Protección de datos y privacidad: problemas no resueltos

EGBERT J. SÁNCHEZ VANDERKAST
Universidad Nacional Autónoma de México

INTRODUCCIÓN

Datos personales y privacidad son temas que han ganado un espacio tanto en la agenda pública como en el ámbito académico. Raab y Mason[1] consideran la privacidad conjuntamente con la *surveillance*; para ellos, la confianza y la regulación son temas controvertidos del área de la información, así como de la propia práctica. Si bien han sido temáticas latentes desde sus inicios, en los años ochenta, siguen siendo de actualidad para su estudio y discusión en el ámbito académico. Debe quedar claro que la privacidad y temáticas relacionadas comparten visiones diferentes, que tienden a ser subjetivas y que constituyen procesos y relaciones estructuradas de acuerdo con las situaciones actuales. Dichos autores aluden, también, a la existencia de muchas perspectivas disciplinarias, desde las cuales se puede realizar investigación sobre tales asuntos,

1 Charles Raab y David Mason (2002), "Privacy, Surveillance, Trust and Regulation", pp. 237-241.

como las ciencias sociales, la informática, la filosofía, el derecho, los estudios de la información y la bibliotecología, entre otras.

El panorama sobre los procesos que sigue la información (denominados ciclo de vida) y los fenómenos surgidos que giraron alrededor de las Tecnologías de Información y Comunicación (TIC), de los sistemas de información y de los procesos de la comunicación en sí, tuvieron un cambio brusco después de septiembre de 2001, y una influencia marcada en los proceso sociales, políticos, económicos y culturales. Este parteaguas en la sociedad del siglo XXI sigue teniendo resonancia hasta la fecha de manera contundente, y ha contribuido a cambios trascendentales en la protección de datos y la privacidad. Todo lo anterior la IFLA lo sintetizó en tres puntos:

1. Las sociedades democráticas llegarán a ser menos democráticas.
2. Se desmoronarán regímenes democráticos como resultado del uso de Internet.
3. Se diferenciarán regímenes democráticos, que continuarán siendo más participativos y transparente mediante la tecnología, de los regímenes autoritarios, que la aprovecharán para fortalecer el control y vigilancia sobre los pueblos.[2]

Se destaca que el esfuerzo para tener sociedades democráticas va a quedar en el intento, y que Internet, proclamado como el instrumento promotor de sociedades democráticas, también sirve como un arma que derrumba regímenes tanto democráticos como autoritarios. Asimismo, se destaca que

2 IFLA. *Reporte Ejecutivo*. Síntesis de la Reunión de Expertos sobre el Informa de Tendencias de IFLA, celebrada los días 4 y 5 de marzo de 2013 en la ciudad de México, en el marco de la Reunión Presidencial de IFLA, p. 20.

la tecnología de información y de comunicación sigue siendo un medio abierto y, a través de él, se establecen flujos de información de toda índole.

Una de las preguntas surgida en todo este mar de afirmaciones que se presenta es la siguiente: ¿el peso del problema central recae encima de la privacidad y la protección de los datos?, o más bien, ¿es un problema de vigilancia o *surveillance*?

Protección de datos y privacidad

La IFLA hace patente que "[…] los límites de la privacidad y la protección de datos se redefinirán".[3] Y afirma que "[…] los grandes volúmenes de datos están en poder de los gobiernos y las empresas y sustentarán la elaboración de perfiles avanzados de cada individuo, mientras que sofisticados métodos de monitoreo y filtración de datos mediante las telecomunicaciones harán seguimiento de las personas más fácil y barato." Esto debido a:

- La avanzada capacidad de procesamiento de datos.
- Las nuevas prácticas para filtrar y rastrear grandes volúmenes de datos.
- El constante monitoreo a través del *tracking* y movimiento de retina.
- La fuerte demanda de los servicios de bienes con base en los datos personales.
- Los cambios en los escenarios, presiones de los gobiernos sobre las empresas en caso especifico de las multinacionales de Internet para la entrega de datos.

3 IFLA (2013), *¿Surcando las olas o atrapados en la marea?: Navegando el entrono en evolución de la información. Percepciones del IFLA Trend Report*, Tendencia número 3.

- Cambio en los niveles de confianza en el mundo digital.[4]

La percepción de IFLA es acorde a nuestros tiempos ya que, desde 1984, la ley del Reino Unido, Data Protection Act, ha marcado algunas pautas para el desarrollo de la protección de datos. Concuerdo con Stephen Flood[5]quien, en 1985, manifestó que hay un dinamismo que gira alrededor a la "protección de datos". En la ley sobre protección de datos perseguía el objetivo de "[…] crear un registro de organizaciones o de individuos que tuvieran datos personales en un sistema computarizado."[6]

El registro, en este sentido, se convierte en un instrumento cuyo propósito es la descripción de los datos personales. Esto indica a quien los posee, si el individuo o la institución, y cómo fueron obtenidos los datos y cómo se divulgan. Para ello habría que abrir los puntos de acceso, los cuales deben tener una estructura clara; deben ser expresados en términos simples y exhibir públicamente los propósitos comparables. Destacan los principios que motivaron tanto el registro como los procesos asentados, lo cual abarca la disponibilidad de las formas para realizar los tipos de registros que contienen detalles de los usuarios.

Los motivos para crear los datos personales son: conocer sus fuentes de obtención, con quiénes se compartieron los datos y el uso de descripción estandarizado. Mientras que el acceso podía ser a través de teléfono, servicio postal o a través de la biblioteca pública. La biblioteca del Reino Unido en esa década jugaba un papel muy importante en la diseminación de la información gubernamental y en la protección de los datos.

4 *Ídem*.
5 Stephen Flood (1985), "The Data Protection Register – content and access".
6 *Ibíd*., p. 75.

Otra forma de percibir la protección de datos es a partir de la Convención de Schengen, que tiene como objetivo la abolición del control en la frontera interna de los países que comparten *espacio de Schengen*, por una serie de arreglos y transferencias de control sobre la movilidad de personas, bienes en los territorios de los países miembros, es decir, la eliminación de la frontera interna del *espacio de Schengen*.[7]

El intercambio de datos personales entre las autoridades de los países miembros del Acuerdo de Schengen es principalmente sobre:

- Personas que buscan asilo político.
- Personas que son buscadas para un arresto.
- Personas o vehículos desaparecidos,
- Testigos o personas que deben aparecer ante la corte de justicia.

Para los fines de este convenio, se creó el Sistema de Información Schengen (SIS), que tiene como función: "Garantizar la integridad de los datos y asegurar de manera permanente el intercambio de datos entre la policía, los cuales están en manos de las autoridades que controlan la protección nacional de datos".[8]

El Sistema de Información Schengen (SIS), de acuerdo con Dumortier,[9] categoriza la información según su contenido en:

- Los datos: concernientes a personas, datos relativos a personas, familia y otros objetos (robados, extraviados,

7 Véase Jos Dumontier, "The Protección of Personal Data in the Schengen Convention", p. 94
8 *Ibíd.*, p. 95.
9 *Ibíd.*, pp. 96-97.

armas, documentos bancarios, documentos de identificación).
- Personas: buscadas para su arresto; individuos con reporte de negación de entrada a los países miembros del Acuerdo de Schengen; personas desaparecidas, testigos, personas o vehículos con propósito de *surveillance.*
- Acciones: un informe que solicita un Estado miembro de Schengen para una acción específica; por ejemplo, extradición.

En este caso, los datos personales son utilizados para ejecutar acciones solicitadas por las partes, como:

- Extradición.
- Extranjero-fugitivo.
- Testigo para comparecer ante la corte de justicia.
- Revisión / vigilancia de personas o vehículos.
- Objetos extraviados o robados, como motores de vehículos, armas, papeles bancarios, documentos de identificación, entre otros.

Concuerdo con Blume[10] acerca de la importancia que la protección de datos recobra en el entorno jurídico, circundado por la tecnología de la información y la sociedad de la información. Para ello, se han elaborado disposiciones legales con el propósito de salvaguardar la privacidad y, en la mayoría de los casos, imponer obstáculos sobre el uso de la tecnología y en el intercambio, a nivel internacional, de datos personales; por ello, hay que estar conscientes de que los procesos de internacionalización han incrementado la necesidad de mayor vigilancia de información transfronteriza, en particular de los datos personales.

10 Peter Blume, "Introduction" (1997), pp. 7-10.

PERSPECTIVA DE POLÍTICA PÚBLICA

Ya hay una nueva perspectiva sobre la protección de datos, pues sólo existía un enfoque desde la administración pública. Sin embargo, autores como Lyon,[11] Haggerty y Ericson,[12] advierten la perspectiva de vigilancia, o *surveillance,* y otras como parte de la privacidad.

Saarenpaa,[13] al profundizar en la protección de datos personales, considera que no es fácil poner en práctica los principios de publicidad y los principios de privacidad, ya que hay una costumbre implícita de poner más atención en los principios de derecho al acceso y en cómo garantizar el acceso. Para ello, Saarenpaa considera que la protección de datos debe ser vista como el respeto hacia el individuo, hacia la persona, es decir, desde un elemento vital de una sociedad, "[…] ya que las personas pueden confiar en la pertenencia del mantenimiento de los archivos/registros de los datos […] debemos respetar al individuo que se encuentra detrás del número personal de identidad."[14]

Una ley sobre datos personales es indispensable en una sociedad de la información. Por lo anteriormente indicado, Saarenpaa manifestó que:

> [por] el respeto hacia las personas estamos obligados a trazar una línea entre lo privado y la publicidad de los datos. En el proceso emergen dos asuntos que requieren un acercamiento minucioso en un Estado legal, constitucional y democrático que busca defender el principio de publicidad. En primer lugar está la relación

11 Véase David Lyon (2002), "Everyday Surveillance: Personal Data and Social Classifications", pp. 242-257.

12 Véase Haggerty Kevin y Richard Ericson (2000), "The surveillance assemblage", pp. 605-622.

13 Athi Saarenpaa (1997), "Data Protection: In Pursuit of Information. Some Background to, and Implementations of Data Protection in Finland", pp. 47-64.

14 *Ibíd.*, pp. 50-51.

> entre la legislación sobre protección de datos y el derecho a la información. Y en segundo, la posible diferencia entre el papel del individuo que asume un rol público o privado.[15]

Esto significa que el debate va más allá de la protección de datos, ya que tiene un trasfondo económico y de autodeterminación. En este contexto, Saarenpaa advierte que el ciudadano es visto como un sujeto administrativo que está obligado a entregar sus datos al gobierno, el cual recopila aquellos que son de importancia para la sociedad y que pueden ser utilizados para fines comerciales. Sin embargo, esto último debe ser visto de acuerdo a los contextos de cada Estado–nación y de las convenciones firmadas.

Sobre el particular, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 –relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos– en su articulo 13 indica que "[…] el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado."[16]

Concuerdo con el autor acerca de que el ciudadano tiene que tomar la decisión sobre la autodeterminación de sus datos, es decir, sobre el contenido de sus datos. Esto debido a que dicha Directiva estipula "[…] en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir y manejar, registrar, conservar o comunicar los datos relativos a las personas físicas, constituidos por sonidos, imágenes, la presente Directiva habrá de aplicarse a los tratamientos que afecten dichos datos."[17]

---

15 *Ibíd*. pp.53.
16 Euro-Lex, *Access to European Union Law*. Document 31995L0046. Directiva 95/46/CE.
17 *Ibíd*.

El derecho de autodeterminación del cual habla Saarenpaa gira alrededor de los derechos humanos, y considera que se debería tomar como principio:

1. El derecho de libertad interna.
2. El derecho de libertad externa.
3. El derecho de competencia.
4. El derecho de poder.[18]

Ante una situación similar, habrá que tomar en consideración los principios que Armagnague[19] señala:

1. El principio de pertenencia; donde los datos deben estar relacionados con los fines perseguidos al crearse el fichero o base de datos.
2. El principio de utilización no abusiva; "[…] los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".
3. Principio de exactitud o de calidad; el responsable del fichero (o base de datos), o tratamiento, deberá realizar los actos útiles para constatar la exactitud de los datos registrados y asegurarse de que estén al día. En caso de que los datos resultaran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos, rectificados o completados.
4. Principio de derecho de olvido; los datos de carácter personal serán cancelados cuando hayan dejado de

18 Saarenpaa, *Op. cit.*, p. 60.

19 Juan F. Armagnague (2002), "El derecho comparado en la protección de datos", pp. 375-415.

ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permitan la identificación del interesado durante un periodo superior al necesario para los fines con base en los cuales hubieran sido recabados o registrados.

5. Principio de lealtad; se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Esto se puede percibir desde dos perspectivas: 1) lo ético y 2) lo jurídico, como una transgresión donde "[…] son infracciones muy graves: la recogida de datos en forma engañosa y fraudulenta."[20]
6. Principio de publicidad o un registro de consulta pública expresado:
   i) Registro General de Protección de Datos; un órgano integrado como una agencia de protección de datos.
   ii) Serán objeto de inscripción en el Registro General de Protección de Datos:
      a) Los ficheros de los cuales sean titulares las administraciones públicas.
      b) Los ficheros de titularidad privada.
      c) Las autorizaciones a que se refiere la ley o normativa.
      d) Los códigos tipo a que se refiere la ley o normativa.
      e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación cancelación y oposición.

20 Armagnague, *Op. cit.*, pp. 381.

iii) Regular el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada.

7. Principio de consentimiento:
   i) el *consentimiento de interesado;* toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernen.
   ii) el *consentimiento del afectado*; el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
   iii) el *consentimiento inequívoco*; no será preciso el consentimiento cuando los datos de carácter personal se recojan por el ejercicio de las funciones propias de las administraciones partes de un contrato o precontrato de una relación [de negocio], laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.[21]

El principio de consentimiento alberga los datos sensibles, también denominados datos especiales, y son aquellos que afectan aspectos de la personalidad humana que requieren de especial atención: aquellos de carácter ideológico o referido a las intimidades. Bajo este rubro se ubica la ideología, la religión y las creencias, por lo que se requiere el consentimiento expreso y por escrito para el tratamiento de datos de relativo a la ideología, la afiliación sindical, la religión y las creencias. Se ubican también "Los datos de

21 Es una cita inextensa de los siete principios que argumenta Armagnague.

carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga la normativa o el afectado consienta expresamente". Velar por la seguridad de los datos y la cesión de ellos está muy ligado al principio de consentimiento.

Cada uno de los siete principios que Armagnague discute, amplía los derechos mencionados por Saarenpaa. Por otro lado, se encuentran los derechos de personas, como son:

- Derecho de no soportar valoraciones automáticas: los ciudadanos tienen el derecho de no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
- Derecho de consulta: la consulta del registro será pública y gratuita.
- Derecho al acceso: centrado en el interesado.
- Derecho de rectificación: los datos personales que resulten inexactos o incompletos pueden ser rectificados por el interesado en el registro respectivo.
- Derecho de cancelación: el efecto que produce la cancelación "[…] dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento."[22]

La normatividad jurídica mencionada obedece a una cultura basada en las tecnologías de información y comunicación, en las cuales las bases de datos llegan a convertirse

22 Armagnague, *Ibíd,* p. 383.

en instrumentos que influyen en la regulación de los datos personales y en el flujo e intercambios de datos, lo cual ha repercutido tanto en los procesos como en las actividades a desempeñar.

PERSPECTIVA DE LOS ESTUDIOS DE LA INFORMACIÓN

Con base en lo anterior, las exigencias de acceso a la información han incrementado al igual que la demanda de transparencia como un servicio de la democracia, con todo lo que esto implica: el uso/mal uso de los datos a través de las redes de información. Turilli y Floridi,[23] desde una perspectiva de los estudios de la información, consideran la regulación como uno de los principios restrictivos de los flujos de información, a partir de conceptos como privacidad, anonimato, libertad de expresión, derecho de copia. Por otro lado, surge la necesidad de la información para la rendición de cuentas, la seguridad y el bienestar con un propósito meramente de control social. Esto quiere decir que la agenda de la política pública de los países tiene que atravesar por un cambio. Cambio que gira alrededor de la propiedad intelectual, la libertad de información y los flujos de información en general. Por supuesto, todos estos aspectos requieren de políticas de información diseñadas para atender cada una de las áreas para incrementar:

- La calidad de los servicios en general.
- El acceso a la información gubernamental.
- La productividad de las organizaciones.
- La generación de modelos de negocios.

23 M. Turilli y L. Floridi (2009), "The Ethics of Information", pp. 104- 112.

La tecnología, en la actualidad, permite una utilización descentralizada de la diseminación de los datos personales, ya que los paquetes de datos se pueden agrupar, combinar, empalmar o integrar para crear nueva información de utilidad, y trasladar estos paquetes a medios de almacenamiento actuales y a transmisiones diversas, lo que hace que la rendición de cuentas, el consentimiento y la transparencia cada vez se dificulten.[24]

Los datos personales, como lo indica la Directiva 95/46/CE, pueden ser utilizados para fines comerciales. Esto significa que los patrones de protección de datos van cambiando, ya que el individuo y las organizaciones con fines comerciales y gubernamentales buscan, desde sus respectivos escenarios, la protección de datos personales y, simultáneamente, la eficiencia de los servicios electrónicos que utilizan esos datos personales. Por otro lado, se encuentran el comercio y el gobierno que explota los datos personales. Ambos buscan legitimar y mantener la confianza de sus clientes a través de la protección de su privacidad. El comercio y el gobierno, además, pueden ser los promotores de las restricciones en la regulación del uso los datos. De acuerdo con Raab, algunos mecanismos para ellos son:

- El modelo de licencia: el estado concede licencias para el uso de los datos personales bajo condiciones preestablecidas.
- Modelo de registro: requiere que los usuarios de los datos registren sus particularidades en una agencia gubernamental con las características específicas.
- Modelo de comisionado: el comisionado y las agencias gubernamentales desarrollan un sistema político /administrativo en la sociedad.

24 Lyon, *Op. cit.*

- Modelo de control voluntario, que abarca la autorregulación por las organizaciones que utilizan banco de datos personales.
- Modelo de control o autoayuda: tiene un vínculo con la definición común de la privacidad, en el cual individuos controlan la información que se comunica de ellos. La atención de los resultados está puesta sobre la interacción entre el usuario de datos y el sujeto de datos, entre el sujeto de datos y el proveedor de tecnologías.[25]

Cada uno de los modelos presentado por Raab puede remitir a los principios de protección de datos, como lo señalan Van de Donk y Van Duivenboden,[26] quienes consideran que llegar a armonizar un mínimo común puede remover los obstáculos y crear un sendero hacia el desarrollo de las economías y de los mercados. Cada principio de protección de datos conduce a una práctica de protección de datos. Estas prácticas, cada vez más, se trasladan a las redes de relaciones tanto en el plano presencial como en el plano virtual, buscando principalmente una visibilidad mediada, antes a través de la televisión y en la actualidad a través de la webcam. Tanto un plano como el otro influyen en la vida cotidiana buscando la eficiencia, la conveniencia y la seguridad. Resalta otro elemento, la vigilancia, que paulatinamente se fue trasladando hacia los medios de la comunicación y de la información y fue recobrando fuerza a través de la infraestructura que facilitó la clasificación y el procesamiento de datos personales. La infraestructura permite realizar las transacciones a distancia. La firma, que era sello de autenticidad de la persona, poco a poco fue reemplazando

25 C. Raab (1997), "Co-producing Data protection", pp.14-16.

26 W. B. H. J. Van de Donk y H. Van Duivenboden, (1996), "Privacy as Policy: A Policy Implementation Perspective on Data Protection at Shopfloor Level in the Netherlands", pp. 513-534.

a los "*tokens* de seguridad". En la actualidad, además del pasaporte, conviven a los *tokens* de seguridad, de autentificación, de confianza. Por lo general, el individuo está más preocupado por cómo son utilizados sus datos, por lo que reclama la privacidad de éstos y, por ende, lo que le interesa es la vigilancia de los mismos, lo cual depende de la infraestructura que ordenan los datos de acuerdo a criterios, propósitos e intereses establecidos.

Uno de esos criterios es la clasificación social por parte del gobierno, los comercios, los servicios de seguridad informática, por lo que, en una sociedad de la información, hay una marcada tendencia hacia una sociedad de visibilidades mediada, dependiendo de las clasificaciones y categorizaciones que realizan, cruzando datos de diferentes redes informáticas establecidas con la ayuda de complejos sistemas de procesamientos de datos.

Las redes intercambian datos entre diferentes nodos, conformando un espacio de flujos, denominado sociedad Red. Lyon[27] señala que las secuencias de intercambio e interacción van formando flujos que vienen a conformar datos de vigilancia (*surveillance*), o comunicación de riesgo, y datos personales, y éstos, como cualquier otro flujo, circulan de acuerdo a lógicas asimétricas en las organizaciones. Es decir, en la sociedad de la información, las infraestructuras se convierten en ejes nodales de coordinación y de intercambio, u operaciones de *surveillance*. La vigilancia llega a ser parte de la gobernabilidad, ya que organiza las relaciones sociales y los patrones de ordenamiento. Actores como:

- Los medios, en específico la prensa, por su posición en la sociedad, crea opinión pública respecto a los acontecimientos sobre la temática.

27 Lyon, *Op. cit.*, pp. 242-257.

- La burocracia, que limita y previene la combinación de datos personales contenidos en archivos.
- El profesional que procesa los datos.
- La política, que restringe la combinación de diversos archivos personales.
- Los emprendedores del márketing, que buscan todas las oportunidades para infiltrarse en los sistemas para conocer los perfiles de los individuos.
- Los académicos, que realizan investigaciones sobre personas y personajes deben de regirse de acuerdo a las reglas para el uso de los archivos y de la información.[28]

Los contextos socioculturales es otro punto importante que se debería de tomar en consideración. Orito y Murata[29] presentan casos sobre el mal uso de los datos personales en Japón y sus consecuencias financieras en la sociedad y en el contexto filosófico Watashi (yo), Miuchi (familia), Uchi (adentro), liminal (zona/vecindario), Soto (afuera) de la sociedad japonesa. Mientras, en el mundo occidental Chalton[30] manifiesta que no es fácil adoptar una disposición como la Directiva 95/46/ CE, extrapolarla a una comunidad determinada que tiene una ley desde 1984 e implementar la visión de la Comunidad Europa. La adaptación de tal Directiva tomará su tiempo.

28 Saarenpaa, *Op. cit.*, pp. 51.

29 Yohko Orito y Kiyoshi Murata (2008), "Socio-cultural Analysis of Information Leakage in Japan", pp. 161-171

30 Simon Chalton, "The Transposition into the UK law of EU Directive 95/46/EC (the Data Protection Directive)", pp. 25-32.

A MANERA DE CONCLUSIÓN

Los datos personales, la privacidad y la vigilancia (*surveillance*) están influidos por la infraestructura tecnológica que, en la actualidad, realiza operaciones complicadas y extrae de varios nodos datos personales vertidos en sistemas de información diferentes para construir una cedula que identifique físicamente, de manera psicológica, biológica y emocional, a la persona que se encuentra detrás de ese número. Ese número atribuye un valor al individuo en la sociedad donde se encuentre registrado. Parte de los datos son cedidos por el propio individuo a sistemas diversos, como en la sociedad japonesa, que le va otorgando datos personales a círculos diversos, de acuerdo con el nivel de intimidad. El problema se centra en quién o quiénes tendrán la cedula que identifique a la persona, no por el número que se le otorga, sino a la persona real que se encuentra detrás de ese número, el propósito de tener esa cedula por qué y para qué lo va a utilizar. La tecnología, con sus avances en el procesamiento y extracción de datos, está dando la pauta y advirtiendo que cada vez más se está aproximando a una sociedad de riesgo que viene siendo parte de conjunción de la sociedad de la información y la sociedad Red. En este análisis sobre la sociedad de riesgo, uno de los puntos a resaltar es la vigilancia de los datos, o mejor dicho, saber en manos de quiénes van a parar los datos relacionados con la persona.

A nivel jurídico-legal la Directiva 95/46/CE brinda muchos lineamientos que pueden ser adaptados a los contextos socioculturales de cada país. Habrá que tomar en consideración los principios establecidos que son socializados en muchos países, no sólo como parte de sus leyes sino también la socialización de los derechos de personas como parte de una los derechos humanos y el derecho a la información.

En suma, la privacidad como política de información, además de tener tintes de vigilancia de los datos, debe generar confianza entre los ciudadanos y entre quienes tienen sistemas de información con sus datos personales que deberían estar protegidos indistintamente de si están en manos de los sujetos públicos o privados.

Referencias bibliográficas

Armagnague, Juan F. (2002), "El derecho comparado en la protección de datos", en María G Abalos y Olga P. Arrabal de Canals (coord.), *Derecho a la información,* habeas data *e Internet,* Buenos Aires, Ediciones La Rocca, pp. 375-415.

Blume, Peter (1997), "Introduction", en *International Review of Law Computers & Technology,* 11 (1), pp. 7-10.

Chalton, Simon, "The Transposition into the UK Law of EU Directive 95/46/EC (the Data protection Directive)", en *International Review of Law, Computers & Technology,* 11 (1), pp. 25-32.

Dumontier, Jos, "The Protection of Personal Data in the Schengen Convention", en *International Review of law, Computers & Technology*, 11 (1), pp. 94

Euro-Lex, *Access to European Union Law. Document 31995L0046. Directiva 95/46/CE* [en línea], http://eur-lex.europa.eu/legal-content/ES/ALL/?uri= CELEX:31995L0046

Flood, Stephen (1985), "The data protection register – content and access", en *ASLIB Information,* 13 (5), pp. 75-77.

IFLA (2013), *Reporte Ejecutivo. Síntesis de la Reunión de Expertos sobre el Informa de Tendencias de IFLA,* celebrada los días 4 y 5 de marzo de 2013 en la ciudad de México, en el marco de la Reunión Presidencial de IFLA.

IFLA (2013), *¿Surcando las olas o atrapados en la marea?: Navegando el entrono en evolución de la información. Percepciones del IFLA Trend Report*.

Haggerty, Kevin y Richard Ericson (2000), "The surveillance assemblage", en *British Journal of Sociology,* 51 (4), pp. 605-622.

Lyon, D. (2002), "Everyday Surveillance: Personal Data and Social Classifications", en *Information Communication & Society*, 5 (2), pp.242-257.

Orito, Yohko y Kiyoshi Murata (2008), "Socio-Cultural Analysis of Information Leakage in Japan", en *Journal Of Information Communication & Ethics in Society,* 6 (2), pp. 161-17.

Raab, Charles (1997), "Co-producing Data protection", en *International Review of Law Computers,* 11 (1), pp.14-16.

Raab y David Mason (2002), "Privacy, Surveillance, Trust And Regulation", en *Information, Communication & Society,* 5 (2), pp. 237-241.

Saarenpaa, Athi (1997), "Data Protection: in Pursuit of Information. Some Background to, and Implementations of Data Protection in Finland", en *International Review Of Law, Computers & Technology,* 11 (1), pp. 47-64.

Turilli, M. y L. Floridi (2009), "The Ethics of Information", en *Ethics and information technology*, 11 (2), pp.104- 112.

Van de Donk, W. B. H. J. y H. Van Duivenboden (1996), "Privacy as Policy: a Policy Implementation Perspective on Data Protection at Shopfloor Level in the Netherlands", en *International Review of Administrative Sciences*, 62 (4) pp. 513-534.