Acerca de la nueva política de Privacidad de Google

Maestropiedra Nicolás

Abogado, Universidad Nacional del La Plata,
Administración de Justicia,
Poder Judiacial de la Provincia de Buenos Aires

Abstract. This paper attempts to provide some elements of analysis on the importance to be the care in the responsible management of personal information. To undertake this analysis as part of the new privacy policy implemented by Google and are confronted with the law in Argentina for the Protection of Personal Data. The core is provided by contextualizing the description of some of the phenomena of the information society.

Keywords: Privacy Policy. Databases. Personal information. Privacy Policy. Information Society. Information Technology and Communication.

1 Introducción

Recientemente, el proveedor de servicios de Internet mas importante de la Web ha introducido cambios en su política de privacidad [1]. Según puede verse, la última modificación hecha por el gigante ha dejado parcialmentente sin efectos los acuerdos anteriores.
Guiado por el objetivo de optimizar los servicios prestados y con la intención de simplificar los esquemas de privacidad los usuarios deberán aceptar los nuevos parámetros de seguridad para seguir disfrutando de las aplicaciones dispuestas on line.
El eje de la cuestión en planteo intenta reflexionar sobre la importancia y alcances que hoy en día tienen las “políticas de privacidad” tomando como punto de análisis la implementada por Google desde marzo de 2012.

2 Cambios mas relevantes

Normalmente las políticas de privacidad se desarrollan bajo tres ejes; Qué datos se recogen, Cómo se recogen, y Como se utilizan.

2.1 Que datos se recogen

El dato es una representación simbólica (numérica, alfabética, algorítmica, entre otros), un atributo o característica de una entidad. Los datos describen hechos empíricos, sucesos y entidades.
Reflexionar acerca de qué datos son recogidos implica adentrar en la materia objeto de protección jurídica por parte de los ordenamientos jurídicos. En nuestro caso se trata del bien jurídico que el ordenamiento argentino ha decidido proteger a través de la sanción de la ley 25.326 al respecto de lo cual nos expediremos en el apartado sobre las "consideraciones legales".
Sin embargo, y para un mejor entendimiento, se vuelve imprescindible hacer mención al fenómeno de "nube de servicios" o Software as a Service (SaaS) ¿que significa esto?
Como consideración de una de las nuevas tendencias en las Tecnologías de la Información y Comunicación se da por instalada la idea de que los usuarios comparten datos con los prestadores de servicios Web.
Ser usuario de alguno de los servicios de google implica tácitamente la adhesión a esta idea;
"*Cuando compartes datos con nosotros (por ejemplo, al crear una* cuenta de Google*)* [6]"
Esta consideración es el punto de partida. Se trata de una adhesión implícita que legitima una amplia gama de procedimientos de tratamiento de información personal por parte del prestador de servicios. Es el usuario el que comparte datos con Google, por medio de una suerte de "consentimiento informado" normalmente expresada a través de la adhesión a la política de privacidad.[1]
Según las nuevas disposiciones en la política de privacidad de la información Google está en condiciones de tomar datos del Dispositivo que se utiliza[2] ;
"*Podremos recoger datos específicos sobre tu dispositivo (como, por ejemplo, el modelo de equipo, la versión del sistema operativo, los identificadores únicos y los datos sobre la red móvil, incluyendo el número de teléfono). Google podrá asociar los identificadores de tu dispositivo o tu número de teléfono con tu cuenta de Google.*
También se podrán tomar Datos sobre tu ubicación física;
"Al utilizar un servicio de Google que pueda registrar tu ubicación física, podremos llevar a cabo la recogida y el tratamiento de datos acerca de tu ubicación real como, por ejemplo, las señales de GPS enviadas por un dispositivo móvil, información sobre los puntos de acceso Wi-Fi y las antenas de telefonía móvil más cercanos"

2.2 Como se recogen los datos

Respecto de cómo se recogen los datos Google advierte sobre dos "maneras"de

1 Esta cuestión será mas ampliamente desarrollada en el apartado de las consideraciones sobre la sociedad de la información junto con otros fenómenos
2 El concepto de "dispositivo" es utilizado con un alcance mas amplio que el de la sola PC, y abarca telefónos, tablets, computadoras, cualquier dispositivo con capacidad de conexión web.

proceder: por un lado *Información libremente facilitada por el usuario*, y por el otro *Datos que obtenemos a través de la utilización de nuestros servicios.*
En el primer caso no habría mayores consideraciones que hacer en tanto se trata de datos personales que el usuario libremente proporciona al momento de crear una cuenta o adherir a un servicio.
Pero los interrogantes se abren en el segundo de los supuestos, es decir, cuando el prestador obtiene datos por la mera utilización de alguna de sus prestaciones. En este ultimo caso la nueva política de privacidad explica que cuando se accede a algunos de los servicios prestados se podrán recoger datos sobre el uso que se haga de ellos. Esto se explisita como: Datos de registro;
"*Cada vez que uses nuestros servicios o que consultes nuestro contenido, es posible que obtengamos y que almacenemos determinada información en los* registros del servidor *de forma automática. Estos datos podrán incluir: información detallada sobre cómo utilizas nuestro servicio (por ejemplo, tus consultas de búsqueda)* como así también *datos telefónicos como, por ejemplo, tu número de teléfono, el número de la persona que realiza la llamada, los números de desvío, la hora y fecha de las llamadas, la duración de las llamadas, información sobre el enrutamiento de mensajes SMS y tipos de llamadas,* la dirección IP, información relativa a tu dispositivo como, por ejemplo, fallos, actividad del sistema, ajustes del hardware, tipo de navegador, idioma del navegador, fecha y hora de tu solicitud y URL de referencia, cookies, que permitirán identificar tu navegador o tu cuenta de Google**."**
Las facultades de recabar información por parte de google son amplias, quedando expresamente plasmado en su política que: "*Podremos recoger y almacenar datos (incluyendo datos de carácter personal) de forma local en el dispositivo utilizando mecanismos, como el almacenamiento web del navegador (incluyendo HTML5) y memorias caché de datos de aplicaciones."* para lo cual "*Utilizamos diferentes tecnologías para recoger y almacenar datos cuando accedes a un servicio de Google, incluyendo el envío de una o varias* cookies *o de* identificadores anónimos *a tu dispositivo*"

2.3 Como es el tratamiento de esos datos

Los datos aisladamente pueden no contener información humanamente relevante. Sólo cuando un grupo de datos se examina conjuntamente a la luz de un enfoque, hipótesis o teoría se puede apreciar la información contenida en dichos datos. Los datos convenientemente agrupados, estructurados e interpretados se consideran que son la base de la información humanamente relevante que se puede utilizar en la toma de decisiones, la reducción de la incertidumbre o la realización de cálculos [2].
El procesamiento de datos personales es una de las cuestiones mas álgidas del tema, porque normalmente los prestadores no reparan en explicar claramente que utilidad harán del dato recogido y es bastante común la utilización de ciertas expresiones de contornos difusos como "*mejorar la experiencia del usuario*", "*la calidad general de nuestros servicios*" u "*ofrecerte contenido personalizado*"
Google expresa en primer termino que "*Los datos que recogemos a través de todos nuestros servicios se utilizan para prestar, mantener, proteger y mejorar dichos servicios, desarrollar nuevos servicios y velar por la protección de Google y de*

nuestros usuarios"
Las problemáticas generadas entorno al tratamiento de datos personales están estrechamente asociadas con la práctica de cruzamiento de bases de datos lo que implica la posibilidad de recrear un perfil del usuario;
"*Podemos combinar la información personal de un servicio con la información de otros servicios de Google, incluida la información personal, para que puedas compartir contenido con usuarios que conozcas más fácilmente, entre otros usos... Por ejemplo, al guardar tus preferencias de idioma, podremos hacer que nuestros servicios se muestren en el idioma que prefieras. Cuando te mostremos anuncios personalizados, no asociaremos cookies o identificadores anónimos a datos especialmente protegidos como, por ejemplo, los relativos a raza, religión, orientación sexual o salud."*
Existen serias consideraciones en el tratamiento que se hace de la información personal por más que en las políticas implementadas se asegure requerir el consentimiento antes de utilizar los datos para cualquier fin distinto de los establecidos.
El dato por si solo no es una información, pero si lo es la inferencia de conocimientos emergentes de la asociación de dos o mas datos. La potencialidad de asociación de datos permite recrear un conjunto de información ampliada relativa a diversos aspectos de la vida de una persona, desde preferencias comerciales hasta su orientación sexual.

3 Consideraciones legales

En Argentina la Ley 25.326, de Protección de Datos Personales, es la encargada de regular lo atinente al tratamiento de informaciones personales. El artículo primero determina como su objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios tecnológicos de tratamiento de datos, asi sean estos públicos o privados.
Como primer inquietud cabe preguntarse si la ley de Protección de Datos Personales es aplicable a los prestadores de servicios como Google, lo cual implicaría la posibilidad de considerar al prestador, también, como un administrador de archivos.
El "tratamiento de datos" es el eje de la cuestión, de eso se trata, puesto que toda actividad de recolección implica siempre un cierto grado de "tratamiento". Normalmente la manipulación de datos comienza por la recopilación pero continúa con otro tipo de acciones como: clasificación, etiquetamiento, almacenamiento, indexación, etc.
En este sentido la ley entiende al Tratamiento de datos como *operaciones y procedimientos sistemáticos, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales.*
El artículo primero de la citada norma al momento de determinar el objeto propio de protección hace referencia a datos personales asentados en archivos, registros, bancos o bases de datos**.** En esta inteligencia no hay duda que muchas de las "actividades" desenvueltas por Google implican un tratamiento de datos, sea por medio de

recolección o que simplemente se limite a tomar datos de los registros de los usuarios. Por esta razón el prestador de servicios estaría dentro del supuesto previsto en el artículo primero.

La autonomía de la voluntad sigue siendo, aun a pesar de los desmedros o avasallamientos, uno de los pilares fundamentales de la libertad individual, protegida por todos los ordenamientos jurídicos en general y en particular por numerosas leyes. En este sentido el artículo 7 de la Ley 25326 expresa que ninguna persona puede ser obligada a proporcionar datos sensibles. Esto es: datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual[3].

Este principio deja a salvo la legalidad del los datos sensibles libremente proporcionados por su titular, razón por la cuál no cabría responsabilidad civil por su obtención en esos casos.

Al respecto de como debe ser la recolección de los datos personales dicho procedimiento no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley (Art. 4). La licitud en el tratamiento implica el necesario consentimiento libre, expreso e informado de la persona (Art.5). Sin embargo la ley admite otras formas de consentimiento por otro medio que permita se le equipare, de acuerdo a las circunstancias.

En este sentido el artículo 4° de la reglamentación de la ley, decreto 1558/2001, hace un aporte significativo afirmando que para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos.

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: la finalidad para la que serán tratados, la identidad y domicilio de su responsable. (Art. 6)

El artículo 5° del decreto reglamentario también viene a hacer un aporte en este sentido dejando de manifiesto que el consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural.

Relativo a como debe ser el tratamiento que se puede hacer de esos datos se expresa que no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención (Art. 6).

En consecuencia el marco regulatorio se expide haciendo referencia a las responsabilidades de los titulares de bancos de datos las cuales no terminan en el correcto deber de información, sino mas bien, allí empiezan.

El responsable o usuario de archivos de datos tiene un doble deber de mantener la seguridad de los datos y preservar la confidencialidad de los mismos. Al respecto de lo cual los artículos 9 y 10 dicen: El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales; Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad; El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos.

La Dirección Nacional de Protección de Datos Personales en sus facultades de policía

ha aprobado disposiciones relativas a medidas de seguridad sobre informaciones personales tanto en Archivos y Registros Públicos como Privados[4].
Como contracara de los deberes de seguridad y confidencialidad se manifiestan las acciones protectorias. El Hábeas Data es la acción por excelencia para la tutela efectiva del derecho sobre las fuentes de información personal, contemplada en el Art. 33 de la ley, pero con reconocimiento constitucional efectivo desde 1994 (Art. 43 C.N.).
Se trata de la acción que busca garantizar la posibilidad de tomar conocimiento de los datos personales almacenados, como exigir su rectificación, supresión, confidencialidad o *actualización*.
La legitimación activa estará en cabeza del principal afectado, sus tutores, curadores o sucesores. A si mismo también podrá se ejercida por los representantes legales cuando se trate de personas de existencia ideal (Art. 34)
La competencia para entender en esta acción corresponde al juez del domicilio del actor (Art. 36). Sin embargo es de tener en cuenta el articulo 12 del Decreto reglamentario en el que se manifiesta que la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular del los datos hubiera consentido expresamente la cesión.
La acción de habeas data tramitará según las disposiciones de la ley de Protección de Datos Personales y por el procedimiento que corresponde a la acción de amparo y supletoriamente por las normas atinentes al juicio sumarísimo.
Por ultimo mencionar que el control de las disposiciones legales corresponde a la Dirección Nacional de Protección de Datos Personales. El conjunto de prerrogativas en la esfera de su competencia incluye entre otras tantas llevar un registro de los administradores de bases de datos hasta homologar los código de conducta pasando por la aplicación de sanciones administrativas.

4 Consideraciones sobre la sociedad de la información

El análisis de las políticas de privacidad debe hacerse en el contexto del actual paradigma de las TIC's.
Uno de los fenómenos sociales y tecnológicos entorno a las nuevas tecnologías es el Cloud Computing. Este concepto evoca la idea de que todo lo que puede ofrecer un sistema informático se pueda ofrece como *servicio* de modo que los usuarios pueden acceder a los servicios disponibles “en la nube de Internet” sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan[3].
En este punto se produce uno de los cambios mas relevantes. Tradicionalmente la forma de almacenamiento de información fué en los dispositivos personales, discos rígidos de PC principalmente, memorias, disketts etc. Ahora la información se “aloja”

3 Según el IEEE Computer Society, es un paradigma en el que la información se almacena de manera permanente en servidores de Interntet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc

en un servidor[4] pudiendo estar disponible total o parcialmente tanto para su propietario como para otros usuarios.
Como consecuencia de ello, la forma de evocar esa información cambió. Se necesita una conexión necesaria para acceder a ella cada vez que se la requiera. Otra consecuencia, quizás la mas relevante, es que esto ha implicado un cambió en el tratamiento de la información personal[5]. En un primer momento el usuario tenía toda su información de interés en su poder y normalmente decidía compartir una porción de ella "subiéndola" a la red. Desde hace un tiempo la tendencia ha cambiado; el usuario tiene la mayoría de su información personal en la Web y decide "bajarla" a la memoria caché de su PC cada vez que la necesita. En este sentido están concentrando sus fuerzas muchos de los grandes operadores tecnológicos[5].
El cloud computing es la tendencia tecnológica que incorpora el Software como servicio. Por esta razón, es que los prestadores de servicios Web tienen que ver y rever frecuentemente la performance de sus políticas de privacidad.
La tendencia a la computación en nube está relacionada con el fenómeno de la publicidad de los actos propios. Comienza a implementarse terminología como social-media. Para algunos se trata de la simple implementación de los recursos de las TIC's en los ya conocidos fenómenos de relacionamientos sociales, mientras que para otros, implica una novedad dada por los nuevos alcances que permiten las RSI o Social Networking Services. La característica mas saliente de estas nuevas formas de comportamiento social tienen que ver con la modalidad de hacer publico (hacer accesible a los demás) un cúmulo considerable de información personal. Se ha producido un cambio en la valoración de la información, en la medida en que se la pueda hacerla conocer a otros valdrá mas que estando a resguardo.

5 Algunos puntos para reflexionar

La ley de Protección de Datos Personales es fundamental por tratarse de la primera instancia de protección legal al mismo tiempo que la base o sustento sin la cual no sería posible accionar contra actividades que impliquen un desmedro de los derechos reconocidos. Esta legislación cumple con los objetivos de regular la actividad y considerar los derechos en juego.
La ley ha querido reconocer como uno de los principios generales la licitud de la actividad de recolección y tratamiento (art. 3) agregando que el almacenamiento de datos es lícito en la medida que se encuentren debidamenete inscripto y siempre que su finalidad no sea contraria a las leyes o a la moral pública.
La ley de Protección de Datos Personales refuerza y sustenta el principio legal de que nigún derecho es absoluto (art. 1071 C.C.) y que la ley puede regular el ejercicio

4 Según afirman algunos pensadores este es uno de los fenómenos caracterizadores de la sociedad de la información en el cual, la información fluye desde los particulares/usuarios hacia los otros usuarios. Encuadra en el paradigma del liberación de las fuentes de información.
5 Como ejemplos de esto puede verse Dropbox, iCloud, Skydrive de Microsoft, entre otros.

normal de un derecho (art. 14 C.N.). En este sentido cumple en regular una situación de hecho innegable al mismo tiempo que reconoce que derechos y obligaciones les asisten a cada uno de los involucrados.

La posibilidad de recabar, almacenar y procesar información es legal aun incluso cuando se trate de datos sensibles puesto que el legislador ha querido poner en cabeza del titular de los datos la facultad de negarse a proporcionarlos (art. 7) pero no la prohibición a recolectarlos. En este sentido podemos afirmar que no hay ningun problema en que Google almacene y trate datos personales.

El campo de las objeciones está planteado por la utilización de herramientas tecnologícas capaces de recabar información de un modo anónimo, permanente, o indiscriminado. La utilización de identificadores anónimos deja varios interrogantes; ¿que son? ¿como funcionan? ¿donde se instálan? ¿que facultades de contról tienen los usuarios al respecto?... La implementación de estas tecnologías suponen un doble peligro, por un lado un cierto grado de injerencia en la vida privada de los usuarios, y por otro la resignacion de las facultades de control sobre ellas. Estas tecnologías ponen en juaque el principio de consentimiento libre y expreso a la hora de proporcionar información.

Otro debate pendiente es el que emerge de los perfiles creados. La posibilidad de disponer de un grán cumulo de información personal abre nuevos horizontes para sociabilizar gustos, preferencias, orientaciones, ideologias etc, pero también puede suponer su tuilizacion con objetivos de control. Entonces es válido preguntarse ¿está permitido crear perfiles? ¿con que finalidades se crean? ¿que indices de valoración se hará de nuestra información? Las guias de buenas prácticas de la DNPDP determinan la necesaria disociación de los datos de carácter sencible. Esto es la necesidad de atomizar el dato al punto de que no pueda ser posible identificarlo con persona alguna. La finalidad que se busca es evitar la proliferación de perfiles. En este aspecto la nueva política de privacidad no se expide.

¿Que hay respecto de la cesión de datos y jurisdicción aplicable? La información es un bien por demás apreciado en una sociedad que busca personalizar la oferta de productos y customizar los servicios de modo que no es posible ignorar el valor económico que esto representa.

El principio receptado en la normativa argentina es la prohibición de transferencia de datos, salvo las excepciones previstas. Sin embargo los datos pueden ser cedidos con el consentimiento del titular. En estos supustos se requerirá que se le informe sobre la finalidad de esa cesion. La nueva politica de privacidad asegura no compartir los datos personales aunque por razones legales de cooperación internacional y a requerimiento de organismos administrativos y/o judiciales Google puede facilitar la información disponible y tambien transferirla. Se trata de algunos de los supuestos de excepción previstos por la ley argentina, con lo cual no habría infracciones legales en principio.

La nueva política de privacidad no hace mención de la jurisdicción aplicable ni sobre la competencia de ningún tribunal. Siguiendo los principios del Derecho Internacional Privado y en concordancia con la ley de protección de datos Presonales es competente el juez del domicilio del actor, y en caso de existir un planteo legal será necesario traer al prestador de servicios en su calidad de administrador de bases de datos a juicio. La competencia será de la justicia federal si los datos se encontraren alojados en bases internacionales o interjurisdiccionales.

6 Para concluir

La actualidad de las TIC's invita a celebrar un nuevo paradigma comunicacional pero también emerge la necesidad de fomentar una utilización responsable de ellas. Lejos de las normas y los imperativos, los usuarios de la Sociedad de la Información debemos trabajar para una educación en el uso responsable y un consumo conciente de las erramientas a nuestro alcance. La responsabilidad de los administradores de datos puede verser reflejada en las constantes actualizaciones que hacen de sus políticas de privacidad y en la proliferacion de movimientos que buscan resguardar estos bienes. Los usuarios somos los principales responsables de velar por la veracidad y fidelidad de los datos asentados sobre cualquier base o registro.

[1] Puede accederse a la nueva política desde https://www.google.com/intl/es/policies/privacy/

[2] Vease al respecto http://es.wikipedia.org/wiki/Dato o también http://www.dataliberation.org/

[3] Vease al respecto la Disposición 7/2008 de la Dirección Nacional de Protección de Datos Personales: "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ambito Público" y el texto modelo de "Convenio de Confidencialidad".Bs. As., 22/8/2008 en http://www.jus.gov.ar/datos-personales.aspx/

[4] Vease al respecto las disposiciones de la DNPDP 11/2006 y 7/2008

[5]Vease http://www.lanacion.com.ar/1467568-mas-alternativas-para-guardar-tus-archivos-en-linea

[6] Información disponible en https://www.google.com/intl/es/policies/privacy/key-terms/#toc-terms-account