

ticular. Por el contrario, lo que entra en juego es el derecho a la privacidad en el ámbito de las telecomunicaciones. Ello, por definición, presupone la interacción con otros interlocutores, cuya ausencia de protección –por ser ajenos al juicio– derivaría, necesariamente, en el fracaso de la protección al amparista mismo.

Desde este punto de vista, la necesidad de protección invocada no podría ser restringida a la “propia” esfera de privacidad. En consecuencia, al no haber sido invocada por la recurrente razón o argumento alguno acerca de cómo sería posible satisfacer la pretensión del reclamante manteniendo la injerencia a la privacidad de terceros ajenos al pleito, pero potenciales interlocutores, el recurso extraordinario presenta falencias en su fun-

damentación de entidad suficiente como para impedir su procedencia.

11) Que, por lo mismo, frente a la ausencia de argumentos relativos a cómo podrían ser restringidos los efectos de la sentencia al caso particular sin vulnerar la protección de la privacidad pretendida, no se advierte relación directa e inmediata entre lo resuelto en estos actuados y la interpretación restrictiva de los alcances del art. 43, CN., propuesta por la recurrente (conf., entre muchos otros, Fallos 329:2060, 329 y 330:4399).

Por ello, oída la procuradora fiscal, se declara improcedente el recurso extraordinario. Sin costas en atención a la naturaleza de la cuestión debatida. Hágase saber, y oportunamente, devuélvase.

## La obtención de pruebas informáticas en el proceso penal a partir del fallo de la Corte Suprema en el caso “Halabi”: ¿necesitamos una reforma del Código Procesal Penal?

Por Pablo A. Palazzi

**SUMARIO:** I. Plataforma fáctica.– II. La decisión de primera y segunda instancia.– III. Un nuevo estándar para analizar las afectaciones a la privacidad: a) *Un nuevo estándar para el derecho a la privacidad*; b) *La privacidad como bien colectivo*; c) *¿Cómo debería ser una futura Ley de Datos de Tráfico para ser constitucional?*.– IV. Conclusión

### I. PLATAFORMA FÁCTICA

El 24/2/2009 la Corte Sup. dictó sentencia en el caso “Halabi v. Estado Nacional” (1). Se trataba de una acción de amparo reclamando que se declare la inconstitucionalidad de la Ley de Datos de Tráfico –ley 25873 y su reglamentación–, en virtud de considerar que sus disposiciones vulneraban las garantías establecidas en los arts. 18 y 19, CN., en cuanto autorizan la intervención de las comunicaciones telefónicas y por internet sin que una ley determine “en qué casos y con qué justificativos” se podrían intervenir (2). El actor alegó que esa intromisión constituye una violación de sus derechos a la privacidad y a la intimidad, en su condición de usuario. Su demanda también se basó en el privilegio de

confidencialidad que, como abogado, ostenta en las comunicaciones con sus clientes.

La norma, aprobada a fines del año 2003, sólo tenía tres artículos y establecía la obligación de empresas de telecomunicaciones de almacenar por diez años datos de tráfico y de usuarios, con la finalidad de poder utilizarlos con fines probatorios en procesos judiciales. Pero los obligaba a tener recursos humanos y tecnológicos necesarios para captar y derivar esas comunicaciones y a pagar los costos derivados de tal actividad. La ley fue reglamentada en noviembre de 2004 (decreto 1563/2004); sin embargo, la controversia mediática que originó hizo que el Poder Ejecutivo suspendiera su aplicación (3).

(1) Corte Sup., 24/2/2009, “Halabi, Ernesto v. Estado Nacional - Poder Ejecutivo”.

(2) El actor se agraviaba de que la referida intervención importa una violación de sus derechos a la privacidad y a la intimidad, y además pone en serio riesgo el “secreto profesional” que como letrado se ve obligado a guardar y garantizar (arts. 6, inc. f, 7, inc. c y 21, inc. j, ley 23187). Su pretensión no se circunscribe a procurar una tutela para sus propios intereses, sino que, por la índole de los derechos en juego, es representativa de los intereses de todos los usuarios de los servicios de telecomunicaciones, como así también de todos los abogados.

(3) La problemática es mucho más compleja. Ver un resumen más completo en nuestras notas tituladas “La regulación de los datos de tráfico en la Argentina: comentario a la ley 25873”, en JA 2004-II-1346, y “La suspensión de la reglamentación de la Ley sobre Datos de Tráfico en materia de telecomunicaciones”, JA 2005-II-1349 (JA del 25/5/2005, Supl. Esp. de Derecho Informático).

## Derecho Penal Informático

El actor no fue la única persona que accionó. También lo hizo CABASe (4) –la Cámara que nuclea a empresas de telecomunicaciones–, que ganó en primera instancia pero cuya decisión fue revocada por otra sala de la Cámara de Apelaciones.

### II. LA DECISIÓN DE PRIMERA Y SEGUNDA INSTANCIA

Tanto en primera como en segunda instancia se declaró la inconstitucionalidad de la norma cuestionada.

En primera instancia (5) los fundamentos fueron los siguientes: a) no existió un debate legislativo suficiente previo al dictado de la ley, la cual carece de motivación y fundamentación apropiada; b) del derecho comparado surge que diversas legislaciones extranjeras tomaron precauciones para no incurrir en violaciones al derecho a la intimidad –por ejemplo, limitaron el tiempo de guarda de los datos– que no fueron consideradas en este proyecto; c) las normas exhiben gran vaguedad (a partir de sus previsiones no queda claro en qué medida pueden las prestatarías captar el contenido de las comunicaciones sin la debida autorización judicial); d) están redactadas de tal manera que crean el riesgo de que los datos captados sean utilizados para fines distintos de los que ella prevé; e) el Poder Ejecutivo se excedió en la reglamentación de la ley al dictar el decreto 1.563/2004.

La sala 2ª de la C. Nac. Cont. Adm. Fed., a su turno, confirmó dicho pronunciamiento (6). Luego de advertir que el recurso de apelación del Estado Nacional exhibía defectos técnicos que conducían a declararlo desierto, estimó que, por la trascendencia de la cuestión debatida, correspondía tratar los argumentos desarrollados en defensa de las normas impugnadas.

En primer lugar aclaró que la pretensión no se había tornado abstracta, pues la ley cuestionada seguía vigente por el hecho de que el decreto 1.563/2004 que la reglamentó sólo había sido suspendido mediante el decreto 357/2005, sin que hubiese sido derogado. En segundo término, precisó que el planteo articulado no era meramente consultivo sino que existía un interés jurídico concreto en cabeza del actor como usuario de distintos servicios de telecomunicaciones y en su carácter de abogado. Respecto del fondo del asunto, hizo suyos los argumentos desarrollados por la jueza de primera instancia. Con citas de jurisprudencia nacional y extranjera añadió consideraciones ge-

nerales sobre el derecho a la intimidad y a la inviolabilidad de la correspondencia, concluyendo que éstos debían primar en situaciones como la que se analizaba, más allá de que el objetivo general de las normas impugnadas hubiera sido el de *combatir el flagelo de la delincuencia*.

Finalmente, concluyó que la legitimación del actor "no excluía la incidencia colectiva de la afectación a la luz del párr. 2º del art. 43, CN.", por lo que la sentencia dictada en tales condiciones debía "...aprovechar a todos los usuarios que no han participado en el juicio". La Cámara dejó así abierta la puerta para que la Corte Suprema introdujera las acciones de clase en el Derecho argentino.

### III. UN NUEVO ESTÁNDAR PARA ANALIZAR LAS AFECTACIONES A LA PRIVACIDAD

El fallo trata dos temas claramente diferenciados. El primero es el relativo a las acciones de clase (7). El segundo es el aspecto del derecho a la privacidad que la Corte aborda, pese a que había quedado firme en segunda instancia. El tribunal dice dar sólo una "ligera mirada" sobre el tema; sin embargo, entendemos que en materia de privacidad el fallo de la Corte es muy importante, por los motivos que explicaremos.

La Corte convalida la inconstitucionalidad de la ley 25873, no sólo por los fundamentos dados por la Cámara de Apelaciones sino también por los propios que añade en los consid. 22 a 27.

Nos parece muy positivo que la Corte ampare la privacidad y que lo haga de manera tan tajante, incluso cuando procesalmente no tenía que hacerlo (la cuestión había quedado firme en la instancia anterior). Es importante semejante postura de la Corte Suprema por lo invasivas que resultan hoy en día las tecnologías de la información, y porque seguramente a futuro nos encontraremos con planteos similares. A mayores peligros, la respuesta de los tribunales debe ser siempre reforzar las garantías constitucionales. La ley 25873, al ordenar la recopilación indiscriminada de datos de tráfico por una década, ponía bajo sospecha y vigilancia a todos los ciudadanos argentinos, y a los extranjeros que se comunicaran con éstos (8). Por supuesto, el almacenamiento de tales datos servía para otros intereses públicos importantes, como el de preordenar prueba informática en procesos judiciales y facilitar su adquisición.

(4) En los autos "Cámara Argentina de Bases de Datos y Servicios en Línea v. Estado Nacional s/amparo" la C. Nac. Cont. Adm. Fed., sala 1ª, con fecha 11/7/2006, se expidió sosteniendo la constitucionalidad de la ley 25873. Para una descripción de este fallo y sus fundamentos ver Calonje, Diego y Pacheco Barassi, Leandro, "Actualidad en Contencioso Administrativo Federal 2/2006", JA 2006-IV-755.

(5) LL 2005-F-318.

(6) C. Nac. Cont. Adm. Fed., sala 2ª, 29/11/2005, LL 2006-B-397; y JA 2006-II-363, con comentario de Lipskier, Natalia C. y Olivera, Noemí L., "Los usuarios de internet y los ISP. ¿Será necesaria una acción de amparo para el cumplimiento de los arts. 45 bis, ter y quater, ley 19798?"

(7) Este comentario no analiza la primera cuestión, salvo en lo que esté relacionado con el derecho a la privacidad y su incidencia en la obtención de pruebas en el proceso penal.

(8) Palazzi, "La regulación de los datos..." cit.

la inviolabilidad de éstos debía ser privada, más allá de las medidas de seguridad que hubiera.

En el actor "no se refiere a la luz del fallo dictado por la sentencia dictada por la Corte Suprema in-terveniente". La Cámara de Apelaciones en lo Criminal y Correccional confirmó el fallo de la Corte Suprema in-terveniente.

LA S

reñidos. El primero (7). El segundo fallo que la Corte emitió en segunda instancia sobre la "mirada" sobre la privacidad en materia de comunicaciones, por los

de la ley 25873, la Cámara de Apelaciones que añade en los

compara la privacidad de los datos cuando se produce la interceptación de comunicaciones. La Corte en su fallo de mayoría consideró que la interceptación de comunicaciones es una medida de seguridad que no viola la privacidad de los datos. La Corte en su fallo de mayoría consideró que la interceptación de comunicaciones es una medida de seguridad que no viola la privacidad de los datos. La Corte en su fallo de mayoría consideró que la interceptación de comunicaciones es una medida de seguridad que no viola la privacidad de los datos.

Vac. Cont. Adm. Fed., confirmación de este fallo y el fallo Federal 2/2006", JA

er, Natalia C. y Olivera, de los arts. 45 bis, ter-za y su incidencia en

Lo resuelto por la Corte en esta materia motiva tres comentarios sobre: a) el test que la Corte utiliza para analizar la constitucionalidad de normas restrictivas de privacidad; b) la privacidad como bien colectivo; y c) la futura reglamentación que debería dictar el Congreso a la luz del estándar enunciado y de las experiencias del derecho comparado.

a) *Un nuevo estándar para el derecho a la privacidad*

En primer lugar la Corte reafirma la protección del derecho a la privacidad en las telecomunicaciones como un derecho constitucional casi absoluto: sólo con orden judicial se puede intervenir una comunicación o su registro (se cita el art. 236, párr. 2º, CPPN, y la Ley de Telecomunicaciones 19798). Esta afirmación no se limita a una mera enunciación de principios ya reconocidos en la Constitución. La Corte fija un claro estándar para saber cuándo una ley que permite una interceptación es constitucional.

En segundo lugar la Corte califica al almacenamiento de los datos personales requerido por las normas cuestionadas como una "restricción que afecta a una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad". Nótese cómo la Corte pasa de analizar las comunicaciones dinámicas (a las que hacen referencia los arts. 236, párr. 1º, y 18, Ley de Telecomunicaciones 19798), que son las que deben ser "interceptadas", a la comunicación almacenada que ya tuvo lugar y que se transforma en un dato personal (regulado por la ley 25326), que son las que pueden ser "accedidas". Dentro de estos últimos encontramos al e-mail almacenado en un servidor, un chat, o un voice mail, o los logs de conexión a un servidor. Todos son datos personales (9). El problema en este caso, entonces, era con datos personales que dicen algo de una persona. Datos que se podrían almacenar por una década sin un debido control. Hay que aclarar, para que el lector entienda bien el problema, que estos datos se seguirán almacenando en forma rutinaria por un cierto período de tiempo. La razón de ello es que son necesarios para efectuar las comunicaciones, o para facturarlas; por ello, de hecho, las empresas de comunicaciones seguirán recopilando esta información.

En tercer lugar, y claramente relacionado con el punto anterior, la Corte demuestra su preocupación por el tratamiento de datos personales por parte del Estado. Señala

que los datos que se recopilarían no estaban amparados adecuadamente por no contar con un régimen legal especial que regule el tratamiento automatizado de datos personales ("...las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales"). Aunque la ley 25326 estaba y está vigente, la Corte pone énfasis en este aspecto. No debemos olvidar que la ley 25326 es otra esfera más del derecho a la privacidad amparado por los arts. 18 y 19, CN. (10). La interacción entre el derecho tradicional a la privacidad y el dominio de los datos personales aún tiene mucho camino que recorrer, pero es saludable este primer paso.

Indudablemente, aún falta mucho más para evaluar el impacto que tendrá la consideración del dato personal (11) —y sus reglas de usos—, pero dado que todo proceso judicial busca indagar la verdad sobre un hecho (su existencia, sus pruebas, sus autores), todo redundará en la recopilación de datos de las más diversas fuentes. Sobre todo en delitos cometidos a través de internet, los rastros que quedan son numerosos. Sólo se trata de saber cómo encontrarlos e interpretarlos (aquí un perito informático idóneo, tanto oficial como de parte, es irremplazable). En un mundo cada vez más dominado por tecnología y bases de datos, estos datos mostrarán el camino al juez. Pero su obtención debe hacerse siempre respetando las garantías constitucionales (12).

El estándar que define la Corte en el consid. 25 para evaluar cuándo se puede restringir válidamente la inviolabilidad de la correspondencia es el siguiente: a) que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto; y d) que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, agrega la Corte, los "fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes".

¿De dónde sale este estándar? Es el que tres votos concurrentes habían propuesto en el consid. 11 del caso "Dessy" (13). En "Dessy" un interno cuestionó y obtuvo la

(9) El Grupo de Trabajo del Art. 29 de la UE sostuvo en numerosas oportunidades que la dirección IP es un dato personal.

(10) Sobre las distintas esferas del derecho a la privacidad ver Palazzi, "El hábeas data y el consentimiento para el tratamiento de datos personales", JA 1999-IV-399.

(11) Ha investigado el tema exhaustivamente en su monografía Fernández Rodríguez, José J., "Secreto e intervención de las comunicaciones en internet", Ed. Thomson-Civitas, Madrid, 2004.

(12) Ver reflexiones sobre este tema en Palazzi, Pablo, "Data protection and fight against crime", publicitado en Pouillet, Yves, Peres Azinari, Verónica y Palazzi, Pablo, "Défis du droit à la protection de la vie privée [Challenges of privacy and data protection law]", Bruselas, Cahiers du Centre de Recherches Informatique et Droit, n. 31, Bruyant, 2008, p. 441. Habrá versión en castellano de esta obra a publicarse en Buenos Aires en el año 2009.

(13) Corte Sup., 19/10/1995, "Dessy, Gustavo G. s/hábeas corpus", Fallos 318:1894, JA 1995-IV-251.

## Derecho Penal Informático

declaración de inconstitucionalidad de una reglamentación penitenciaria que permitía la apertura de correspondencia que los detenidos enviaban a terceros. La norma cuestionada en ese caso era sumamente vaga y discrecional, como lo señala la mayoría en el consid. 9 de "Dessy". Ahora ese estándar hizo mayoría en "Halabi". Es muy positivo que la Corte fije estándares para analizar leyes. Más positivo aún será que en el futuro los respete y los siga aplicando.

En el consid. 26 la Corte aplica estos recaudos al caso concreto. Primero sostiene que el fallo de Cámara se ajusta a ese estándar enunciado. Luego de recordar la aplicación de criterios de interpretación restrictivos en el examen de las interceptaciones de las comunicaciones personales, señala: "...es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos".

La Corte entendió que la falta de precisión de la norma tenía como efecto crear un filtro en el cual quedan atrapadas todas las comunicaciones (añadimos: de todo tipo) entre toda clase de sujetos (añadimos: de futuros imputados o demandados, pero también de inocentes y no culpables).

En especial el fallo claramente señala que "el tratamiento del tráfico de información de internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos". Veamos un ejemplo. Si un proveedor de acceso a internet guarda como dato de tráfico el hecho de que su usuario tuvo acceso a un sitio de internet determinado, el contenido del sitio está implícito en un dato de tráfico, pero ese también será un dato de contenido en la medida de que indica qué estuvo leyendo el usuario (incluso podría ser un dato sensible). En pocas palabras, la ley 25873 permitía almacenar no sólo datos de tráfico sino también, en el supuesto señalado, datos de contenido sin que exista la orden judicial que manda la Constitución. Con esto quedaba claramente demostrada la inconstitucionalidad de la norma (al menos en estos supuestos). Se puede deducir que en estos supuestos el dato de tráfico equivaldría a los de contenido. O bien se

podría asumir que todos los datos de tráfico, al formar parte de la comunicación, también son contenido (en este caso no se entendería la distinción que hace la Corte Suprema). La Corte, lamentablemente, se detiene aquí. No entra a diferenciar si interceptar datos de tráfico solamente podría equipararse a los de contenido en otros supuestos (por ej., comunicación telefónica fija o por celular, SMS en celulares o correo electrónico), y si es o no constitucional hacerlo. Hay que admitir—como ya señalamos—que en la práctica los ISP y las telefónicas tratan estos datos como si formaran parte de la comunicación, pues exigen en todo momento una orden judicial para su obtención.

Por eso la Corte concluye: "...resulta inadmisibles que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos". Se entiende que esta afirmación se da en el contexto de la ley cuestionada, donde, ya sea por orden de juez o de un fiscal (art. 1, ley 25873), se podría acceder a ese cúmulo de información por una década.

### b) La privacidad como bien colectivo

Respecto de lo colectivo que encerraba el presente caso no podemos menos que compartir lo decidido (tanto por la mayoría como por los tres votos en disidencia parcial). Tal visión arroja una nueva mirada sobre la caracterización del derecho a la privacidad, que siempre fue visto como un derecho individual y personalísimo, limitado a la faz interna del individuo. Esto más que nada nos recuerda la complejidad, que siempre fue subrayada por tratadistas y fallos, de la definición del derecho a la vida privada. Es un derecho que va mutando frente a las nuevas tecnologías y se adapta con nuevas respuestas, como lo demuestra la evolución de un derecho en su faz negativa (el derecho a la vida privada y a excluir a terceros de esa esfera) a la expresión positiva del mismo derecho (la protección de datos y hábeas data, y el acceso a los datos personales).

Pero lo colectivo del derecho a la privacidad no sólo se afecta con normas sino también con hechos concretos por parte del sector privado: los nuevos diseños de políticas empresariales. Cada vez más los cambios mínimos realizados a cualquier arquitectura de internet afectan a millones de individuos y trascienden las fronteras y las regulaciones locales. Por ejemplo, si Google decide cambiar su política de privacidad (14), millones de logs pueden quedar en el olvido o ser entregados a las autoridades o

(14) En efecto, a modo de ejemplo señalamos que Google vinculó durante cierto tiempo los links de las búsquedas a una "cookie" (un archivo de texto conteniendo caracteres únicos para identificar a un sujeto). Google transmite esta cookie cuando un usuario se conecta por primera vez para identificar al usuario con su servidor. La cookie quedará instalada en el ordenador del usuario hasta su vencimiento o cuando sea borrada (algo que muy pocos saben hacer). La fecha de vigencia decidida por Google era el año 2038, lo que concitó críticas de la prensa, sobre todo porque muy pocos usuarios sabían o entendían esto (ver Cohen, Adam, "What Google should roll out Next: A Privacy Upgrade", publicado en NY Times A18, del 28/11/2005). En marzo de 2007 Google anunció públicamente que cambiaba su política de privacidad y que "anonimizaría" los datos sobre búsquedas luego de un plazo de dieciocho a veinticuatro meses (ver Fleischer, Peter y Wong, Nicole, "Taking Steps to Further Improve Our Privacy Practices", publicado en el blog oficial de Google, The Official Google Blog, 14/3/2007, en <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>). En un

ráfico, al formar contenido (en este caso la Corte Su- detiene aquí. No gráfico solamente otros supuestos por celular, SMS as o no constitu- señalamos— que atan estos datos sión, pues exigen a su obtención.

admisible que las desprovistas del que excluya la po- por agentes de la ás libre discreción afirmación se da donde, ya sea por 25873), se podría or una década.

vo  
 el presente caso ecidido (tanto por lisidencia parcial). a la caracterización re fue visto como , limitado a la faz da nos recuerda la la por tratadistas y vida privada. Es un uevas tecnologías omo lo demuestra egativa (el derecho de esa esfera) a la o (la protección de datos personales). vacidad no sólo se hechos concretos is diseños de políti- cambios mínimos : internet afectan a las fronteras y las oogle decide cam- nes de logs pueden a las autoridades o

das a una "cookie" (un cuando un usuario se iador del usuario hasta oogle era el año 2038, n, Adam, "What Google e anunció públicamente dieciocho a veinticuatro al blog oficial de Google, rprove-our.html). En un

usados con fines de *marketing*. Si Facebook—actualmente con 150 millones de usuarios en todo el mundo— altera sus términos y condiciones de uso y decide que toda la información subida por sus usuarios le pertenece (incluyendo fotos, videos, imágenes y datos personales), hay poco que se pueda hacer a nivel local. Estas políticas también conciernen al ejercicio del poder público: rutinariamente empresas globales contestan a jueces locales con negativas de provisión de información, pese a tener sucursales en el país requerido, con el argumento de que "sus servidores están localizados en California, o Washigton...". Ello ha generado la necesidad de lograr acuerdos de colaboración entre el sector público y el sector privado (el caso de Chile), y en algunos casos hasta respuestas violentas de las autoridades locales (el caso de Brasil y Google Orkut).

Hoy en día la globalización ha logrado un fenómeno adicional: los tratamientos de datos son cada vez más transnacionales y globales, y por ende afectan por igual a muchas personas ubicadas en diversas jurisdicciones sujetas a distintas normas de protección de datos personales. Citamos como ejemplo los casos del PNR, el caso Swift, el caso del *rootkit* de Sony BMG (15), o el intento de cambio de política de la red social Facebook (16) que ya mencionamos.

Hay otra dimensión más de lo colectivo. En materia de telecomunicaciones, las actividades de los Estados en materia de seguridad y defensa nacional pueden tener efectos sobre las actividades de otros habitantes de otros Estados (17), lo que supera el derecho de un estado a defender a sus habitantes. Por ejemplo, la decisión del entonces presidente de Estados Unidos de intervenir todo el tráfico telefónico y de internet a través de la NSA (18) no sólo afecta a comunicaciones con los EE.UU. sino también a otras comunicaciones que, dada la arquitectura de internet, transitan por las redes pero con origen y destino fuera de los Estados Unidos. La Corte de aquel país (19) implícitamente convalidó estas actividades al dejar firme un fallo que rechazó el planteo de inconstitucionalidad (justamente se trataba de una acción de clase iniciada por varias organizaciones contra estas prácticas).

Como es dable observar, la actividad cada vez más frecuente de intervenir comunicaciones, de monitorear correos electrónicos o actividades de navegación o de espiar en internet de algún modo afecta a una pluralidad inde-

terminada de personas y justifica soluciones colectivas como la adoptaba por la Cámara y confirmada y expandida en este fallo de la Corte.

No podemos dejar de mencionar que en materia de herramientas procesales colectivas el tema ya había sido tratado judicialmente cuando la Cámara Comercial reconoció la procedencia del "hábeas data colectivo" (20). No se trataba de una acción de clase sino de un proceso colectivo llevado adelante por una asociación de defensa de consumidores y expresamente reconocido en el art. 52, LDC. Lo importante es que se aceptó el uso de una vía procesal clásicamente individual para discutir cuestiones atinentes a la Ley de Protección de Datos Personales. Y la Corte ya había colectivizado también el hábeas corpus.

c) ¿Cómo debería ser una futura Ley de Datos de Tráfico para ser constitucional?

La pregunta es importante, porque la suspensión, declaración de inconstitucionalidad (*erga omnes*) de la ley 25873 y probablemente su futura derogación han creado un *limbo jurídico* en materia de prueba digital. Hoy en día no existe obligación de almacenar estos datos, por más que, como dijimos, de hecho se almacenan pues son necesarios para efectuar una comunicación. Pero si no se almacenan, no se pueden solicitar judicialmente, pues se corre el riesgo de una respuesta negativa por parte del ISP o la telefónica. Cabe plantearse entonces qué debe hacerse en esta materia. Nuestra propuesta es simple: siguiendo los pasos indicados por la Corte, diagramar en el Código Procesal Penal (y en la misma medida, en el Código Procesal Civil y Comercial Federal) una medida de prueba consistente en la obtención con orden judicial de las direcciones IP de una determinada comunicación.

Veamos primero una cuestión "política". Un punto previo en el razonamiento de la Corte que llama la atención es la mención del hecho de que las interceptaciones actuales las realiza la SIDE, bajo control del "poder político".

El tribunal señala que "tal afirmación adquiere relevancia si se advierte que es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del 'poder político', la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos". Resaltamos que

trabajo anterior señalamos el problema que ocasionaba que los actores institucionales privados establezcan reglas privadas sobre estas cuestiones de datos personales y el efecto que producía en las normas nacionales (básicamente las anula cuando no existe jurisdicción sobre la compañía) (ver Palazzi, Pablo, "Google y el derecho a la privacidad sobre las búsquedas realizadas en internet", JA 2007-II-430).

(15) Para más detalles del caso ver la nota de Mulligan, Deirdre y Perzanowski, Aaron "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident", 22 Berkeley Tech. L.J. 1157 (2007).

(16) Vascellaro, Jessica E., "Facebook's About-Face on Data", *Wall Street Journal*, 19/2/2009.

(17) Ver Irion, Kristina, "Privacy and Security. International Communications Surveillance", *Communications of the ACM*, vol. 52, n. 2, febrero de 2009, p. 26.

(18) Ver Wikipedia, "NSA warrantless surveillance controversy", [http://en.wikipedia.org/wiki/NSA\\_warrantless\\_surveillance\\_controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy).

(19) Savage, David, "Supreme Court rejects wiretap suit", *Los Angeles Times*, 20/2/2008.

(20) C. Nac. Com., sala E, "Unión de Usuarios y Consumidores v. Citibank s/sumarísimo", 12/5/2006.

## Derecho Penal Informático

esto no estaba en discusión, y es un claro *statement* de la Corte al Poder Ejecutivo y Legislativo.

Está bien que la Corte haya hecho esto porque, como guardian de los derechos y garantías constitucionales, su papel no debe limitarse a resolver el caso concreto sino que también debe fijar un rumbo futuro en la legislación que sobre este tema tan delicado deberá aprobar el Congreso. En estos casos de importancia, donde estaba en juego la intimidad de una clase entera de ciudadanos, el *self restraint* no es ninguna virtud. Lo que sigue por lógica de esta declaración es preguntarse si una futura reforma legal no debería modificar el sistema vigente de interceptación y captación de comunicaciones (21). El punto, obviamente, supera el debate sobre los datos de tráfico, pero se soluciona simplemente sacando del medio a la SIDE y permitiendo que el Poder Judicial les ordene directamente a los prestadores a través de una oficina propia las interceptaciones que correspondan en cada caso concreto.

¿Cómo deberá ser entonces una nueva ley que apruebe el Congreso? El estándar de la Corte requiere cuatro presupuestos.

Primero debe existir una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia. Entendemos que debe ser una ley en sentido formal.

Hay dos extremos en cuanto a los casos y a sus justificaciones: uno, la tradicional orden judicial de interceptación de comunicaciones, en la cual un juez en un caso concreto bajo determinadas circunstancias y por orden fundada manda intervenir una comunicación. En el otro extremo tenemos la ley 25783 —declarada inconstitucional—, que sin ninguno de estos requisitos presentes (no había "casos"; éstos, teóricamente, vendrían después) mandaba guardar todos estos datos por si se llegaran a necesitar a futuro, y encima por diez años. No es sólo una cuestión de plazo (ver el próximo punto) sino también de los recaudos para acceder a esa información.

En Europa esto fue especialmente debatido, y finalmente en la Directiva Europea sobre Retención de Datos se estableció que el acceso a estos datos sólo será en casos específicos (22). Esta norma está claramente destinada a evitar un *data mining* virtual sobre esos datos, más conocido en la jerga procesal penal como "*fishing expedition*" tecnológico (23).

En la Argentina una ley especial que requiera orden judicial para obtener datos de tráfico y que precise los supuestos es necesaria, porque el art. 18, CN, y la interpretación que dieron los tribunales así lo requieren (de lo contrario la Cámara podría haber declarado parcialmente la inconstitucionalidad de la ley sólo cuando los datos de tráfico se "anudan" a los de contenido). Por otra parte, la verdad es que los datos de tráfico a veces dicen tanto o más que la propia comunicación, de allí su utilidad para el proceso judicial, sobre todo el penal.

En Europa, donde existió un gran debate sobre la Directiva que regula esta misma materia (24), toda la discusión giró en torno a la necesidad de encontrar una base legal para legitimar el almacenamiento de estos datos. Sin tal legitimación la retención de datos sería una interferencia en la privacidad no autorizada por ley (arg. art. 8, Convenio Europeo de Derechos Humanos). También era necesaria porque la jurisprudencia europea equiparaba los datos de tráfico a los de contenido (25). En la práctica alcanzaba con que se reflejara en una Directiva y luego fuera internalizado en las leyes nacionales. Pero en realidad, más allá de que en ello existió siempre un acuerdo, la discusión pasó por usar el primer o tercer pilar de la Unión Europea, que legitima la medida por la intervención del Parlamento Europeo.

En Estados Unidos no es necesaria una ley porque estos datos se almacenan pese a no existir ley que lo ordene; curiosamente, el sector privado los almacena, no porque esté interesado en colaborar con la justicia y ayudar a detener e investigar la comisión de delitos sino porque (a veces desagregados y otro no tanto) poseen un enorme

(21) El art. 21, Ley de Inteligencia Nacional 25520 dispone: "Créase en el ámbito de la Secretaría de Inteligencia la Dirección de Observaciones Judiciales (DOJ), que será el único órgano del Estado encargado de ejecutar las interceptaciones de cualquier tipo autorizadas u ordenadas por la autoridad judicial competente".

(22) El art. 4 dice: "Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. 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".

(23) En nuestro derecho el término es usado en varios fallos judiciales. Ver C. Nac. Crim. y Corr. Fed., sala 2ª, 21/10/1997, "Díaz Chagas, Wellington"; C. Nac. Crim. y Corr., sala 2ª, causa 7170, "Ramírez Sánchez", 21/5/1991, reg. 8036.

(24) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, del 15/3/2006, 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, y por la que se modifica la directiva 2002/58/CE.

(25) Se trata del caso "Malone" del TEDH, donde se discutía la validez de datos obtenidos a través de un "*pen register*" o "*comptage*". Allí se dijo: "El Tribunal no acepta, sin embargo, que la utilización de los datos así obtenidos no pueda plantear problemas en relación con el art. 8 [que se refiere a la vida privada]. En los registros así efectuados se contienen informaciones —en especial, los números marcados— que son parte de las comunicaciones telefónicas. En opinión del Tribunal, ponerlos en conocimiento de la policía sin el consentimiento del abonado se opone también al derecho confirmado por el art. 8".

valor para *marketing* y su comercialización a terceros (26), actividades que el régimen de privacidad allí vigente no prohíbe (y que en Europa, por la vigencia de leyes de protección de datos es anatema). Además su acceso es más fácil, pues a partir del fallo de la Corte Suprema estadounidense en "Smith v. Maryland" (27) tales registros tienen un estándar menor de protección constitucional que las comunicaciones en tránsito. Por lo menos ésta es la interpretación de cierta jurisprudencia y doctrina vigente.

El segundo requisito es que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión: en estos supuestos una ley como la de Retención de Datos de Tráfico (ley 25873) estaría justificada en tener los elementos necesarios para combatir el crimen, habiendo sido así reconocido por el fallo de Cámara en el caso "Halabi". Sin embargo, este reconocimiento judicial en un único caso no era suficiente. Si los datos estaban almacenados por una década, probablemente cualquier litigante empezaría a usarlos pidiendo las pruebas del caso mediante órdenes judiciales en juicios civiles, laborales, penales o de cualquier índole. Así no se usarían solamente en casos de secuestros o pedofilia, sino también en un divorcio, injurias o un juicio laboral (como de hecho sucede actualmente).

En Europa inicialmente la propuesta de la Directiva estaba diagramada para toda clase de delitos (incluyendo terrorismo y crimen organizado), pero finalmente se limitó sólo a "delitos graves". En efecto, su art. 1 reza: "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, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro". Los Estados miembros, al internalizar esta norma, deben respetar estos límites.

Volviendo a nuestros pagos, hay que señalar que siempre estaría presente la tentación del Estado administrador, que un buen día podría pedir "prestada" una "copia" de la base de datos. Es decir, para hablar en términos constitucionales actuales, los "ciudadanos" no tenemos "derechos adquiridos" a que esa inmensa base de datos creada por la ley 25873 continuara siempre "privatizada". Algún día algún funcionario la estatizaría y haría un verdadero *data mining* (dejo al lector completar la finalidad), invadiendo la privacidad de los datos personales de millones de individuos.

Tercero, la Corte requiere "que la aludida restricción resulte un medio compatible con el fin legítimo propuesto". Esto requiere analizar, ni más ni menos, la proporcionalidad de la medida. Responde a la pregunta acerca de si las medidas adoptadas sirven para el fin propuesto y si ello puede probarse de alguna forma. Prueba, claro está, que está a cargo del gobierno, que es el que aprueba la medida restrictiva.

En la Argentina la argumentación sobre la proporcionalidad de la ley 25873 brilló por su ausencia. Es más, la ley 25873 se aprobó solapadamente, sin discusión oficial ni explicación de ninguna especie. El mismo presidente que la reglamentó luego la suspendió presionado por la "opinión pública". No existió el debate serio y maduro que ocurrió en las instituciones europeas, donde en la redacción de la Directiva participaron la Comisión Europea, el Consejo, el Parlamento Europeo, el Supervisor Europeo de Protección de Datos (una suerte de *ombudsman* a nivel europeo especializado en materia de protección de datos), las autoridades locales de protección de datos personales representadas por el denominado "Grupo de Trabajo del Art. 29", universidades, académicos y multitud de entidades privadas y empresas afectadas (28). Es claro que los ciudadanos europeos están un poco mejor representados que los argentinos, y que sus instituciones funcionan.

La Directiva Europea en la materia claramente reconoce la importancia de estos datos: "Dada la importancia de los datos de tráfico y de localización para la investigación, detección y enjuiciamiento de delitos, según demuestran la investigación y la experiencia práctica de varios Estados miembros, existe la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones se conservan durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva".

Es decir, de alguna forma una medida que retenga por breve tiempo información sí sería proporcional al fin buscado. De hecho, como venimos diciendo, estos datos se crean y se almacenan por cierto tiempo pues son necesarios para la comunicación. Así que un breve lapso no es complicado. Pero la mejor solución para la Argentina sería establecer un plazo corto, o ningún plazo, y mejorar las órdenes y herramientas procesales existentes para obtener estos datos, tal como proponemos en las conclusiones de esta nota.

Finalmente, el tribunal exige en su test que "dicho medio no sea más extenso que lo indispensable para el aludido

(26) Bellia, Patricia L., "The Memory Gap In Surveillance Law", 75 U. Chi. L. Rev. 137 (2008); Bignami, Francesca, "Privacy and Law Enforcement in the European Union: The Data Retention Directive", 8 Chi. J. Int'l L. 233 (2007).

(27) Caso "Smith v. Maryland", 442 US 735 (1976).

(28) El debate europeo sobre esta cuestión y los intereses en juego de cada player está brillantemente narrado en el trabajo de Bignami, Francesca "Privacy and Law Enforcement in the European Union: The Data Retention Directive", 8 Chi. J. Int'l L. 233-254 (2007).

tido, y finalmente de Datos se es- sólo será en casos imente destinada s datos, más co- fishing expedition"

iera orden judicial ise los supuestos nterpretación que de lo contrario la mente la inconsti- latos de tráfico se parte, la verdad es anto o más que la d para el proceso

sobre la Directiva la la discusión giró na base legal para latos. Sin tal leg- ia interferencia en ; art. 8, Convenio ién era necesaria araba los datos de ráctica alcanzaba luego fuera inter- en realidad, más ierdo, la discusión la Unión Europea, ón del Parlamento

á ley porque estos ley que lo ordene; racena, no porque usticia y ayudar a itos sino porque (a ioseen un enorme

encia la Dirección de nes de cualquier tipo

midad con la presente e conformidad con la irse y las condiciones ad y proporcionalidad, lico, y en particular el

21/10/1997, "Díaz generados o tratados is de comunicaciones,

gister" o "comptage". problemas en relación especial, los números nto de la policía sin el

## Derecho Penal Informático

logro. A su vez, fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes".

La Corte no se pronunció sobre el plazo de diez años para guardar datos de tráfico que señala la ley (no tenía que hacerlo), pero igual convalidó la declaración de toda la ley como inconstitucional. Sería positivo que el Congreso estudie de alguna forma el reemplazo de la ley y legisle un plazo menor, de seis meses a dos años, como el derecho comparado, dado que la Corte no invalidó ningún plazo pero la proporcionalidad del test requiere un plazo adecuado con el fin perseguido.

### IV. CONCLUSIÓN

Como consecuencia del fallo de la Corte se ha creado un vacío legal: con la ley 25873 declarada ilegal, falta en la Argentina un régimen que determine en forma global por cuánto tiempo se deben guardar los datos de tráfico, y, por ende, se atenta contra su fácil obtención para que sean usados en procesos penales con prueba informática.

Es necesario, además, proveer a los litigantes y abogados de un mecanismo ágil para obtener prueba en juicios civiles y penales, por ejemplo, autorizando a un juez a "congelar" la información hasta que se pueda pedir mediante orden al ISP, o mediante un orden de entrega de datos (29). Estas medidas estaban previstas en el Proyecto de Código Procesal Penal de la Nación (arts. 181 y 190 a 193) preparado por el Ministerio de Justicia, que aún no fue tratado por el Congreso (30).

También el Congreso debe decidir a qué clase de datos de tráfico se aplicará, pues la Corte en su fallo no hizo distinciones. Queda claro que para la Corte "los datos de navegación anudan a los contenidos". Esto equivale a decir que los datos de tráfico de navegación en internet implican develar datos de contenidos, y en esto la ley clara-

mente era inconstitucional porque estas comunicaciones se almacenaban por diez años sin orden de juez competente. Hoy en día esos datos se almacenan automáticamente por cierto tiempo, pues, como explicamos, son necesarios para realizar la comunicación, pero no existe obligación de mantenerlos por tiempo indeterminado. La práctica en la industria es guardarlos si son necesarios para la facturación, o, como máximo, por el plazo de prescripción de las acciones pertinentes para poder ejercer una adecuada defensa de sus intereses.

La cantidad de datos que se almacenen, así como el plazo, será importante para cumplir con el último punto del estándar de la Corte ("...que dicho medio no sea más extenso que lo indispensable para el aludido logro"). Este punto fue arduamente discutido en Europa durante el debate de la Directiva de Retención de Datos. Inglaterra presentó estadísticas en las cuales demostraba que en ciertos casos estos datos habían sido claramente útiles para encontrar a autores de ciertos delitos. Las autoridades de protección de datos estaban escépticas con estas pruebas y exigieron una prueba más científica de la utilidad de los datos.

La Sociedad de la Información está cambiando la forma de vivir, al abrir nuevas posibilidades comunicativas, informativas y de organización social. Las tecnologías de la información han modificado el modo en que afrontamos nuestra relación con los demás y nos ofrecen herramientas para avanzar en la democratización de nuestras sociedades. Sin embargo, esta tecnología también puede tener otros usos que podrían poner en peligro nuestros derechos más básicos. Ponerle los límites adecuados es un imperativo para no perder las libertades que hemos conseguido. Pero es importante no perder por ello otras facultades tan valiosas como la de poder investigar adecuadamente los hechos ilícitos.

(29) Ejemplos internacionales abundan: se puede citar el Convenio del Cibercriminológico o la Directiva Europea de Retención de Datos.

(30) Me refiero al Anteproyecto de Reforma del Código Procesal Penal de la Nación, que fue elaborado recientemente por una Comisión Especial designada por el Ministerio de Justicia. Dicha Comisión Asesora estuvo integrada por los diputados Juan Becanni, Luis Cicogna y Rosario Moreno, los senadores Sanz, Ibarra y Pichetto, los jueces Luis García y Adriana Ledesma, el secretario general de la Procuración General de la Nación, Adrián Marchisio, el representante académico Fernando Díaz Cantón, el abogado Marcos Salt y Carlos Beraldi.