LA CONSERVACIÓN DE DATOS DE TRÁFICO EN LA LUCHA CONTRA LA DELINCUENCIA INORMÁTICA

Horacio FERNÁNDEZ DELPECH [154][155]

I.- Introducción

Frecuentes debates doctrinarios y legislativos, motiva hoy en día la obligación de conservación de datos de tráfico en las comunicaciones,[156] por parte de los prestadores de los servicios de comunicaciones, a los fines de la lucha contra la delincuencia informática**.**

Si bien el tema hace ya tiempo que es materia de tratamiento con relación a las comunicaciones telefónicas, el creciente uso del correo electrónico como medio de comunicación y transferencia de datos, está imponiendo la necesidad del estudio de las obligaciones que le caben a los ISP como necesarios partícipes del envío y recepción del correo electrónico. De allí entonces que este trabajo está dirigido principalmente al análisis del tema con relación al correo electrónico por Internet.

Pero cuando se habla de la obligación genérica de conservación de datos se está haciendo referencia también a dos posibles situaciones:

- El almacenamiento y conservación *del contenido* de las comunicaciones;
- El almacenamiento de los *datos* de tráfico relativos a estas comunicaciones.

Para algunos en ambas situaciones se encuentra afectado el principio de la confidencialidad y privacidad de las comunicaciones, principio que hoy en día se encuentra garantizado por diversos instrumentos internacionales y legislaciones nacionales. Para otros, solo cuando el almacenamiento y conservación es sobre los contenidos hay afectación de este principio.

Gran parte de las Constituciones del mundo dan amparo a la confidencialidad y privacidad de las comunicaciones, y las diversas leyes de Protección de Datos Personales que se están dictando brindan también esta protección.

La creciente capacidad de almacenamiento y tratamiento informático de datos relativos a usuarios de Internet y del Correo Electrónico que se está produciendo en el mundo, hace cada vez mas necesaria una regulación pormenorizada de estas situaciones y de las obligaciones consecuentes de los ISP, que establezca un justo límite para lograr un necesario equilibrio entre el derecho a la intimidad y privacidad de

---

[154]Especialista en Derecho informático, Profesor Universitario, Presidente de la Asociación de Derecho Informático de Argentina.

[155] Horacio Fernández Delpech, abogado argentino, especialista en Derecho Informático, Profesor Universitario, Presidente de la Asociación de Derecho Informático de Argentina y autor de numerosas publicaciones, entre ellas “Internet: Su Problemática Jurídica” – Editorial LexisNexis-Abeledo Perrot de Buenos Aires. Junio de 2004.

[156] comunicaciones de la telefonía (de red fija o móvil) y las comunicaciones generadas a través de Internet (acceso a Internet, correo electrónico por Internet y telefonía por Internet).

las comunicaciones y, ciertas situaciones que, en miras a un interés general de protección y defensa de la seguridad pública o con la finalidad de la investigación y persecución de delitos, se pueda alterar ese derecho a la privacidad.

II.- El contenido de las comunicaciones

El almacenamiento y conservación del contenido de las comunicaciones electrónicas, plantea un agudo debate.

Cuando un usuario remite un correo electrónico y otro usuario lo recibe, se ha producido un intercambio similar al envío y recepción de un correo postal.

Pero sin embargo existe una diferencia esencial.

En el correo postal, el contenido de lo enviado dentro del sobre no es conocido por el agente transportador (Empresa de Correos), mientras que en el correo electrónico el contenido de mail no es secreto para el transportador, que en este caso es el ISP.

El deber de confidencialidad del transportador creo es en principio una de sus principales obligaciones. No puede revelar a terceros el contenido de los correos electrónicos transmitidos, y debe además adoptar las medidas técnicas de seguridad necesarias para que esa confidencialidad no pueda ser violada por terceros.

Pero se plantean entonces varias preguntas:

¿Ese contenido que se ha transmitido, debe ser conservado por algún determinado tiempo?

¿Puede el ISP revelar ese contenido a un tercero bajo alguna circunstancia?

Creo que el almacenamiento y conservación del contenido de las comunicaciones electrónicas por parte de los ISP, solo es posible excepcionalmente:

- Cuando fuera automático, transitorio y necesario para llevar a cabo la transmisión;
- Cuando la ley expresamente así lo establezca y por el tiempo y modalidad establecido por la misma. La normativa debiera disponer que solamente este almacenamiento y conservación sería posible, cuando fuera ordenado previamente por un Juez y con fundamento en la defensa de la seguridad del estado o la investigación de un delito;
- Cuando las partes intervinientes en la transmisión, así lo hayan requerido expresa y previamente a los fines de la prueba de una transacción comercial. Esta situación debiera estar contemplada por la ley y, quizás lleve a un futuro no muy lejano en donde encontremos el correo electrónico con copia certificada, o aviso de entrega, etc., similares a los del correo postal, y en donde ambos intervinientes en una comunicación electrónica hayan convenido someterse a algún tipo especial de correo electrónico, en donde el ISP conserve los contenidos y los datos de trafico de esa comunicación. Recordemos que los sistemas procesales difícilmente pueden dar cabida a la prueba del correo

> electrónico en la medida que no se puede probar el envío y recepción del mismo. La equiparación del documento electrónico con el documentos papel que todas las legislaciones de firma digital han adoptado, requiere con relación al documento electrónico contenido en un correo electrónico, un complemento que hace a probar la veracidad de su envió y recepción, convencionalmente convenido y aceptado por las partes.

Como ya lo adelantara, en todos estos casos el ISP debe garantizar la confidencialidad de la información, adoptando las medidas de seguridad necesarias a tal fin.

Fuera de estos supuestos y condiciones, el almacenamiento y conservación del contenido de las comunicaciones viola el derecho a la privacidad, y no pude ser permitido.

III.- Los datos de tráfico relativos a las comunicaciones

Los datos de tráfico no están referidos a los contenidos sino solamente a la duración, fecha, origen y destino, de esas comunicaciones.

La privacidad de la información contenida no está allí en peligro.

Lo que se trata es la conservación de los datos de trafico, entendiendo por tal todos los elementos que hacen a ese correo electrónico en cuanto a su individualización de partida y llegada, fecha, hora y demás datos, que no impliquen la vulneración y conocimiento del texto contenido en el mensaje.

Se discute así si existe obligación por parte de los ISP de conservar durante un período de tiempo relativamente largo los datos de tráfico generados por las comunicaciones establecidas durante la prestación de su servicio, y si con éste almacenamiento y conservación no se está afectando al derecho a la privacidad y confidencialidad de las comunicaciones.

Algunos han dicho que este tipo de conservación de datos es violatorio de principios fundamentales ya que implica una clara interceptación de las comunicaciones, que produce una violación al principio de la privacidad de estas.

Se ha afirmado también que ésta conservación de los datos, constituye asimismo una violación a uno de los principios más importantes en materia de protección de datos personales como es el principio de finalidad, que exige que los datos personales se recojan para finalidades determinadas, explícitas y legítimas y no se traten posteriormente de manera incompatible con ellas.

Sin embargo, creo ello no es así.

Lo único que se conserva son los datos de tráfico pero nunca los de contenido de las comunicaciones, por lo que no existe violación alguna a los principios de privacidad de las comunicaciones y de la protección de los datos personales, ni existe interceptación no permitida de las comunicaciones. Hago presente que incluso cuando se habla de los datos de tráfico de acceso a Internet, no son considerados tales las

informaciones consultadas utilizando Internet, las cuales deben ser consideradas datos de contenido, tal como así lo establece con acierto la última Directiva Europea en su art. 1, apartado 2 in fine.[157]

Muchos son los motivos que aconsejan el establecimiento de la obligación de los ISP de guarda de estos datos de tráfico por algún tiempo, pero me permito resaltar que muchas veces es necesario conocer los datos de tráfico en la investigación de un delito. En los últimos años ha aparecido una nueva forma de delinquir y es utilizando el correo electrónico como medio o como finalidad en si misma del delito. El secuestro, la estafa informática, el terrorismo, el pishing, en fin, numerosas nuevas formas de cometer el delito, en forma creciente se multiplican, siendo el dato del trafico y de localización del correo electrónico un instrumento decisivo necesario y a veces único para la investigación, detección y castigo del delito, y de esta forma para contribuir a la seguridad física de las personas.

Con relación a la obligación de conservación de datos de tráfico por parte de los ISP se ha dicho reiteradamente que tal obligación se justifica ante la necesidad de conservación tanto de las informaciones de tráfico canalizadas a través de ellos, como del número o identificación de los equipos de origen y del destino de la comunicación, tiempo de duración de la conexión, volumen de datos transmitidos, todo ello a los fines que estos elementos puedan servir como prueba en procesos judiciales. Este último requisito se ha considerado una condición necesaria y fundamental y trata de garantizar así los derechos de los usuarios al secreto de los datos de conexión que les afecten.

Diferentes criterios se han aplicado en legislación comparada con relación a cual debe ser el plazo de conservación de los datos, cuales son los datos a retener así como quien debe cargar con el costo de tal obligación. Otro tema importante es la determinación de en que caso y a quien, los datos retenidos deben ser suministrados.

Tratare de analizar estos temas, que creo de singular importancia.

Con relación al *plazo de la conservación*, las legislaciones extranjeras han establecido en general como plazo de conservación obligatoria términos que van desde los seis meses hasta los dos años.

Se ha considerado que establecer plazos mayores incrementa el alto costo que genera tal conservación y por lo tanto hace inconveniente la medida.

Personalmente creo que un plazo razonable y que responde a las necesidades demostradas de los servicios policiales y al mismo tiempo produce costos soportables, es el de un año.

Es interesante resaltar que la Directiva Europea sobre Conservación de Datos de Tráfico, de la cual me referiré mas adelante, acordó que cada estado miembro debe establecer el plazo de conservación de los datos de trafico dentro de un período

---

[157] "…No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".

mínimo de 6 meses y máximo de 24 meses a partir de la fecha de la comunicación, si bien también se establece que los estados que lo soliciten podrán retener los datos por un plazo mayor.

Destaco que la propuesta de Directiva en su primer redacción, luego no aprobada, había establecido una distinción entre los datos del tráfico telefónico en donde el plazo de retención era de un año, y los datos de tráfico en Internet en donde el plazo era de seis meses.

Con respecto a *cuales datos deben retenerse*, considero que la legislación debe tratar de limitar los datos a retener y almacenar a los estrictamente necesarios para la individualización, y que debe cuidarse especialmente que a través de ellos no sea posible acceder a los datos de contenido. Para eso es importante el establecimiento de medidas de seguridad adecuadas que limiten el acceso a los datos y que aseguren también la seguridad de los mismos. En efecto es necesario asegurar una seguridad en su doble aspecto: Seguridad que solo en determinadas circunstancias y por determinadas personas se tenga el acceso y utilización de los datos retenidos, y Seguridad en las bases de datos que contengan los datos, a fin de evitar su violación por terceros, lo que conlleva a la existencia de medidas técnicas y organizativas adecuadas.

Con relación al *costo que esta obligación genera para los Proveedores de los Servicios*, se ha afirmado que estos costos son muy onerosos para los proveedores de los servicios, y que entonces debe encontrarse alguna forma en la cual estos ISP no carguen con tales costos.

Al respecto es interesante ver como en el texto inicial de la Propuesta de nueva Directiva Europea [158], se establecía que los estados miembros debían asegurar que los proveedores de servicios de comunicaciones debían ser reembolsados por los costes adicionales que demostrasen haber incurrido para cumplir las obligaciones de conservación impuestas.

Tal compensación había sido incluida en el texto por considerarse que la conservación de datos generaría evidentemente una serie de costos adicionales de consideración para los proveedores de los servicios, y ya que los beneficios, en términos de la seguridad pública, estaban dirigidos a la sociedad en su conjunto, debían ser los estados quienes afrontasen tal costo.

Esta norma no fue incluida en el texto final recientemente aprobado, lo que creo es un aspecto criticable.

Con relación a la *determinación de en que casos y a quien, los datos retenidos deben ser suministrados*, creo interesante lo establecido en la Directiva Europea que limita el destino de los datos retenidos a fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada estado. Disponiendo también que los datos solo se proporcionaran a las autoridades

[158] Art. 10 del texto inicial de la Propuesta de nueva Directiva Europea , que fuera aprobado por el Parlamento Europeo en año 2005

nacionales competentes en casos específicos y de conformidad con la legislación nacional.

Creo que la formula empleada es correcta ya que deja a la decisión de los estados la determinación expresa dentro de un doble marco: *"investigación, detección y enjuiciamiento"*, y *"delitos graves"*.

Seria interesante entonces, en los casos concretos, que las legislaciones establecieran expresa y claramente cuales son los delitos graves que validan la entrega de estos datos y que autoridades judiciales son las que pueden recabar los datos.

IV.- El tratamiento del tema en la Unión Europea y en la Legislación Española

En Europa, tanto la *Directiva General 95/46/EC* del Parlamento Europeo y del Consejo 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, como la *Directiva 97/66/EC* relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones, no aceptaban en forma alguna el almacenamiento de datos de tráfico de las comunicaciones, consagrando el principio de la protección del derecho a la vida privada, precisando como obligación de los estados miembros la protección del secreto de las comunicaciones por medio de normativas nacionales que garanticen la confidencialidad de las comunicaciones efectuadas a través de redes públicas de telecomunicaciones o de servicios de telecomunicaciones accesibles al público.

En 2001, incluso se aprobó el borrador del proyecto de nueva Directiva sobre privacidad en las comunicaciones, el que tampoco contenía ninguna disposición de este tipo, sino que por el contrario se pronunciaba en contra de la posibilidad que dicha información sobre los ciudadanos europeos se retuviera y se pusiera a disposición de las fuerzas de seguridad. Se expresaba en los considerandos *"el Parlamento Europeo pretende bloquear los esfuerzos de algunos estados de poner a sus ciudadanos bajo sospecha y vigilancia generalizada, siguiendo el ejemplo de Echelon"*.

Sin embargo los atentados del 11 de Septiembre de 2001, hicieron repensar muchas ideas y aceptar, en miras a la seguridad, la restricción de ciertos derechos.

Fue así como el 12 de julio de 2002 se aprobó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.[159]

[159] A esta Directiva se la conoce como Directiva sobre la privacidad y las comunicaciones electrónicas [Diario Oficial L 201 de 31 de julio de 2002] y reemplazo a la Directiva 97/66/CE.

Allí se *"faculta a los Estados para establecer excepciones a las normas de destrucción de datos de tráfico (...) para proteger la seguridad y defensa nacional".* Concretamente, el artículo 15 de esta Directiva autorizó a los estados miembros a retener por ciertos períodos datos de tráfico con la finalidad de prevenir e investigar delitos.

A partir de entonces varios estados europeos dictaron normativas que contemplan la conservación de datos, normativas estas que varían sustancialmente en sus contenidos y alcances.

Estas diferencias motivaron la necesidad de dictar una nueva directiva a fin de tratar de unificar la legislación de los estados de la UE.

En Mayo de 2004 el Consejo de Europa emitió una declaración sobre la lucha contra el terrorismo en la que se estableció la necesidad de dictar normas comunitarias que garantizasen la disponibilidad de los datos de tráfico con fines antiterroristas.

Fue por todo ello que el Consejo de Europa decidió encarar el estudio de una nueva Directiva sobre la conservación de datos de tráfico, que modificase la Directiva 2002/58/CE, con vistas a su adopción durante el año 2005.

La propuesta de esta nueva Directiva fue presentada el 21.9.2005, aprobada por el Parlamento Europeo en Bruselas el 14.12.2005 y elevada al Consejo de Ministros de Justicia e Interior de los veinticinco, quien luego de efectuarle varias modificaciones, le dió final aprobación el 15 de Marzo de 2006.

Esta nueva *Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre Conservación de Datos de Tráfico y de Localización Telefónicos y de Comunicaciones Electrónicas* [160] , obliga a los operadores de telecomunicaciones telefónicas y de Internet a almacenar los datos de tráfico y de localización de las comunicaciones durante un período de entre 6 y 24 meses. [161]

El objetivo de la Directiva es tratar de armonizar las legislaciones de los estados miembros de la Unión Europea, relacionadas con la obligación de los Proveedores de los Servicios de Comunicaciones, de conservación de determinados datos de tráfico, a fin de que los mismos estén disponibles a los fines de la investigación, detección y enjuiciamiento de delitos graves, según estén estos definidos en la legislación nacional

---

[160] Directiva 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 (Publicada en el Diario Oficial de la Unión Europea del 13.4.2006)

[161] El tema lo he tratado con mayor amplitud en mi trabajo: "Nueva Directiva de la Unión Europea sobre Conservación de Datos de Tráfico", publicado por la Revista de Contratación Electrónica de la Universidad Complutense de Madrid. Nº 68 – Junio de 2006

de cada estado miembro, principalmente los relacionadas con el terrorismo y el crimen organizado.

Conforme lo dispone la Directiva, los datos a retener serán los datos de tráfico y de localización sobre personas físicas y jurídicas, y los datos relacionados necesarios para identificar al abonado o al usuario registrado, detallando en el art. 5 cuales son esos datos de trafico y de localización y datos relacionados que deben retenerse.

Expresamente, la Directiva establece que no se aplicará *"al contenido de las comunicaciones electrónicas".*

En el artículo séptimo se establece también la obligación de los estados de velar por que los proveedores de servicios de comunicaciones cumplan, respecto de los datos conservados, como mínimo, los siguientes principios de seguridad de los datos:

a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;
b) los datos estarán sujetos a las medidas tecnológicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, perdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;
c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas; y
d) Los datos, excepto los que hayan sido accesible y se hayan conservado, se destruirán al término del período de conservación.

Es interesante resaltar que poco después de aprobada la Directiva, el Grupo de Autoridades Europeas de Protección de Datos (conocido como GT29) adoptó el dictamen 3/2006 en el que reitera una serie de reservas que había efectuado con anterioridad a la aprobación de la misma, y a fin de una mayor garantía de los individuos propuso una transposición uniforme de la Directiva en todos los países Europeos, respetando el máximo nivel posible de protección de los datos.

En concreto este dictamen requiere un respeto exquisito al *principio de finalidad* en la retención, lo que implica la necesidad de una definición clara y precisa del concepto "delito grave" prohibiéndose o restringiéndose seriamente cualquier tratamiento posterior ; la necesidad de *restringir el acceso* únicamente a aquellas fuerzas de seguridad específicamente designadas públicamente así como la necesidad de que los accesos de las mismas queden registrados y a disposición de las autoridades de control; la *minimización de los datos guardados; la prohibición de la utilización de técnicas de "minería de datos" a gran escala* sobre los datos retenidos; la necesidad de que los *accesos sean autorizados caso por caso* por las autoridades judiciales; la *prohibición de que los datos retenidos sean utilizados por los proveedores de servicios de comunicaciones para sus fines* y en su propio beneficio; la *separación física entre los sistemas* en los que se almacenan los datos retenidos y los que se

utilizan habitualmente en la actividad comercial y la definición e implantación de *medidas de seguridad adecuadas*.

En España, la ley 25 del 18 de Octubre de 2007 [162], dictada como consecuencia de la obligación de incorporar a la legislación española la directiva 2006/24/CE, regula ampliamente el tema, estableciendo que los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones deben retener los datos de conexión y tráfico por el termino de doce meses computados desde la fecha en que se haya producido la comunicación.

Se establece también expresamente en el art. 1 de la ley que la misma *"se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado."* Pero agregando que *"Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas"*

La ley española precisa los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

V.- La situación en Estados Unidos

En EE.UU. en 1994 fue aprobada la "Communications Assistance for Law Enforcement Act", pero la misma se aplica solamente a las empresas de telecomunicaciones, a las que obliga 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

Esta normativa se entendió que no era de aplicación a los Proveedores de Servicio de Internet.

Pero poco tiempo después de los atentados del 11 de Septiembre de 2001, el Congreso de EE.UU. aprobó la H.R.3162, llamada Acta Patriótica que otorga amplios poderes especiales al FBI y a las agencias de inteligencia de EE.UU. para poder monitorear el trafico de correo electrónico.

VI.- El Convenio de Budapest

---

[162] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Es importante destacar que el Convenio sobre Cibercriminalidad (ETS 185) suscripto en Budapest el 23 de Noviembre de 2001, y que fue elaborado por el Consejo de Europa conjuntamente con EE.UU., Canadá, Japón y Sud Africa, y abierto para las firmas en Noviembre de 2001, (a la fecha firmado por 43 estados), pretende homogenizar las leyes penales sobre criminalidad en el ciberespacio para proteger los derechos de los ciudadanos y perseguir la delincuencia entre países.

Este convenlo de indudable trascendencia internacional, dispone la creación como figuras penales de una serie de conductas, estableciendo: "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal..."

Pero dispone también la adopción de medidas procesales, de conservación de datos de tráfico, sobre extradición, colaboración entre estados, etc.

De esta forma los estados que han adherido a Budapest están obligados entre otras cosas a establecer un sistema de conservación de datos de tráfico, como una medida más en la lucha contra la delincuencia informática-

VII.- En otros países

En Inglaterra, pese a una gran oposición de numerosas organizaciones, fue aprobada The Regulations of Investigatory Powers (RIPA), que se aplica a los proveedores de servicio de Internet y obliga a retener datos de tráfico e incluso obliga a los proveedores de telecomunicaciones que usan encriptado, a entregar a pedido oficial, las claves del mismo para poder acceder a la comunicación codificada. También the Anti-Terrorism Crime and Security Act Part 11, lo permite a los fines de la seguridad nacional o la lucha contra el delito

En Italia, el nuevo Código de Protección de Datos Personales vigente desde enero de 2004, admite la conservación de los datos de tráfico por el término de 30 meses.

En otros países se están estudiando normativas al respecto, tal los casos de:

Austria en donde se esta considerando incluir esta obligación en el Proyecto de futura ley de Comunicaciones.

En Bélgica la Computer Crime Act (28 Nov. 2000) admite la conservación para la investigación criminal pero la norma no se encuentra aun reglamentada.

En Dinamarca la Sec.786 de la ley de Administración de Justicia, admite la obligación para la investigación policial por el término de un año, pero no se encuentra aun vigente pues debe ser reglamentada.

En Finlandia existe una fuerte corriente de apoyo a su implementación por un periodo de dos años, pero aun no ha sido establecida.

En Francia se admite a los efectos de la investigación criminal por un año pero con importantes limitaciones.

En Grecia existe una tendencia a aceptarla por un año.

En Suecia es un tema actual de discusión, y se sugiere 12 meses como mínimo de la obligación.

No puedo terminar este punto sin señalar que, el 28 de abril de 2004, el Reino Unido, Francia, Irlanda y Suecia, presentaron una propuesta, conocida como "Propuesta de Decisión Marco sobre Retención de Datos de Tráfico de Comunicaciones Electrónica", que pretendía armonizar en los Estados Europeos normas mínimas sobre la retención de datos de tráfico, dada la importancia que se considera que dichos datos tienen hoy en día en la investigación de delitos graves, incluido el terrorismo.

VIII.- En la República Argentina

En la Argentina no existía ninguna normativa relativa a la conservación de los datos de tráfico por parte de las empresas prestadoras de servicios de comunicaciones, sino que solamente algunos proyectos de ley contemplaban estas situaciones.

Tal el caso del Proyecto de Ley Nº 64/02 de delitos informáticos que tuvo durante el año 2003 media aprobación legislativa, pero que finalmente no ha prosperado. En la versión original de este proyecto no se contemplaba ésta situación, pero el posterior dictamen de la Comisión de Asuntos Penales del Senado del 21.11.2002 había propuesto la introducción, como nuevo art. 7, de la obligación de los ISP de conservar los datos de tráfico durante dos años. [163]

[163] El texto propuesto expresa: Dictamen Comisión: "Artículo 7: Deber de conservación de datos. Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos, deberán conservar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de los servicios que suministran, por un período de dos años. Los datos se conservarán para su utilización en el

Sin perjuicio de este antecedente a fines del año 2003 el Parlamento Argentino sancionó la ley 25873 que incorporó a la ley Nacional de Telecomunicaciones, tres artículos, que fundamentalmente regulan dos aspectos relacionados a las telecomunicaciones:

El primer aspecto de la normativa autoriza la intercepción de las comunicaciones telefónicas o por Internet, incluido los contenidos, pero supeditando esta intercepción a la previa orden judicial o del Ministerio Público.

Se reafirmó así lo que ya dispone la ley 25520 de Inteligencia Nacional en su art. 18 que establece que *"cuando en el desarrollo de las actividades de inteligencia o contrainteligencia sea necesario realizar interceptaciones o captaciones de comunicaciones privadas de cualquier tipo, la Secretaría de Inteligencia deberá solicitar la pertinente autorización judicial"*

De esta forma se trata de evitar las intercepciones clandestinas o dispuestas sin orden judicial que configuran afrentas reales y concretas al derecho a la privacidad de los individuos.

El segundo aspecto de la ley 25873 establece la obligación de conservación de los datos de tráfico de las comunicaciones por parte de las empresas prestadoras de los servicios y por el término de diez años, con la finalidad de su consulta por parte del Poder Judicial.

Esta exigencia de conservación de los datos de tráfico ya se venía realizando por las empresas telefónicas a efectos de la facturación de los servicios, pero no ocurría así con las proveedores de Servicios de Internet que no conservaban los datos de tráfico del correo electrónico.

Esta conservación de datos, reitero se refiere únicamente a los datos de tráfico, pero nunca a la conservación de los contenidos.

Quizás el plazo de diez años, establecido en la normativa argentina, fue demasiado extenso, ya que en general se ha estimado que el término correcto debe ser de 1 o 2 años.

---

marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Público que los requiera.

Los datos que deberán conservar serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información o para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio. En ningún caso, la obligación de conservación de datos afectará la confidencialidad de las comunicaciones, debiendo adoptar las medidas de seguridad apropiadas para evitar su utilización para otros fines no previstos en esta ley, su pérdida o alteración y el acceso no autorizado a los mismos".

El 8 de Noviembre de 2004 fue reglamentada la ley 25873 con el dictado del Decreto 1563.

Personalmente entiendo que tal reglamentación no alteró el contenido de la ley, si bien su falta de claridad provocó una aguda polémica en la Argentina, en donde muchos, incluidos los medios periodísticos, informaron erróneamente que tal decreto y la ley que reglamentaba, permitían la conservación de los datos de contenido por el término de diez años, sin ningún requisito.

Esto no es así, ya que como antes expliqué son dos situaciones distintas, y la conservación de los datos por 10 años se refiere a los datos únicamente de tráfico.

Como consecuencia de esta polémica el Gobierno argentino, dictó el Decreto 357/05 que suspendió la aplicación del Decreto 1563.

Por su parte la Justicia Argentina estableció la inconstitucionalidad de la ley 25873 y del Decreto 1563/04 en un amparo planteado por CABASE [164], y en el caso Halabi [165], causas ambas tramitadas ante la Justicia Contencioso Administrativo de la Capital Federal. Recientemente, la Corte Suprema de Justicia de la Nación, ha confirmado la declaración de inconstitucionalidad que había sido dictada en el Caso Halabi.

Personalmente creo que tanto el Decreto 357/05 como los fallos judiciales son equivocados y privan a la Argentina de una normativa, que pese a algunas deficiencias que pudieron ser corregidas, era útil y acorde a las modernas legislaciones, y que lejos de afectar la privacidad, brindaba un importante instrumento en la lucha contra la delincuencia.

Solo me cabe para concluir deseando que en un futuro cercano se proyecte una normativa de conservación de datos de tráfico, que recoja los antecedentes internacionales en cuanto a la finalidad y plazo, y que no contenga los errores de la normativa argentina que fue suspendida y declarada inconstitucional.

---

[164] "Cámara Argentina de Bases de Datos y Servicios en Línea c/Estado Nacional Ley 25873 Dto.1563/04 s/amparo Ley 16986" – Sentencia del Juzgado Nº 6 en lo Contencioso Administrativo Federal del 13.05.2005, confirmada por la Sala I de la Cámara el 11.7.2006.

[165] "Halabi, Ernesto v. PEN – ley 25873 Dto. 1563/04 s/ amparo ley 16986" – Sentencia confirmada por la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal – Sala 2ª el 29.11.2005.