Retención y Privacidad de Datos: Algunas Lecciones Derivadas de las Diversas Prácticas Internacionales

Escrito por
Daniel Kapellmann Zafra
Benjamín Reyes Ampudia

Colaboraciones
Samuel Bautista Mora
Gonzalo Rojon González
Carlos Silva Ponce de León

Índice

Abstract

Las prácticas internacionales en temas de privacidad y retención de datos, sugieren un marco de referencia para dirigir y orquestar la conformación de lineamientos en la materia. En particular, existe una clara y sostenida tendencia por buscar un equilibrio eficiente entre la procuración de justicia y el cuidado a la información privada de los individuos. No obstante, para la implementación exitosa de este mecanismo legal, también existen diversas consideraciones que deben ser previamente ponderadas y evaluadas. Entre éstas destacan los tipos de datos susceptibles a retención (contenidos o metadatos), el periodo de almacenamiento, los organismos que contarán con acceso a la información retenida y los costos de implementación. En suma, las prácticas internacionales generan una experiencia dotada de una diversidad de matices que fungen como herramienta de planeación, estructuración y desarrollo del marco regulatorio.

Introducción

Durante las últimas décadas, los avances tecnológicos han logrado permear sobre múltiples dimensiones de la vida humana. En consecuencia, existen importantes consideraciones que deben realizarse con respecto a la interacción de los usuarios realizada a través de medios digitales.

A diferencia de la mayoría de las actividades en el ámbito físico, en el plano digital toda interacción interpersonal deja un rastro de lo acontecido. Esta huella se refiere al cúmulo de información que se genera y perdura más allá de la comunicación emitida entre dos o más usuarios, y que por lo mismo puede quedar a disposición de distintos agentes como otros individuos, compañías proveedoras del servicio o gobiernos.

Cabe denotar que este rastro electrónico puede contener información sensible y en muchos casos, de interés personal. Es por esto que las mismas cualidades regulatorias que se aplican a las actividades humanas en el plano físico, deben extenderse y adaptarse a la protección y regulación del tratamiento del plano digital.

Siguiendo este principio, en el ámbito digital debe respetarse también el sexto artículo de la Constitución de los Estados Unidos Mexicanos en que se establece que "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos…" salvo excepciones planteadas por seguridad nacional, orden y salud pública. Asimismo, se menciona que "Las comunicaciones privadas son inviolables", a menos de que se trate con aportaciones voluntarias o investigaciones judiciales debidamente justificadas.[1]

En particular, este documento se enfoca en una de las disposiciones legislativas que ha causado gran polémica en el contexto internacional: la retención, registro y control de datos generados por las tecnologías de la información. En términos generales, la gestación de esta discusión consiste en la existencia de una línea divisoria muy tenue entre lo que puede ser una legítima acción de procuración de la justica y un acto de violación a la privacidad individual.

Son diversos los argumentos que sustentan que estas disposiciones legislativas son de gran eficiencia y utilidad para la protección y procuración de la justicia. Sin embargo, estas medidas deben de ser diseñadas con cautela para evitar generar

[1] Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

implicaciones negativas en contra de la privacidad, libertad de expresión, e incluso derivar en gastos excesivos.

Algunas de las principales consideraciones que deben preverse para la regulación en este ámbito, incluyen la sensibilidad e intimidad de la información, el tipo de datos sujetos a manejo o tratamiento, la logística en el procesamiento de los mismos y, en general, el proceso a seguir para permitir una implementación eficiente y adecuada.

En este documento se realizará en primer lugar una breve descripción con respecto a los distintos tipos de datos existentes, seguido por un análisis descriptivo contextual de la experiencia y legislación internacional en cuanto al tratamiento, control y almacenamiento de datos. Finalmente, se hablará sobre el gasto e implicaciones económicas de este tipo de regulación con la finalidad de presentar un panorama completo de la polémica y así generar una base epistémica sobre las principales consideraciones en el entorno global.

Seguridad y Datos

La implementación de estrategias o sistemas para retención, registro y control de datos por parte de los gobiernos responde a la necesidad de utilizar la tecnología para responder ante actuales escenarios de inseguridad. La recopilación de información y el monitoreo de las comunicaciones que se llevan a cabo entre los individuos representa una herramienta complementaria en la consecución de la justicia.

Existen dos tipos de datos que pueden ser utilizados por las autoridades, que son de contenido y de tráfico o contexto. Los primeros se refieren en particular al mensaje transmitido, es decir, que permiten conocer tal cual el intercambio de información que se llevó a cabo entre dos o más usuarios.

Los segundos, también conocidos como "metadatos", permiten revelar la localización, fecha, el emisor, receptor, tiempo, formato, características técnicas, dispositivo utilizado para emitir el mensaje y fuente de la información, entre otras cosas. Si bien no existe una definición única y universalmente aceptada de este tipo de datos, es posible asegurar que se trata de información complementaria que acompaña al contenido.

A continuación se brindan algunas definiciones adicionales de metadatos utilizadas en distintas regiones:

Localidad	Significado
Unión Europea	Datos generados o procesados como consecuencia de la comunicación o servicio de comunicación y sin relación al contenido de las mismas[2].
Reino Unido	Una de las definiciones más comunes de "metadatos" es "datos sobre datos". En términos formales, los metadatos son información estructurada acerca de algún recurso.[3]
Estados Unidos	De acuerdo con el *American National Standards Institute*, los metadatos son información estructurada que describe, explica, localiza y facilita la obtención y uso de recursos informativos.[4]

Fuente: Cuadro recopilado por The Social Intelligence Unit

A manera de ejemplo, al realizar un envío por correspondencia los datos de tráfico o metadatos son el sobre y las direcciones del remitente y destinatario mientras que los datos de contenido son la carta misma. Si bien ambos tipos de datos pueden proveer importantes piezas de información para la protección de la seguridad pública y nacional, la retención y acceso a contenidos, puede llegar a infringir los derechos fundamentales de privacidad, opinión y expresión del individuo salvo que exista un monitoreo y control adecuado sobre esta práctica.

Lo anterior ha desatado la discusión en el ámbito internacional, incitando a una serie de reconfiguraciones en los sistemas regulatorios utilizados para la recopilación de datos de los usuarios. A continuación se presentan algunos de los casos más representativos a nivel global que tratan la presente cuestión.

[2] Data Retention Directive, Diario Oficial de la Unión Europea , Directiva 2006/24/EC, Unión Europea 2006, Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[3] e-Goverment Metadata Standard, Reino Unido, 2006, Disponible en: http://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf

[4] Understanding Metadata, American National Standards Institute 2004, Disponible en: www.niso.org

Experiencia Internacional

Bajo el liderazgo de Brasil y Alemania, en diciembre de 2013 la Asamblea General de las Naciones Unidas aprobó la Resolución 68/167, mejor conocida con el nombre de "El Derecho a la Privacidad en la Era Digital".[5] En este documento, se realizaba un énfasis en la importancia de proteger las libertades fundamentales de los individuos para transmitir, recibir y compartir información sin interferencia arbitraria o ilegal a sus derechos de privacidad familiar, en el hogar o de correspondencia.

Tomando en cuenta el veloz desarrollo de las tecnologías de la información y las recientes disputas sobre privacidad digital en el escenario internacional, esta resolución sentó las bases para detonar el diálogo multilateral y fomentar la creación de marcos regulatorios adecuados para la retención de datos. Hasta ahora, varios gobiernos han buscado apoyo en el sector privado para retener información de los usuarios que les permita mejorar su seguridad, sin embargo, este tipo de práctica requiere de una planeación cuidadosa para no atentar contra los derechos fundamentales de los individuos.

Como se menciona en el documento, los derechos de las personas en el ámbito físico deben ser protegidos también en el mundo digital. Por ende, se invita a la comunidad internacional a evitar violaciones a la privacidad, incluso bajo el argumento de que dicha información sea necesaria para fomentar la seguridad nacional en temas como la lucha contra el terrorismo.

Si bien este marco representa una base para la elaboración de legislación a nivel global en cuanto a la retención y uso de datos, cada región o país ha delimitado sus propias condiciones. A continuación se muestran algunos de los principales casos:

[5] General Assembly, Resolution adopted by the General Assembly on 18 December 2013, 21 de enero 2014. Disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (Consulta: 11 de febrero 2015)

Unión Europea

Tras los atentados terroristas acontecidos en Madrid (2004) y Londres (2005), se creó la Directiva de Retención de Datos (2006) con el objetivo de armonizar el clima social por medio de una mejor persecución del crimen organizado. En este caso, se utilizó la retención de información para identificar el tráfico de datos así como la localización de su emisión. [6]

Es importante resaltar que los datos retenidos nunca incluyeron contenidos, sino que se limitaban a metadatos. Entre la información destinada a retención destacaba el nombre y dirección de los usuarios de servicios de telefonía fija y móvil, así como los números que recibieron llamadas del sujeto dispuesto a retención de datos, la fecha y hora de las comunicaciones, conexión y desconexión de internet, e incluso la dirección IP de los usuarios.

La directiva original estipulaba que la retención de información era una herramienta útil para el combate del crimen organizado y el terrorismo. Con base en esto, justificaba que las autoridades públicas podían intervenir en la privacidad de los datos personales en casos de seguridad nacional y pública, siempre y cuando esto se realizara conforme a las leyes internas del país. Asimismo incitaba a los operadores a contar con un periodo de retención de datos de entre 6 meses y 2 años.

A grandes rasgos, la justificación legal se asemejaba a gran parte de las sanciones legales ante actos delictivos. Específicamente, la Directiva permitía la intervención y recopilación de datos personales, siempre y cuando existiera un daño o interferencia a la integridad o derechos de terceros.

Es importante recordar que la Directiva obligaba a los Estados miembros a incorporar en su marco legal esta regulación, por supuesto bajo un esquema casuístico. La directiva generaba un panorama legislativo de recomendaciones para el fomento e instauración de regulaciones afines, pero llevadas a cabo por las autoridades pertinentes para el manejo y control de información en el ámbito local de cada país.

Adicionalmente, en la evaluación de esta Directiva realizada en el 2011, [7] se

[6] Diario Oficial de la Unión Europea, Directiva 2006/24/Ce Del Parlamento Europeo Y Del Consejo, 15 de marzo 2006. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

[7] Reporte de la Comisión para el Consejo y Parlamento Europeos, Reporte de Evaluación sobre la Directiva de Retención de Datos, Bruselas, 2011, Disponible en : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

señala que la retención de datos genera barreras importantes para las empresas de telecomunicaciones. Dichas barreras son construidas por los elevados costos de almacenamiento, además de que se crean fricciones entre el consumidor y la empresa debido a la invasión a la privacidad de datos personales.

Esta evaluación no solo denotaba la importancia de los costos de implementación y operación de la medida, sino que a la vez reflejaba la pérdida en el ímpetu regulatorio que vivía la tendencia inicial de esta regulación. De este modo, en 2014 la Corte de Justicia de la Unión Europea invalidó la Directiva de Retención de Datos.

La invalidación tuvo un argumento fundamental y claro: no se establecieron suficientes medidas para proteger los derechos a la privacidad y la información personal. En general, esto ilustra un hecho, la seguridad no justifica una intervención a los derechos fundamentales de la privacidad más que en casos específicos con condiciones precisas y dentro de un entorno de responsabilidad bilateral.

Alemania

A la par del desarrollo en las tecnologías de la información, Alemania cuenta con una Ley Federal de Protección de Datos desde 1977, misma en que se determinó que el individuo debía ser capaz de determinar el uso de su información personal. [8] A partir de entonces, este documento (con sus posteriores modificaciones) ha sido el principal código encargado de controlar el manejo de los datos de los usuarios a nivel nacional, protegiéndolo tanto del gobierno, como de empresas privadas.

Con el fin de combatir al terrorismo y el crimen organizado que se había fortalecido regionalmente en los años anteriores, así como mantener la línea con la Directiva de Retención de Datos de la Unión Europea, Alemania estableció en la Ley de Telecomunicaciones la obligación de los proveedores de servicios de retener los metadatos de los usuarios por el periodo mínimo de seis meses. De modo complementario, la última versión de la Ley Federal de Protección de Datos (promulgada en 2003 y con sus más recientes modificaciones en 2009) establecía los principios y condiciones para el almacenamiento de información generada por servicios de telecomunicaciones.[9]

[8] Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). Disponible en: http://www.iuscomp.org/gla/statutes/BDSG.htm

[9] Bundesministerium der Justiz un für Verbraucherschutz, Federal Data Protection Act, 2014. Disponible en: http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

Este esquema dio pie a una serie de discusiones que orillaron a la Corte Constitucional Alemana en 2010 a anular dicha legislación, argumentando que el modo en que se implementaba la Directiva en el país representaba una seria intromisión a la privacidad de las personas. De este modo, Alemania fue sujeto de sanciones y acusaciones por parte de la Unión Europea ante la falta de implementación de los acuerdos establecidos en la Directiva. Finalmente, la cancelación en 2014 de la Directiva europea, liberó al país de las anteriores acusaciones y frenó las discusiones sobre una nueva legislación para retención de datos a nivel nacional, al menos hasta que los ataques terroristas llevados a cabo en Francia en 2015 comenzaran nuevamente la discusión.

Por el momento, la legislación alemana en materia de protección y retención de datos se limita al establecimiento de una serie de principios que deben seguirse para el almacenamiento y uso de los mismos; así como una descripción clara de que únicamente órganos judiciales y legislativos pueden tener acceso a la información obtenida.

Los principios que menciona la legislación alemana son, en primer lugar la reducción y "economía de los datos", es decir que los sistemas de recaudación deben estar diseñados para seleccionar y procesar tan poca información como sea posible. Por otro lado, implica la petición de permiso exclusivo por el individuo o alguna autoridad, un propósito claro para la recolección de datos, recolección directa, posibilidad de acceso por el usuario, corrección de datos incorrectos y la eliminación de la información una vez que ya no sea necesaria.[10]

Argentina

Este caso se distingue del resto ya que es una de las pocas legislaciones realizadas previas a la Directiva de la Unión Europea. En 2005, el entonces presidente Néstor Kirchner, realizó un decreto para reformar la Ley de Telecomunicaciones aprobada en 2003. Esta ley obligaba a las empresas de telecomunicaciones y proveedores de internet a indexar, registrar y almacenar Datos de Tráfico por un periodo equivalente a 10 años.

La reforma a la ley, recibió poco apoyo por parte de la población y fue derogada en el 2005 por representar una amenaza a los derechos de privacidad de datos personales y por proponer un plazo de almacenamiento excesivo.

[10] Thomas Jansen y Britta Hinzpeter, Data protection in Germany: overview, DLA Piper, Alemania. Disponible en: http://us.practicallaw.com/3-502-4080

Para entender los argumentos legales que sustentaron la defensa ante el decreto de Kirchner es importante conocer el contexto legal previo a la confrontación. En la "Ley de Protección de los Datos Personales"[11] del año 2000 se hace referencia a los "medios técnicos de tratamiento de datos", y se afirma lo siguiente:

Capítulo 1

- Art. 1° - 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…

- Art. 6° - Cuando se recaben datos personales, se deberá informar previamente a sus titulares en forma expresa y clara:
  a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
  b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable

- Art 7° -
  1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
  2. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.

Bajo esta misma idea, el Artículo 19 de la actual "Ley Nacional de Telecomunicaciones"[12] muestra lo siguiente:

- 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

[11] El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, Ley de Protección de Datos Personales, Octubre 2000. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[12] Ley Nacional de Telecomunicaciones, Argentina, 1972. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/30000-34999/31922/texact.htm

comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos.

Por ende, queda claro que la regulación argentina ha enfatizado la protección no solo de los datos personales, sino que también ha detallado que esta protección debe extenderse hasta el mundo de las telecomunicaciones.

Australia

Entre 2013 y 2014, el Parlamento Australiano desarrolló la "Enmienda en Materia de Telecomunicaciones y Retención de Datos"[13]. En este documento se especificaba que las actividades criminales hacían un uso intensivo de diversas tecnologías para llevar a cabo sus actos ilícitos. Bajo este motivo, se sustentó la necesidad de combatir las actividades criminales por medio de la retención, intercepción y acceso de datos, con el fin de proteger la seguridad nacional.

En cuanto a las consideraciones básicas sobre retención de datos, la legislación australiana es similar a otros casos. En general, limita la retención de información a metadatos y excluye el contenido de las comunicaciones así como historiales de búsqueda. El plazo de retención será de 2 años y solo se autorizará el acceso a estos datos para organismos dedicados a la procuración de la ley.

A pesar de la similitud que muestra la Enmienda con otras legislaciones internacionales, existen varias características que deben destacarse sobre ella. Primero, resalta que en el documento se incluye una breve sección sobre el "impacto financiero", misma en que se declara que la medida generará un impacto económico en el sector y que éste ya ha sido considerado por los reguladores. De hecho, durante la negociación de esta ley, se discutió arduamente sobre los costos de implementación y operación que generan este tipo de medidas debido a la enorme cantidad de datos generados diariamente.

Otra cuestión importante, es la enunciación de la importancia y cuidado a los derechos y libertades fundamentales de los individuos. Por medio de esta enmienda, el Parlamento Australiano especifica que la ley, dentro de todas sus condiciones, debe de ser "compatible con los derechos humanos", enfatizando en la libertad de expresión, la vida y la seguridad personal.

[13] Telecommunications (Interception and Access) Amendment (Data Retention) Bill, Australia 2014. Disponible en: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001%22

Para cumplir con esta compatibilidad se dedican distintas secciones del documento a cuestiones como: el derecho a la protección contra la interferencia arbitraria o ilegal, el derecho a un "juicio justo", la definición de los términos utilizados y la asignación de los organismos públicos capaces de acceder a los datos. Con esto, se busca proteger a los usuarios de servicios de telecomunicaciones y evitar la violación de sus derechos por medio de la procuración judicial.

Brasil

El primer intento de regulación y retención de datos en Brasil surgió con la Ley Aceredo propuesta en 2005 con la finalidad de regular cibercrímenes, e incluyendo la recopilación de información por parte de los proveedores de servicios. Sin embargo, esta regulación generó demandas sociales por privacidad por lo cual no fue aprobada, y a partir de 2010 se adoptó una nueva posición basada en la formulación de un marco de derechos para el mundo digital.

A partir de los recientes acontecimientos en el panorama internacional a causa de la revelación del espionaje de la NSA al resto del mundo, Brasil no solo ha jugado un rol de liderazgo ante la Organización de las Naciones Unidas, sino que también ha defendido una postura propia que se refleja en su Marco Civil para el Internet. Durante el primer día del foro NETMundial en abril 2014, se aprobó en Brasil dicha legislación mostrando un nuevo marco de derechos para los usuarios de la red.

Según dicha regulación, la intervención de los datos privados en Brasil no es obligatoria para los proveedores de servicios, sino que solo se podrá llevar a cabo bajo una orden judicial. Los datos o registros solamente pueden ser guardados por el plazo de un año y bajo las condiciones estipuladas por la ley, tomando en cuenta la protección de la intimidad, imagen y honra de las partes involucradas. En general, las intervenciones deben de ser aprobadas de manera individual, por lo cual se trata de un sistema casuístico y a discreción del sistema judicial brasileño.

Adicionalmente, debe contemplarse que según el artículo 11 del Marco Civil para el Internet, esta ley tiene estricta aplicación no solamente para los ciudadanos locales, sino para cualquier comunicación que incluya al menos a una persona en territorio nacional o para empresas que realicen tratos u ofrezcan servicios para el público nacional. Adicionalmente, obliga a los proveedores de internet a presentar información que permita verificar un trato adecuado de la información de acuerdo con las leyes brasileñas.[14]

[14] Congreso Interactivo, Traducción al Castellano del Marco Civil de Internet de Brasil. Disponible en:

España

En España, este tipo de legislación fue establecida desde el 2002 con la "Ley de Servicios de la Sociedad de Información y de Comercio Electrónico".[15] Sin embargo, el Artículo 12, que especificaba la retención de datos de tráfico relativos a medios electrónicos fue derogado en octubre de 2007, dando pie a la conformación de la "Ley de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones".[16]

De acuerdo con la ley de 2007 y vigente hasta 2015 (a pesar de la anulación de la Directiva de Retención de Datos de la Unión Europea), en España los proveedores de servicios de telecomunicaciones deben almacenar los datos por un periodo de un año, o bajo consulta previa hasta dos años. En particular, se especifica que los contenidos no son susceptibles a retención, sino que únicamente se tratará con datos para rastrear e identificar origen, destino, fecha y hora, tipo de comunicación, equipo y localización del equipo.

Asimismo, diferencia qué tipo de datos pueden recaudarse en comunicaciones móviles o en internet, incluyendo en el segundo caso la dirección IP del usuario, identificación del usuario, conexión y desconexión, tipo de servicio utilizado, línea digital de abonado DSL. Por otro lado, los agentes facultados para solicitar dicha información son los miembros de las fuerzas y cuerpos de seguridad, funcionarios de la Dirección Adjunta de Vigilancia Aduanera y el personal del Centro Nacional de Inteligencia.

Estados Unidos

De acuerdo con el artículo 222 del "Código de Privacidad de la Información del Consumidor"[17], los operadores de telecomunicaciones en Estados Unidos tienen el deber de proteger la confidencialidad de información propietaria sobre otras

http://blog.congresointeractivo.org/traduccion-al-castellano-del-marco-civil-de-internet-de-brasil/

[15] Jefatura del Estado, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, mayo 2014. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/Ley_34-2002_de_11_de_julio_de_servicios_de_la_sociedad_de_la_sociedad_de_la_informacion_y_de_comercio_electronico.pdf

[16] Jefatura del Estado, Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, España, 2007. Disponible en: http://noticias.juridicas.com/base_datos/Admin/l25-2007.html#a3

[17] Office of the Law Revision Counsel, United States Code, Title 47, Chapter 5, Subchapter II, Part I, § 222. Disponible en: http://uscode.house.gov/browse/prelim@title47/chapter5/subchapter2&edition=prelim

compañías y clientes. Las únicas excepciones en que esto podría verse limitado son ante la aceptación del cliente con respecto al uso de su información para otros fines, o por mandato legal.

A diferencia de las directivas europeas concentradas en la retención de datos, la ley estadounidense se enfoca en la preservación de los mismos (en vez de la retención).[18] Es decir, que según la "Ley de Privacidad de Comunicaciones Electrónicas de 1986"[19], los proveedores de comunicación electrónica o servicios de informática a mantener la información por 90 días, únicamente cuando las agencias gubernamentales correspondientes así lo requieran.

Además, los periodos de preservación deben ser financiados o compensados por el gobierno, y no se establece un plazo para que las compañías borren dicha información, de modo que pueden permanecer con la misma de modo voluntario. De acuerdo con la U.S. Internet Service Provider Association, la preservación de los datos es "el mecanismo que minimiza el riesgo de eliminación de registros y comunicaciones que podrían ser necesarias durante la investigación de un crimen".20

A partir de los atentados de 9/11 en Estados Unidos, estas legislaciones han sufrido constantes modificaciones en busca de promover la seguridad nacional. En este ámbito, la labor de la Asociación de Seguridad Nacional (NSA por sus siglas en inglés) ha destacado, pues incluye el análisis y recaudación de información sobre metadatos y contenidos, con base en la sección 215 del *Patriot Act*[21].

Para ello, esta legislación se apoya en las consideraciones de la *Foreign Intelligence Surveillance Act (FISA)*[22] con su última versión en 2008, que estipula las condiciones a partir de las cuales es posible el acceso a datos de los usuarios en distintos escenarios (extranjeros fuera del territorio, extranjeros en el territorio, estadounidenses fuera del país, entre otros casos). A partir de la sospecha de actividades terroristas, la NSA cuenta con la facultad de solicitar a los operadores de

[18] Kristina Ringland, The European Union's Data Retention Directive and The United States's Data Preservation Laws: Finding the Better Model. Disponible en: https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/427/vol5_no3_art13.pdf?sequence=1

[19] Office of the Law Revision Counsel, United States Code, Title 47, Chapter 5, Subchapter II, Part I, § 222. Disponible en: http://uscode.house.gov/browse/prelim@title18/chapter119

[20] Rodney Petersen, Toward a U.S. Data-Retention Standard for ISPs. Disponible en: http://www.educause.edu/ero/article/toward-us-data-retention-standard-isps

[21] US Department of Justice, The USA PATRIOT Act: Preserving Life and Liberty. Disponible en: http://www.justice.gov/archive/ll/highlights.htm

[22] Govtrack, Text of the FISA Amendments Act of 2008. Disponible en: https://www.govtrack.us/congress/bills/110/hr6304/text

servicios de telecomunicaciones todos los datos que requiera para realizar sus labores de inteligencia.

Si bien el rol de dicha institución continúa siendo ejercido, este tipo de monitoreo ha generado gran polémica a tanto a nivel local como internacional. Ha surgido un gran debate en torno a las prácticas de intercepción de datos de Estados Unidos, dando pie a la discusión de distintas regulaciones, como por ejemplo, la "Ley de Libertad"[23]. Este documento contempla, entre otras cosas, poner fin a la recopilación masiva de datos y establecer un defensor de la privacidad para supervisar el trabajo de la NSA.

Además, varios estados del país y jurisdicciones no estadounidenses han promulgado leyes que establecen los derechos de geolocalización. Estos proyectos de ley plantean el proceso mediante el cual las agencias gubernamentales pueden tener una orden judicial para investigar una "causa probable" y así obtener información sobre la localización de los usuarios. Este mecanismo funcionaría de manera similar a las órdenes que utilizan actualmente para escuchar llamadas telefónicas o de otros tipos de vigilancia electrónica. Particularmente, la "Location Privacy Protection Act"[24] propone que las empresas tengan que pedir permiso de los usuarios antes de recopilar datos sobre su ubicación proveniente de smartphones, tabletas, dispositivos de navegación.

México

En 2010 el Registro Nacional de Usuario de Telefonía Móvil (RENAUT) fue creado por decreto del gobierno con el objetivo de tener un control más exacto de los usuarios de líneas móviles por medio del registro de los teléfonos celulares con la cédula de identificación (CURP) de los ciudadanos. Con base en esto, buscaba convertirse en un sistema de prevención de fraudes y una herramienta contra delitos del crimen organizado. Sin embargo, esta legislación fracasó debido a que resultó inoperante y contradictoria con otras normas.

Actualmente, en concordancia con los artículos 189 y 190 de la "Ley Federal de Telecomunicaciones y Radiodifusión"[25] en México, aprobada en 2014, los concesionarios de telecomunicaciones se encuentran obligados a colaborar con las instancias de seguridad y justicia. Para ello, deben realizar la geolocalización en

[23] United States Congress, H.R.3361 USA FREEDOM Act, noviembre 2013. Disponible en: https://www.congress.gov/bill/113th-congress/house-bill/3361

[24] Senator Al Franken, The Location Privacy Protection Act of 2014. Disponible en: http://www.franken.senate.gov/files/documents/140327Locationprivacy.pdf

[25] Cámara de Diputados, Ley Federal de Telecomunicaciones y Radiodifusión, México, D.F., 5 de julio de 2014.

tiempo real de equipos móviles además de conservar registro de los datos relacionados con las comunicaciones que se realicen en sus redes.

Particularmente, en este país la retención y procesamiento de datos se especifica en un periodo de dos años, el primero manteniendo la información fácilmente accesible para instituciones de gobierno, y el segundo únicamente almacenando los datos por cualquier imprevisto. Asimismo, se especifica que se trata únicamente de metadatos, incluyendo nombre, denominación o razón social y domicilio del suscriptor, tipo de comunicación, origen, fecha, hora y duración, activación del servicio, identificación y características técnicas de los dispositivos.

Por otro lado, se especifica que las telecomunicaciones privadas son inviolables, a excepción de que la autoridad judicial federal a petición de la autoridad federal o el titular del Ministerio Público de la entidad autorice la intervención de los contenidos. Esto es únicamente posible en el caso de una investigación judicial, más no se trata de una práctica generalizada para los operadores de servicios.

Cabe destacar que esta legislación realiza una primera aproximación a la retención de datos en el país, sin embargo, se encuentra en proceso la realización de regulación más específica que cubra la implementación de esta iniciativa. El nuevo marco que se realice, deberá incluir especificaciones particulares para los servicios de internet, así como la designación de los agentes o servidores públicos facultados para tratar con dicha información.

Paraguay

En Paraguay, el "Proyecto de Ley de Retención de Datos" fue presentado tras una iniciativa parlamentaria a fines de 2014. Como la mayoría de las legislaciones en el tema, la motivación principal detrás de la retención de datos es enfrentar las "conductas antijurídicas que ponen en peligro diversos bienes jurídicos protegidos por el Estado."[26]

Esta legislación contempla únicamente la recopilación de Datos de Tráfico, es decir excluye el contenido. Para especificar esto la ley define lo que considera como datos de tráfico de la siguiente manera: "Aquellos generados en torno a una comunicación electrónica o magnética realizada por medio de un programa o

[26] Iniciativa de Ley que Establece la Obligación de Conservar Datos de Tráfico, Paraguay, Asunción, 11 de junio de 2014, Disponible en: http://sil2py.diputados.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F102821

sistema informático y que indica la dirección de IP, origen y destino de la misma, hora y fecha de la conexión y desconexión, itinerario, tamaño y duración de la comunicación." [27]

Asimismo, esta ley dictamina que la retención de datos se realizará sobre "todos los datos de tráfico generados" por un periodo de 12 meses. Mientras que la aplicabilidad recae sobre las personas físicas o jurídicas que "presenten o proporcionen" servicios de internet en Paraguay. Es importante agregar que la regulación es aplicable para toda persona dentro del territorio, sin embargo, no se expresan las especificaciones técnicas o de infraestructura para llevar a cabo esta medida.

En la actualidad, el proyecto se encuentra en proceso de aprobación tras una serie de modificaciones. Así, destaca el hecho que la Comisión de Derecho Humanos local lo ha rechazado en dos ocasiones, frenando su proceso de instauración por la incapacidad de garantizar los derechos fundamentales de los ciudadanos.

Otra de las principales críticas (principalmente realizada por medios y prensa) que distinguen a este caso es la obligación que tendrán las empresas para afrontar los gastos necesarios para cumplir con la ley. La preocupación radica en la posibilidad de la transferencia de este costo del oferente al consumidor. Esto indica que las empresas que proveen los servicios de telecomunicaciones podrían elevar los precios de mercado para solventar sus nuevos gastos a costa de los consumidores.

Reino Unido

En el 2012, el Reino Unido publicó una nueva Propuesta de Ley de Comunicaciones (Communications Data Bill)[28] con el objetivo de combatir el crimen en la región por medio de la retención de datos a lo largo de un periodo de 12 meses. Esta propuesta significaba el seguimiento de la Directiva de la Unión Europea en el 2006.

De manera similar, esta ley excluía los contenidos de estos datos y se enfocaba en fechas, emisores y receptores, así como localización de los datos generados, identificación del usuario y dirección IP, entre otras cosas. Mencionaba

[27] Iniciativa de Ley que Establece la Obligación de Conservar Datos de Tráfico, Artículo 3°, Asunción, 11 de junio de 2014. Disponible en: http://sil2py.diputados.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F102821

[28] Parliament UK, Draft Communications Data Bill, diciembre 2012. Disponible en: http://www.parliament.uk/draft-communications-bill/

cuáles eran las seis instituciones judiciales o de inteligencia que podían tener acceso a dicha información y permitía al Secretario de Estado agregar organismos por necesidad, como ha sucedido por ejemplo con la Autoridad Federal Financiera.[29]

En este contexto, una de las principales cuestiones que ha generado disgusto entre los proveedores de la región son los costos necesarios para llevar a cabo el almacenamiento y uso de información. De hecho, el mismo gobierno lo reconoce y estimó que el costo total de implementar esta ley sería equivalente a 1.8 billones de libras esterlinas para un periodo de diez años.[30] Traducido a pesos (con el tipo de cambio actual de 1 libra por 21.13 pesos) esto sería equivalente a 38.03 billones de pesos ó 3.8 billones de pesos anuales. Estos costos, en el caso de Reino Unido serían subsidiados en su totalidad por el gobierno.

Posteriormente, a raíz de la invalidación de la Directiva de la Unión Europea en 2014, se publicó un nuevo documento en Reino Unido para dar seguimiento a su política de retención de datos. Este documento fue la Propuesta de Ley sobre la Retención de Datos y Poderes Investigativos (Data Retention and Investigatory Powers Bill)[31] que brinda las facultades al Secretario de Estado, bajo argumentos de seguridad, para solicitar el almacenamiento (máximo por un año) de datos relevantes, a las compañías de telecomunicaciones. Es decir, que promueve la preservación de datos al estilo de Estados Unidos, no únicamente con un mandato de retención, sino también cuando sea solicitado explícitamente por el gobierno.

Asimismo, esta legislación ha sido criticada ya que, además de permitir el acceso a contenidos en casos judiciales, expande este derecho a entidades externas que mantengan una relación con Reino Unido. Por lo tanto, que al igual que la NSA en Estados Unidos, cuenta con la facultad de monitorear las comunicaciones foráneas cuando así se crea conveniente.

Suecia

En el caso de Suecia, forzado por la legislación europea en 2012 se implementó la retención de datos obligatoria por parte de los proveedores de servicios de Internet y telecomunicaciones con fundamento en la Directiva de Retención de Datos de 2006. De este modo, se determinó un periodo obligatorio de

[29] Parliament UK, What RIPA does and how the system currently functions. Disponible en: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7905.htm#a5

[30] Joint Committee on Draft Communications Data Bill, Draft Communications Data Bill, Written Evidence, 2012. Disponible en: http://www.parliament.uk/documents/joint-committees/communications-data/written-evidence-Volume.pdf

[31] Parliament UK, Data Retention and Investigatory Powers Act 2014. Disponible en: http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers.html

almacenamiento equivalente a seis meses y centrado específicamente en la recolección de metadatos.

Este esquema fue aplicado adecuadamente hasta 2014, año en que la invalidación de la legislación europea dio pie a una nueva discusión en el país. Inicialmente, la empresa proveedora de servicios de internet, Bahnhof, se resistió a continuar con el almacenamiento de los datos apoyándose en la previa anulación de la Directiva de Retención de datos europea, sin embargo, el gobierno sueco determinó que su legislación no violaba los derechos de privacidad cual previsto en la directiva.

Actualmente, Bahnhof (liderando un conjunto de proveedores de servicios como Telia, Tele2 y Three) enfrenta una demanda realizada por el gobierno sueco y ha solicitado el apoyo de la Unión Europea para sancionar la falta de atención del gobierno sueco respecto a la anulación de la Directiva de Retención de Datos.[32] Esto refleja la importante controversia que existe en estas medidas, no solamente en cuestión de derechos humanos, sino de costos e inversión para el sector privado y la injerencia que pueden tener los organismos regionales en este proceso.

Por otro lado, cabe destacar que Suecia cuenta con una agencia semejante a la NSA en Estados Unidos, conocida como el Establecimiento Nacional de Radio Defensa (FRA por sus siglas en sueco), que cuenta con la facultad de encargarse de la inteligencia de señales. Es decir, que de acuerdo con la controversial legislación establecida en 2008, puede monitorear el contenido de las comunicaciones de individuos únicamente con fines de seguridad nacional, por un periodo de seis meses, con la aprobación del Departamento de Defensa y Operaciones de Inteligencia, y en mensajes que crucen las fronteras externas del país, nunca a nivel nacional. La principal finalidad de ello es el combate al terrorismo y colaboración con otras agencias semejantes a nivel internacional, además de que se opera bajo la supervisión del Consejo de Inspección de Datos.[33]

[32] Loek Essers, Swedish ISP urges European Commission to end 'illegal data retention, in *Computer World UK*, septiembre 2014. Disponible en: http://www.computerworlduk.com/news/it-business/3571873/swedish-isp-urges-european-commission-to-end-illegal-data-retention/

[33] Library of Congress, Foreign Intelligence Gathering Laws: Sweden, Disponible en: http://www.loc.gov/law/help/foreign-intelligence-gathering/sweden.php

Legislaciones de Retención de Datos para la Prevención de Delitos

En términos generales, las legislaciones de retención de datos para la prevención de delitos han resultado polémicas a nivel internacional, por lo cual han tendido a ser derogadas o acotadas considerablemente. Por ello, existe un gran dinamismo en el tema y resulta de gran importancia conocer la experiencia que se ha llevado a cabo en distintas regiones.

A continuación se muestra un cuadro consolidado que sintetiza la postura de los países previamente mencionados en materia de regulación sobre retención y privacidad de datos:

Origen	Regulación	Descripción
Unión Europea	Directiva de Retención de Datos (2006)	• Datos Retenidos: Metadatos • Periodo de Retención: Entre 6 meses y 2 años • Las autoridades con acceso a los datos son designadas a nivel nacional • Invalidada en 2014
Alemania	Ley Federal de Protección de Datos (2003-2006)	• Datos Retenidos: Metadatos • Periodo de Retención: 6 meses • Establecimiento de principios para la protección y procesamiento de datos • Las autoridades con acceso a los datos son aquellas dedicadas a la procuración de la justicia
Argentina	Ley Nacional de Telecomunicaciones (1972)	• Inviolabilidad de correspondencia de telecomunicaciones
	Ley de Protección de Datos Personales (2000)	• Prohíbe la generación de registros o almacenamiento de datos personales • Protección integral de datos personales en distintos medios de tratamiento
Australia	Enmienda en Materia de Telecomunicaciones y Retención de Datos (2013-2014)	• Datos: Metadatos • Periodo de Retención: 2 años • Acceso a organismos de procuración judicial • Contempla costos financieros • Compatibilidad explícita con Derechos Humanos • Excluye la retención de datos generados por búsquedas en internet

Brasil	Marco Civil para el Internet (2010)	• Datos: Metadatos bajo proceso judicial • Periodo de Retención: 1 año • Impulsada en el marco de NETMundial • Protege a ciudadanos brasileños dentro y fuera del territorio, así como instituciones que sirvan a ciudadanos locales
España	Ley de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones (2007)	• Datos: Metadatos, excluye contenidos • Periodo de Retención: entre 1 y 2 años • Los miembros de fuerzas y cuerpos de seguridad, funcionarios Aduana y personal del Centro Nacional de Inteligencia pueden acceder a los datos. • España fue pionero en este tipo de regulación, antecediendo a la Unión Europea en 2002
Estados Unidos	Código de Privacidad de la Información del Consumidor, *Foreign Intelligence Surveillance Act* y *Patriot Act* (1986-2008)	• Datos: Metadatos y contenidos con fines de seguridad nacional • Periodo de Retención: 90 días, sujeto a petición gubernamental • Estados Unidos muestra un cúmulo de leyes interrelacionadas en la materia • La labor de la Asociación de Seguridad Nacional (NSA) ha destacado en el análisis y procesamiento de metadatos y contenidos • Brinda un trato distinto de acuerdo con la localización geográfica y origen de los usuarios
México	Ley Federal de Telecomunicaciones y Radiodifusión (2014)	• Datos: metadatos, salvo excepción judicial • Periodo de Retención: 2 años • Se encuentra en proceso de derivar en una legislación particular para protección de datos • Instituciones relacionadas con la procuración de justicia con acceso a datos, ya sea autoridades federales o el Ministerio Público local
Paraguay	Proyecto de Ley de Retención de Datos (2014)	• Datos: metadatos o datos de tráfico • Periodo de Retención: máximo 12 meses • Proceso legislativo frenado por comisión de derechos humanos local • No se han designado los organismos con posibilidad de acceso a la información
Reino Unido	Proyecto de Ley de Retención de Datos (2012)	• Datos: metadatos, excluye contenidos • Periodo de Retención de datos: 12 meses • Acceso a instituciones judiciales o de inteligencia, permite al Secretario de Estado agregar otros organismos

	Ley sobre la Retención de Datos y Poderes Investigativos (2014)	• A pesar de la invalidación de la Directiva de la Unión Europea, Reino Unido ha continuado esta corriente de legislación • Promueve preservación de datos estilo Estados Unidos y responde a solicitud explícita por el gobierno. • Susceptible a la inclusión de contenidos y monitoreo de comunicaciones foráneas en casos particulares
Suecia	Iniciativa de Retención de Datos (2012)	• Datos: metadatos • Periodo de Retención: 6 meses • Agencia FRA, encargada de la inteligencia de señales puede monitorear contenidos transfronterizos desde 2008 • Actual litigio contra proveedores de internet por controversia entre Directiva de la Unión Europea y legislación local

Fuente: Cuadro realizado por The Social Intelligence Unit

Como se aprecia en la tabla anterior, en la mayoría de los casos se tiende al manejo exclusivo de metadatos con el apoyo de los proveedores de servicios en un plazo entre 6 meses y dos años, además, dicha información se encuentra limitada al acceso de organismos especializados en la procuración de la ley. Sin embargo, existen algunos casos en que es posible acceder a contenidos estrictamente bajo la autorización de instituciones de inteligencia o judiciales.

Cabe hacer un último énfasis en las diferencias que existen entre los periodos para retención de datos en distintos países. Mientras que por ejemplo en Estados Unidos este tipo de práctica se realiza tan solo por 90 días (salvo petición expedita de la justicia) y en Alemania se respeta el plazo mínimo de 6 meses, en México se está recurriendo al plazo máximo permitido según la experiencia internacional de dos años. Si bien la Directiva de Retención de Datos de la Unión Europea de 2006 establecía este intervalo de tiempo como aceptable y recomendable, actualmente dicha legislación ha sido revocada, no resultando así un buen referente para regulación.

Costos de Implementación

Existen pocas estimaciones sobre los costos de implementación de las medidas de retención de datos. Esta escasez se debe a varias razones, entre las cuales se encuentra el rápido desarrollo de nuevas tecnologías, los constantes cambios de regulación en el ámbito y el hecho de que son pocos los países que han implementado de modo continuo dichas medidas hasta la fecha. Es importante recordar también que estas estimaciones difieren con el paso del tiempo, debido a que la cantidad de datos que transitan hoy en día por la red ha aumentado de manera importante en los últimos años.

Por otro lado, es necesario mencionar que gran parte de estas estimaciones son realizadas directamente por las empresas, por lo cual podrían sobreestimar los costos como una medida para evitar las regulaciones. Sin embargo, si algo es claro, es que el almacenamiento de grandes cantidades de información deriva en costos de operación que incluyen insumos como electricidad, mano de obra, software y hardware, entre otras cosas.

A continuación se muestra una tabla con algunos estimados de costos potenciales de retención y procesamiento de datos:

Localidad	Costo Estimado
Reino Unido	El gobierno del Reino Unido estima un costo de $2.77[34] billones de dólares[35] por un periodo de 10 años, tomando en cuenta una población aproximada de 63 millones de personas.[36] Por otro lado, la empresa America Online estimó que el costo de establecer un sistema de retención de datos en este país le sería equivalente a $46 millones de dólares[37] por año.[38]

[34] Utilizando un tipo de cambio de 1.5362 dólares por libra esterlina.
[35] Esta cantidad equivale a 41.32 billones de pesos con un tipo de cambio de 14.92 pesos por dólar
[36] Computerworld, Australia 2012, Disponible en: http://www.computerworld.com.au/article/434911/data_retention_could_cost_over_500m_comms_alliance_amta/
[37] Utilizando un tipo de cambio de 1.5362 dólares por libra esterlina.
[38] Kristina Ringland, The European Union's Data Retention Directive and the United States' Data Preservation Laws: Finding the Better Model, 5 SHIDLER J. L. COM. & TECH. 13 (2009), Disponible en: https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/427/vol5_no3_art13.pdf?sequence=1

Australia	En la legislación australiana se especifica que existirán impactos financieros derivados de implementar medidas de retención de datos. Por otro lado, la proveedora de internet australiana, iiNet, estima que el costo de la medida sería de $101 millones de dólares[39] al año:[40] $7.78 millones de dólares en electricidad $65.28 millones de dólares en infraestructura $27.98 millones de dólares en hardware Por otro lado, la Asociación de Telecomunicaciones Móviles Australiana (AMTA) indica que el costo de la medida para la industria superaría la cifra de medio billón de dólares australianos. Los costos de instauración serían equivalentes a $77.72 millones de dólares, y podrían llegar hasta $544 millones de dólares si se incluyen las direcciones IP.
Unión Europea	Se calcula que el costo de almacenamiento de datos por una empresa con medio millón de usuarios de internet sería de 0.85 dólares por individuo en el primer año y 0.27 dólares en los siguientes años.[41] Esta cifra se incrementa de forma importante si se pondera por el número de usuarios en cada país, y se agregan los datos correspondientes a otros servicios de telecomunicaciones.

Fuente: Cuadro realizado por The Social Intelligence Unit

Las estimaciones presentadas anteriormente refuerzan la idea de que el monitoreo continuo de datos deriva en amplios costos que deben de ser contemplados por los órganos reguladores antes de establecer una legislación, y que en caso de incluir contenidos serán mucho mayores. Asimismo, se requiere de una planeación cuidadosa para la implementación de modo que los costos no sean absorbidos por el consumidor final, ni perjudiquen sustancialmente al mercado de operadores de telecomunicaciones, derivando en una peor calidad de servicios.

[39] Utilizando un tipo de cambio de .7772 dólares por dólar australiano
[40] Business Insider Australia, 2014, Disponible en: http://www.businessinsider.com.au/australian-data-retention-plan-will-cost-consumers-130-year-says-iinet-2014-8
[41] European Digital Rights, Data Retention Directive 2011, Disponible en: https://www.edri.org/files/shadow_drd_report_110417.pdf

Conclusiones

Actualmente son varios los países que han incorporado en su regulación el monitoreo y la retención de datos de los usuarios de telecomunicaciones como un medio complementario para generar un entorno seguro. Sin embargo, la experiencia internacional muestra que existe una tendencia a la recopilación únicamente de metadatos, excluyendo la posibilidad de acceder a los contenidos generados por los consumidores.

En este sentido, la regulación del tipo de información que puede ser recaudada por un gobierno resulta de suma importancia para evitar que los intereses en el ámbito de la seguridad se opongan a los derechos fundamentales de los individuos. Evitar que las autoridades puedan acceder a los contenidos o mensajes de los usuarios responde a dos principales factores, que son por un lado la protección de la privacidad, y por el otro los altos costos que implica la implementación de este tipo de iniciativa.

Si bien la retención de datos es actualmente una acción complementaria fundamental para la seguridad de un país, conocer cuáles son las prácticas que se realizan a nivel internacional permite generar lineamientos eficientes y a la vez no intrusivos. Es decir, que brinda una guía para facilitar la toma de decisiones en los órganos regulatorios especializados regionales, permitiendo partir de experiencias tangibles.

Debe tomarse en cuenta que la retención de datos (aún con fines de seguridad) resulta un tema polémico independientemente de la región en que se regule. Esto ha generado un gran dinamismo en los últimos años, dando pie a constantes reconfiguraciones sobre todo en países desarrollados como Estados Unidos o en los miembros pertenecientes a la Unión Europea.

Por otro lado, es importante mencionar que este documento se encuentra centrado en particular, en la regulación sobre datos y privacidad a nivel nacional, pero también existen líneas de estudio con respecto a la política al exterior. Tomando en cuenta que la transmisión de información a través de la red se realiza sin fronteras, es posible profundizar en la investigación sobre el trato de datos de otros países o empresas transnacionales.