organismos de seguridad no ven perjudicado su accionar por verse limitados en el tiempo, dependiendo de una orden judicial que habilite la retención, y la intimidad de la ciudadanía se ve debidamente protegida por circunscribirse el procedimiento solo a casos concretos y debidamente fundados.

En forma conjunta, se elude uno de los escollos principales a la hora de poner en aplicación la retención de datos de tráfico por parte de los prestadores de comunicaciones, el costo de implementación. Almacenar datos de comunicaciones ante solicitudes concretas, no requiere la implementación de grandes sistemas informáticos destinados al almacenamiento de la información, evitándose de esta manera el consecuente gasto millonario en hardware y mantenimiento anual del sistema.

Al mismo tiempo, deben tener una especial consideración dos cuestiones de trascendental importancia, las categorías de datos a almacenar y los delitos que pueden suscitar la implementación de la medida. Con respecto a la primera cuestión, es de suma importancia que la ley a sancionar determine en su propio articulado, y en forma detallada, los datos objeto de almacenamiento, haciéndose referencia a cada tipo de comunicaciones en particular. En relación a los delitos que pueden suscitar la solicitud de la medida, cabe realizar una interpretación restrictiva y destinarse a la lucha contra el terrorismo, secuestros, amenazas de vida, y otras formas delictivas que representen una seria amenaza. Siendo en tal sentido inexcusable que el texto de la ley sea claro y preciso y haga una referencia directa a los delitos comprendidos, sin utilizar formas genéricas como “delitos graves” u otras que permitan dejar a la libre interpretación de los magistrados cual es su contenido.

La búsqueda por parte del estado del mantenimiento de la seguridad nacional y la lucha contra la delincuencia, necesariamente debe realizarse en un marco donde los derechos individuales no se vean afectados. La implementación de la retención de datos de tráfico en los términos que aquí se propugnan, encuentra una adecuada proporcionalidad y balance entre los intereses en juego, estableciéndose como una herramienta positiva y beneficiosa en su inclusión en el ordenamiento jurídico argentino.

Apéndice

Ley 25.873

Modifícase la Ley Nº 19.798, en relación con la responsabilidad de los prestadores respecto de la captación y derivación de comunicaciones para su observación remota por parte del Poder Judicial o Ministerio Público.

Sancionada: Diciembre 17 de 2003.

Promulgada de Hecho: Febrero 6 de 2004.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1º — Incorpórase el artículo 45 bis a la Ley 19.798 con el siguiente texto:

"Todo prestador de servicios de telecomunicaciones deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente.

Los prestadores de servicios de telecomunicaciones deberán soportar los costos derivados de dicha obligación y dar inmediato cumplimiento a la misma a toda hora y todos los días del año.

El Poder Ejecutivo nacional reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Público."

ARTICULO 2º — Incorpórase el artículo 45 ter a la Ley 19.798 con el siguiente texto:

"Los prestadores de servicios de telecomunicaciones deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años."

ARTICULO 3º — Incorpórase el artículo 45 quáter a la Ley 19.798 con el siguiente texto:

"El Estado nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros, de la observación remota de las comunicaciones y de la utilización de la información de los datos filiatorios y domiciliarios y tráfico de comunicaciones de clientes y usuarios, provista por los prestadores de servicios de telecomunicaciones."

ARTICULO 4º — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS DIECISIETE DIAS DEL MES DE DICIEMBRE DEL AÑO DOS MIL TRES.

— REGISTRADA BAJO EL Nº 25.873 —

EDUARDO O. CAMAÑO. — DANIEL O. SCIOLI. — Eduardo D. Rollano. — Juan Estrada.

Decreto 1563/2004

Reglaméntanse los artículos 45 bis, 45 ter y 45 quáter de la Ley Nº 19.798 y sus modificaciones, con la finalidad de establecer las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones en relación con la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o del Ministerio Público. Obligaciones de los operadores y licenciatarios de servicios de telecomunicaciones. Reclamos administrativos y vía judicial. Adecuación del equipamiento y tecnologías que se utilizan para la prestación de servicios de telecomunicaciones, a los efectos de la presente normativa. Plazos referidos a los requerimientos de interceptación y de información que se efectúen. Sanciones. Reglaméntase asimismo el artículo 34 de la citada Ley en relación con la competencia del órgano del Estado legalmente encargado de las verificaciones e inspecciones.

Bs. As., 8/11/2004

VISTO la Ley Nº 25.873, modificatoria de la Ley Nacional de Telecomunicaciones Nº 19.798, y sus modificaciones, y la Ley Nº 25.520 y su Decreto Reglamentario Nº 950/02, y

CONSIDERANDO:

Que la Ley Nº 25.873 incorporó a la Ley Nacional de Telecomunicaciones los artículos 45 bis, 45 ter y 45 quáter.

Que el objetivo de la ley es combatir el delito, y a la par servir al esquema de seguridad colectivo de la Nación, ello mediante la utilización de modernas herramientas de captación y monitoreo de comunicaciones de las redes públicas y/o privadas de telecomunicaciones, cualquiera sea su naturaleza, origen o tecnología, en tanto operen en el territorio nacional, orientado a desbaratar las amenazas que resultan factibles de vislumbrar.

Que las actividades ilícitas son un flagelo que se vale de múltiples herramientas para su ejecución, entre las cuales sobresale el uso de sistemas de telecomunicaciones de la más variada gama, evidenciado en la utilización de modernas tecnologías, particularmente, y a sólo título de ejemplo, en los casos de secuestros extorsivos y narcotráfico.

Que, asimismo, y en el marco también de los objetivos apuntados, resulta conveniente y necesario establecer temperamentos de acción concretos y dinámicos, que hagan factible al órgano estatal legalmente encargado de materializar la interceptación de las telecomunicaciones, formular los requerimientos del caso a los prestadores, orientados al objeto de esta normativa, con sustento en las incumbencias que emanan de la Ley Nº 25.520 y su reglamentación, en un marco de máxima celeridad, sencillez y eficacia.

Que el tercer párrafo del artículo 45 bis incorporado a la Ley Nº 19.798 y sus modificaciones establece que el PODER EJECUTIVO NACIONAL reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o del Ministerio Público.

Que otros países ya han normado sobre la materia, con resultados eficaces tanto en el ámbito público como el privado.

Que ha tomado la intervención de su competencia el Servicio Jurídico pertinente.

Que la presente medida se dicta en virtud de lo dispuesto en el artículo 99, inciso 2 de la Constitución Nacional.

Por ello,

EL PRESIDENTE DE LA NACION ARGENTINA

DECRETA:

Artículo 1º — A los efectos del presente decreto, se adoptan las siguientes definiciones:

Telecomunicaciones: Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, cable eléctrico, atmósfera, radio electricidad, medios ópticos y/u otros medios electromagnéticos, o de cualquier clase existentes o a crearse en el futuro.

Prestador: Es el licenciatario del servicio de Telecomunicaciones, en cualquiera de sus formas o modalidades, presentes o futuras.

Usuario: Es toda persona física o jurídica que utiliza los servicios de un prestador.

Captación de la telecomunicación: Es la obtención e individualización, a través de medios técnicos, del contenido de una telecomunicación que se produce entre dos o más puntos o destinos.

Derivación de la telecomunicación: Es la modificación de la ruta de la telecomunicación con el fin de permitir su observación remota, sin modificar su contenido y características originales.

Observación remota: Es la observación de las telecomunicaciones efectuada desde las centrales de monitoreo del órgano del Estado encargado de ejecutar las interceptaciones.

Lugar de observación remota: Son los centros de monitoreo del órgano del Estado encargado de ejecutar las interceptaciones, desde los cuales se efectúa la observación de las telecomunicaciones.

Información asociada: Debe entenderse por tal, toda la información original, no alterada por proceso alguno, que permita individualizar el origen y destino de las telecomunicaciones, tales como registros de tráfico, identificación y ubicación del equipo utilizado, y todo otro elemento que torne factible establecer técnicamente su existencia y características.

Organo del Estado encargado de ejecutar las interceptaciones: Conforme a la Ley Nº 25.520 es la DIRECCION DE OBSERVACIONES JUDICIALES de la SECRETARIA DE INTELIGENCIA de la PRESIDENCIA DE LA NACION.

Autoridad de Aplicación: Es la COMISION NACIONAL DE COMUNICACIONES, dependiente de la SECRETARIA DE COMUNICACIONES del MINISTERIO DE PLANIFICACION FEDERAL, INVERSION PUBLICA Y SERVICIOS.

Autoridad de Regulación: Es la SECRETARIA DE COMUNICACIONES dependiente del MINISTERIO DE PLANIFICACION FEDERAL, INVERSION PUBLICA Y SERVICIOS.

Art. 2º — Reglaméntase el artículo 45 bis de la Ley Nº 19.798 y sus modificaciones:

a) En todos los casos, la obligación establecida en el artículo 45 bis de la Ley Nº 19.798 y sus modificaciones abarcará la información inherente a las telecomunicaciones y la información asociada a las telecomunicaciones, incluyendo la que permita establecer la ubicación geográfica de los equipos involucrados en ellas, como asimismo todo otro dato que pudiera emanar de los mismos.

b) Cuando, por el tipo de tecnología o estructura de redes seleccionado u otras razones técnicas, resulte necesario utilizar herramientas o recursos técnicos, inclusive software o hardware específicos, para la interceptación y derivación de las comunicaciones, las compañías licenciatarias de servicios de telecomunicaciones deberán disponer de estos recursos desde el mismo momento en que el equipamiento o tecnología comience a ser utilizado. A tal fin, previo a ello, se deberán realizar las pruebas técnicas operativas del equipamiento que se trate y será un requisito ineludible su consecuente aprobación por parte de las autoridades públicas intervinientes, quienes a los fines de la presente normativa, tendrán facultades de supervisión e inspección. Los prestadores deberán mantener informados a dichos organismos acerca de sus innovaciones tecnológicas y operativas, y sobre la aplicación de nuevos servicios que tengan implicancias técnicas.

c) Los prestadores de servicios de telecomunicaciones serán responsables por el uso que se dé a los recursos mencionados en el punto anterior fuera del marco del cumplimiento de la presente norma. Dicha responsabilidad comprende a todo acto realizado por sí, por sus dependientes o por terceros de cuyos servicios se valgan.

d) Los prestadores de servicios de telecomunicaciones deberán mantener la confidencialidad de las actividades técnicas y administrativas que deban realizar a fin de cumplir con los requerimientos que se le efectúen en el marco de la presente norma, y deberán guardar secreto aun respecto de la existencia misma de los requerimientos que les sean efectuados. Serán aplicables con relación a lo aquí dispuesto las normas penales que tutelan el secreto.

e) Los prestadores de servicios de telecomunicaciones no podrán, bajo ningún concepto, incorporar arquitectura de redes, tecnología ni equipamiento que impida la interceptación en forma remota de las comunicaciones conforme a los procedimientos legalmente establecidos. Tampoco podrán incorporar servicios que pudieren entorpecer, limitar o disminuir, de cualquier manera, la obtención de la interceptación y de toda la información que se prevé en el presente.

f) Los operadores arriendan infraestructura a terceros deberán contar con los medios técnicos que permitan la observación de todas las comunicaciones que se cursan por sus redes, aun las de otras licenciatarias o usuarios que utilizan su estructura.

g) Todas las comunicaciones originadas en redes de telecomunicaciones, sin excepción alguna, deben ser cursadas sólo si el operador que las origina envía un número que identifique al usuario y al prestador de origen, siempre que no provenga de una llamada desviada.

Los prestadores de servicios de telecomunicaciones de larga distancia internacional que reciban tráfico de terceros operadores internacionales con destino a redes locales, deberán identificar igualmente dichas llamadas de modo de establecer su origen, prestador y abonado de origen.

La autoridad de regulación, puede establecer excepciones para los casos de llamadas internacionales entrantes de países que no transmitan el ANINúmero de A con formato de número internacional.

h) La información que se intercambiará en tiempo real en la señalización para la interconexión entre redes deberá incluir:

El número de "A", entendiéndose por tal al "Número que identifica el origen de una llamada", con formato de "número nacional", de acuerdo a lo dispuesto en la Resolución Nº 47 de fecha 13 de enero de 1997 de la SECRETARIA DE COMUNICACIONES (Plan Fundamental de Señalización Nacional), o la normativa que la reemplace en el futuro.

Lo expuesto es aplicable a las llamadas de servicios montados sobre redes inteligentes, como tarjetas y cualquier otra modalidad actual o futura, siendo a tal fin insuficiente la sola identificación de plataforma del operador.

La categoría de "A" deberá contener al menos: operadora, teléfono público o abonado normal.

El número de "B", entendiéndose por tal al "Número que identifica al destino de una llamada" con formato de número nacional o número internacional, según corresponda.

El estado de "NB", derberá contener al menos: abonado libre, abonado ocupado y contestación (conexión).

i) Asimismo, los operadores deben poner a disposición los medios técnicos y humanos necesarios para que esa información pueda ser recibida en tiempo real y en condiciones de ser interpretada por el órgano del Estado encargado de ejecutar las interceptaciones, salvedad

hecha, en su caso, de una comunicación que se encuentre en curso, al momento mismo de la efectivización de la interceptación.

j) Las interceptaciones y derivaciones que deben efectuar las compañías licenciatarias de servicios de telecomunicaciones a requerimiento del órgano del Estado encargado de ejecutarlas, deberán hacerse efectivas de inmediato, a través de sistemas de gestión de conexión directa, salvedad hecha de aquellos prestadores que merezcan un tratamiento particular justificado por parte del Organo del Estado encargado de ejecutar las interceptaciones y de manera tal que:

1- Permitan la observación aún cuando el usuario intervenido desvíe las llamadas hacia otros servicios de telecomunicaciones o equipos terminales, incluidas las llamadas que atraviesen más de una red o que estén procesadas por más de un operador de red/ proveedor de servicio.

2- En el caso de abonados de telefonía móvil, permitan su observación desde la central de monitoreo designada por el órgano del Estado encargado de ejecutar las interceptaciones, aun cuando el usuario intervenido se encuentre en tránsito en el área de cobertura de otro prestador que le brinde servicio. Cuando el servicio a observar se encuentre en tránsito fuera del ámbito nacional, el prestador deberá informar en forma inmediata, en cuanto sus sistemas lo permitan, cual es el proveedor del exterior que ha adquirido acceso a esas comunicaciones y resguardar toda la información de tasación y tráfico que registre.

3- Se obtenga y transmita para su observación en tiempo real, el contenido de la telecomunicación en formato y calidad original, y en forma simultánea, toda la información asociada con que cuente la compañía y que pueda resultar útil al organismo estatal para cumplir con su cometido; como ser: número de "A", número de "B", hora de inicio, finalización y duración de la comunicación o conexión, señalización de acceso a estado disponible; número de "B" para conexiones salientes aún en los casos en los que no haya una conexión establecida en forma satisfactoria; número de "A" para conexiones entrantes aún en los casos en los que no haya una conexión establecida en forma satisfactoria; todas las señales emitidas por el objetivo, incluídas aquellas emitidas para activar servicios tales como la llamada en conferencia y la transferencia de llamadas; destino actual y otros números en los casos en los que se haya desviado la llamada, identificación y ubicación del receptor (celda, sector, radio de acción de la celda).

4- Permita lograr una correlación exacta de los datos mencionados en el punto anterior con el contenido de las llamadas.

5- La interceptación incluya todos los servicios y facilidades brindados al cliente.

6- La medida se realice sin que se produzcan alteraciones en el servicio que puedan alertar al causante.

7- Sean provistas sólo las telecomunicaciones desde y hacia un servicio tomado como objetivo, con exclusión de cualquier telecomunicación que no esté incluida dentro del alcance de la autorización de interceptación.

8- Las comunicaciones interceptadas serán derivadas decodificadas, descomprimidas y desencriptadas para el caso de que los operadores de red/ proveedores de servicio codifiquen, compriman o encripten o de cualquier otro modo, modifiquen a efectos de la transmisión o tráfico, el contenido de las telecomunicaciones que cursan. Esta obligación subsistirá para el caso en que la codificación, compresión, encriptado o modificación sea realizada por el usuario o cliente con herramientas o recursos técnicos provistos por el prestador.

9- Sin perjuicio de lo establecido en los apartados precedentes, las prestatarias proporcionarán al órgano del Estado encargado de ejecutar las interceptaciones los medios técnicos necesarios para que, al recepcionarse la orden judicial, éstas sean efectivizadas en forma inmediata por el propio organismo estatal desde su centro de monitoreo, ello con la salvedad prevista en primer párrafo del presente apartado, adoptando las medidas de resguardo y conservación a que hubiere lugar, debiendo luego darse estricto cumplimiento al procedimiento establecido en el artículo 22 de la Ley Nº 25.520 y en el artículo 15 del Anexo I del Decreto Nº 950/02. A tal fin, los prestadores deberán adecuar equipamiento y tecnología necesarios de conformidad con lo previsto en el primer párrafo del artículo 5º del presente.

k) Las compañías licenciatarias de servicios de telecomunicaciones deberán suministrar al órgano del Estado encargado de ejecutar las interceptaciones, la información asociada a sus abonados que les sea requerida para el cumplimiento de su cometido.

l) Los prestadores de servicios de telecomunicaciones deberán instrumentar los recursos pertinentes para recibir y dar respuesta a las solicitudes de aquél órgano estatal que requieran su inmediata instrumentación, las VEINTICUATRO (24) horas del día y todos los días del año.

m) Los prestadores deberán contar con la capacidad necesaria para llevar adelante las obligaciones que emanan de la presente normativa. Asimismo, los prestadores deberán coordinar con el órgano del Estado encargado de ejecutar las interceptaciones, los procedimientos conducentes al desarrollo de las tareas técnicas necesarias para el cumplimiento de la presente normativa.

n) La autoridad de contralor garantizará el cumplimiento de estas medidas y estará facultada en su caso, de oficio o a pedido de parte, a sancionar el incumplimiento mediante la aplicación del régimen pertinente, sin perjuicio de las responsabilidades personales a que hubiere lugar conforme a las normas legales vigentes.

o) Los prestadores de servicios de comunicaciones, deberán soportar los costos de todo equipamiento, elemento tecnológico (software o hardware), vinculación, línea o trama, nueva o existente, necesaria para la captación de las comunicaciones y conexión efectiva entre sus centrales y el lugar de observación remota, y la obtención de los datos asociados en las condiciones establecidas en la presente norma. Asimismo, deberán tomar a su cargo los costos de equipamiento, personal, insumos y todo otro gasto que resulte necesario para el cumplimiento de las obligaciones establecidas en la ley conforme al presente decreto, incluyéndose los servicios que se presten al órgano encargado de ejecutar la interceptación para transportar las telecomunicaciones, y los del tendido de cualquier vínculo con dicho propósito, como asimismo la totalidad de los servicios o actividades que fueran necesarios para el cumplimiento de las tareas que impone para la materia la normativa aplicable.

Para los casos previstos en la salvedad incluida en el artículo 2º, apartado j), se admitirán vínculos conmutados.

p) A los efectos de la presente normativa, el órgano del Estado legalmente encargado de ejecutar la interceptación deberá indicar el lugar de observación remota en el requerimiento de interceptación. Dicho organismo podrá determinar otros lugares físicos hacia los cuales se deberán efectuar las derivaciones, según las necesidades operativas propias de cada requerimiento.

Art. 3º — Reglaméntese el artículo 45 ter de la Ley Nº 19.798 y sus modificaciones:

a) Los operadores deberán dar acceso a los datos contractuales actualizados que con relación a sus clientes posean, inclusive la ubicación geográfica y demás datos respecto de los abonados, incluyendo la ubicación geográfica exacta de abonados públicos y semipúblicos.

b) Los licenciatarios de servicios de telecomunicaciones deben arbitrar los medios técnicos y humanos necesarios para que la información esté disponible de inmediato, a toda hora y todos los días del año. Los requerimientos serán realizados por el órgano del Estado encargado de ejecutar las interceptaciones en el marco de la legislación vigente y con sustento en las normas que establece la Ley Nº 25.520 y su reglamentación.

c) Para dar respuesta a los requerimientos aludidos, los licenciatarios deberán establecer mecanismos que permitan la inmediatez de su respuesta. A tal fin, los pedidos y sus contestaciones podrán ser canalizados a través de medios electrónicos u otros medios fehacientes, siempre que guarden la debida tutela de la información, y en tanto resulten idóneos conforme a la celeridad y certeza que la tarea exige.

d) Los licenciatarios de servicios de telecomunicaciones deberán conservar los datos filiatorios de sus clientes y los registros originales correspondientes a la demás información asociada a las telecomunicaciones, por el término de DIEZ (10) años.

Art. 4º — Reglaméntase el artículo 45 quáter de la Ley Nº 19.798 y sus modificaciones:

1- Será requisito previo la formulación del pertinente reclamo administrativo por ante los organos mencionados en la presente reglamentación. Una vez agotada dicha vía quedará expedita la acción judicial.

2- La responsabilidad atribuida al Estado Nacional será declinada en los prestadores o terceros cuando resulte manifiesta la responsabilidad de estos últimos, sin que ello obste a las defensas que aquel pueda ejercitar tanto en sede administrativa como judicial, o a las investigaciones internas a que hubiere lugar, y sin perjuicio de la posibilidad de la acción de regreso del Estado Nacional contra los prestadores que por acción u omisión hubieran ocasionado un daño a un tercero.

Art. 5º — Los prestadores deberán adecuar el equipamiento y tecnologías que utilizan para la prestación de los servicios de telecomunicaciones, a los efectos de la presente normativa, antes del 31 de julio de 2005. La autoridad de contralor deberá velar por el cumplimiento de lo dispuesto, y podrá sólo en casos excepcionales otorgar un plazo de gracia cuando razones técnicas atendibles así lo justifiquen, el cual no podrá extenderse en ningún caso más allá del 30 de septiembre de 2005. En tal supuesto, se deberá efectuar un estricto seguimiento de los planes de adecuación.

Las únicas salvedades a la pauta temporal expuesta serán:

1- La relativa a las modificaciones y adecuaciones tendientes a dar respuesta a los requerimientos de información registral, las cuales deberán hacerse efectivas en un lapso improrrogable de NOVENTA (90) días hábiles administrativos, contados a partir de la entrada en vigencia de esta norma.

2- Las tecnologías y equipamiento incorporados con posterioridad a la entrada en vigencia de la presente reglamentación, para los cuales, el cumplimiento será obligatorio desde su implementación (conforme a lo previsto por el inciso b) del artículo 2).

Art. 6º — Los requerimientos de interceptación y de información que se efectúen conforme al presente régimen deberán responderse en forma adecuada, oportuna y veraz, en los siguientes plazos:

a) Los requerimientos de interceptación calificados como "urgente", deberán hacerse efectivos en forma inmediata, con los tiempos mínimos que técnicamente resulten necesarios para la implementación de la derivación.

b) Los restantes requerimientos de interceptación deberán hacerse efectivos en el plazo de en UN (1) día a partir de la recepción del requerimiento.

c) Los requerimientos de información relativos a los datos filiatorios de usuarios de servicios vigentes deberán ser respondidos de inmediato.

d) Los requerimientos de información calificados como "urgente", correspondientes a telecomunicaciones que están siendo observadas, y relativos al período de observación o a los TREINTA (30) días anteriores al pedido, deberán ser respondidos de inmediato.

e) Los restantes requerimientos de información, calificados como "urgente" según el período comprendido deberán ser respondidos en los siguientes plazos:

- De hasta TRES (3) meses anteriores al requerimiento: en el término de UNA (1) hora.

- De más de TRES (3) meses y hasta DOS (2) años: en el término de SEIS (6) horas.

- De más de DOS (2) años: en el término de DOS (2) días.

f) Los restantes requerimientos según el período comprendido, deberán ser respondidos en los siguientes plazos:

- De abonados conectados y relativos al período de intervención: en el término de UNA (1) hora.

- Del mes del requerimiento: en el término de UN (1) día.

- De más de TRES (3) meses y hasta DOS (2) años: en el término de DOS (2) días.

- De más de DOS (2) años: en el término de CINCO (5) días.

Art. 7º — La potestad sancionatoria será ejercida por la autoridad de aplicación. Cualquier violación a las disposiciones de la presente normativa, imputable a un prestador, verificada de oficio o a pedido de parte, será susceptible de ser sancionada de acuerdo a lo establecido en la respectiva licencia y en el artículo 38 del Decreto Nº 1185/90 y sus modificatorios, adecuándose a la norma del presente artículo cuando así proceda.

La Autoridad de Aplicación verificará los incumplimientos denunciados y una vez comprobada la falta, evaluará la sanción a aplicar considerando las siguientes circunstancias:

a) La gravedad de la falta.

b) Los antecedentes del prestador con relación al presente régimen.

c) Sus antecedentes generales, particularmente sus recursos tecnológicos.

d) Las reincidencias.

e) Los elementos del caso, la actitud asumida por el prestador y el perjuicio causado por su acción u omisión.

f) El grado de afectación del interés público.

Art. 8º — Reglaméntase el artículo 34 de la Ley 19.798 y sus modificaciones:

A los efectos de las verificaciones e inspecciones relativas al cumplimiento de las obligaciones legales relativas a las interceptaciones de las telecomunicaciones, será competente el órgano del Estado legalmente encargado de ejecutarlas, con el concurso de la Autoridad de Aplicación.

Art. 9º — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — KIRCHNER. — Alberto A. Fernández. — Julio M. De Vido**. —** Aníbal D. Fernández.

Decreto 357/2005

Suspéndese la aplicación del Decreto Nº 1563 del 8 de noviembre de 2004.

Bs. As., 22/4/2005

VISTO la Ley Nº 25.873, modificatoria de la Ley Nacional de Telecomunicaciones Nº 19.798 y el Decreto Nº 1563 del 8 de noviembre de 2004, y

CONSIDERANDO:

Que la Ley Nº 25.873 incorporó a la Ley Nacional de Telecomunicaciones Nº 19.798 los artículos 45 bis, 45 ter y 45 quáter, los que oportunamente fueron reglamentados a través del Decreto que se cita en el Visto.

Que dicha reglamentación se dictó en el marco de los objetivos tenidos en mira por ese cuerpo legal, esto es combatir el delito y servir al esquema de seguridad colectivo de la Nación, mediante la utilización de modernas herramientas de captación y monitoreo de comunicaciones de las redes públicas y/o privadas de telecomunicaciones, cualquiera sea su naturaleza, origen o tecnología, en tanto operen en el territorio nacional.

Que en esta instancia, razones que son de público conocimiento aconsejan suspender la aplicación del citado decreto, a los fines de permitir un nuevo análisis del tema y de las consecuencias que el mismo implica.

Que la presente medida se dicta en uso de las atribuciones conferidas por el artículo 99, incisos 1 y 2 de la CONSTITUCION NACIONAL.

Por ello,

EL PRESIDENTE DE LA NACION ARGENTINA

DECRETA:

Artículo 1º — Suspéndese la aplicación del Decreto Nº 1563 del 8 de noviembre de 2004.

Art. 2º — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — KIRCHNER. — Alberto A. Fernández. — Aníbal D. Fernández. — Julio M. De Vido.

Bibliografía

Aguilar Valdez, Oscar R, Algunas pautas para clarificar un importante debate. Acerca de la llamada "Ley de Escuchas" 25.873, La Ley 2005-C, p. 944

Arazzi, Roland, Derecho Procesal Civil y Comercial, Rubinzal Culzoni Editores, Buenos Aires, 1999

Bidart Campos, Germán J., Manual de la Constitución Reformada, EDIAR, Buenos Aires, 2002

Bourguignon, Marcelo, El debido proceso. Garantía Constitucional, La Ley 1983-D, p.1144

Cafferata, Juan Carlos, La acción de hábeas data, LLC 1996, p.313

Cassagne, Juan Carlos, Derecho Administrativo, Lexis Nexis, Buenos Aires, 2002

Carbone Carlos A., Grabaciones, escuchas telefonicas y filmaciones como medios de prueba. Derecho constitucional de utilizar los medios de prueba pertinentes. Rubinzal-Culzoni, Buenos Aires, 2005

Carrió, Alejandro, Derecho constitucional a la privacidad: Zonas claras de protección y zonas de penumbra, La ley 1993-C, p.752

Carrió Alejandro, Garantías constitucionales en el proceso penal, 5° Edición, Hammurabi, Buenos Aires, 2006, p.229

Chichizola, Mario I., El debido proceso como garantía constitucional, la ley 1983-C, p.910

Cifuentes, Santos, Protección inmediata de los datos privados de la persona. Hábeas data operativo, La Ley 1995-E, p.293

Cifuentes, Santos, Acciones procesales del artículo 43 de la Constitución Nacional - Naturaleza personalísima de los datos informáticos de la persona, La Ley 1999-A, p.258

Cifuentes, Santos, Reconocimiento jurisprudencial del derecho a los datos personales informáticos y del hábeas data en su verdadero fin tutelar, La Ley 1999-E, p.151

Conway, Graciela M., Las medidas de seguridad en los bancos de datos, La Ley 2002-D,

p.1237.

Colautti, Carlos E., Reflexiones preliminares sobre el "habeas data", La ley 1996-C, p.917

Di Vito, Aldo M.; Guerendiain, Hilario J., La ley de habeas data. Aspectos Procesales. Aportes doctrinarios y jurisprudenciales, La Ley 2001-F, p.1362

Dromi, Roberto, Derecho Administrativo 10° Edición actualizada, Ciudad Argentina, Buenos Aires, 2004

Ekmekdjian, Miguel Angel, El hábeas data en la reforma constitucional, La Ley 1995-E, p.946

Ekmekdjian, Miguel A., Manual de la Constitución Argentina 4° Edición Actualizada, Depalma, Buenos Aires., 1997

Fernández Delpech, Horacio, Internet: Su problemática Jurídica 2° Ed, Lexis-Nexis, Buenos Aires, 2004

Friedman, Lawrence M., La republica de las opciones infinitas, Grupo Editor Latinoamericano, Buenos Aires, 1992

Gallardo, María Cecilia; Soria Olmedo Karina; Flori, José Luis, Habeas Data, La ley 1998-A, p.977

García Luis M., La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal penal de la Nación: un cheque en blanco para espiar nuestra vida privada; Cuadernos de Doctrina y Jurisprudencia Penal, Ad-Hoc, Bunos Aires, 1995, N°6, p.419

Graña, Eduardo, Álvarez, César, Principios de Teoría del Estado y de la Constitución, Ad-Hoc, Buenos Aires, p.174

Gonzalez Zavala, Rodolfo M., Multa Civil: La reacción del derecho de daños contra el lucro injusto del responsable, Foro de Cordoba N°72, p.29

Gozaini, Osvaldo Alfredo, El debido proceso en la actualidad, la ley 2004-A, p.1242

Kemelmajer de Carlucci, Aida, Las “Escuchas telefónicas” en la experiencia judicial, Revista de Derecho Privado y Comunitario N° 14, Rubinzal Culzo ni, Santa Fé, 1997, p.79

Kilgelmann, María Romina Sánchez, Sabrina, Autodeterminación informativa y Bancos de Datos, a la luz de un reciente fallo de la Corte Suprema de Justicia de la Nación, RCyS 2007-IV, p.33

Marcos, Gustavo H., Pinedo, Alejandro, Intervención de comunicaciones: Responsabilidad del los prestadores de servicios de telecomunicaciones, La Ley 2004 - A, p.1486

Marienhoff, Miguel S., Tratado de Derecho Administrativo, Tomo IV, 3ª Edición Actualizada, Abeledo Perrot, Buenos Aires, 1980

Molina Sandoval, Carlos A., Elementos para una conceptualización adecuada de los daños punitivos a partir de un área de aplicación. ED 205-988.

Mosset Iturraspe, Jorge, La Multa Civil o Daño Punitivo. Comentario al proyecto de reforma al Código Civil de 1998. La Ley, 2000 B, p.1277

Nobile, Lisandro E, Nuevas formas de intromisión en la vida privada, ADLA 2005-C, p.3589

Othon Sidou, J.M., Las nuevas figuras del derecho procesal constitucional brasileño: mandamiento de ejecución y habeas data, LA LEY, 1992-E, p.1016.

Padilla, Miguel M., La directiva 95/46/CE de la Unión Europea, la ley 1999-B, p. 970

Palazzi Pablo, la regulación de los datos de tráfico en la Argentina: Comentarios a la ley 25.873, Jurisprudencia Argentina, 2004-II, p.1346

Palazzi, Pablo A., La controversia sobre la retención de datos de trafico en Internet, La Ley, columna de opinión, 28/04/2005, p.1

Piaggio, Anibal Norberto; Compani, M. Fabiana; Cabrera, Delma y Vetrano, Alejando Javier, Las condenaciones punitivas y el proyecto de Código Civil de 1998, R.C. y S., año II, marzo - abril, 2000, p.28

Pérez Asinari, María V., La regulación de los datos de tráfico en la Unión Europea: ¿Entre la seguridad y los derechos fundamentales?, Jurisprudencia Argentina, 2004-II, p.1417

Pizarro, Ramón Daniel, Daño Moral, Hammurabi, Buenos Aires, 2000

Pucinelli, Oscar Raúl, Habeas data: aportes para una eventual reglamentación, ED 161, p.913

Quiroga Lavié, Humberto, Constitución de la Nación Argentina Comentada Segunda Edición Actualizada, Zavalia, Buenos Aires, 1997

Rodota, Stefano, La conservación de los dato de tráfico en las comunicaciones electrónicas, Revista de Internet, Derecho y Política N°3, www.uo c.edu/idp

Rojas, Ricardo Manuel, La multa civil en el proyecto de Código Unificado Civil y Comercial y los peligros para la seguridad jurídica, Revista de Derecho Comercial y de las Obligaciones N° 220, Lexis Nexis, p.371

Salas -Trigo Represas, Código Civil Anotado, 2º Edición Actualizada, Depalma, Buenos Aires, 1982

Simari, Virginia, Daños Punitivos: una herramienta eficaz, ED 182-1617

Tale, Camilo, Cuarenta y dos objeciones fundamentales al Proyecto de Código Civil de 1998, en materia de responsabilidad civil, ED 191-953

Travieso, Juan Antonio Moreno, María del Rosario, La protección de los datos personales y de los sensibles en la ley 25.326, La ley 2006-D, 1151

Vilasau, Mónica, La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad, Revista de Internet, Derecho y Política N°3, www.uoc.edu/idp

Zarini, Helio Juan, Derecho Constitucional, Astrea, Buenos Aires, 1992