

La protección de datos personales en América Latina: entre la Unión Europea y los Estados Unidos de Norteamérica

Seminario Internacional de Protección de Datos Personales 2018
en conmemoración del
Día Internacional de Protección de Datos Personales del INFODF



1



El sistema iberoamericano de protección de datos en los albores del Siglo XXI



LA PROTECCION DE DATOS EN LAS CONSTITUCIONES DE LOS ESTADOS



- No existía reconocimiento expreso del derecho a la protección de datos personales (Uruguay 1967).
- La mayoría de los países poseía mecanismos constitucionales de defensa del derecho a la privacidad (Colombia 1991, 2003).
- Algunas constituciones proveían de medios para hacer valer el derecho a la protección de datos personales, como por ejemplo el hábeas data (Brasil 1988, Paraguay 1992, Argentina 1994).



LA PROTECCIÓN DE DATOS PERSONALES Y LA LEY



- No existían leyes que consagraran el derecho con carácter general, con la excepción de los casos de Chile (Ley No. 19.628 de 1999), Argentina (Ley No. 25326 de 2000).
- Se consideraba la protección de datos como un derecho inherente a la condición humana o derivado de la forma republicana de gobierno.
- En ese entendido, el derecho humano a la protección del dato debe ser tutelado y punible por el ordenamiento jurídico (Chile 1999, Peru 2001).



LA PROTECCION DE DATOS EN LOS INSTRUMENTOS INTERNACIONALES



- Instrumentos de cooperación para la protección de los datos en sus instancias de procesamiento tales como:
 - Convención Internacional de Derechos Civiles y Políticos – 1966, 1967
 - La Declaración Universal de los Derechos del Hombre – 1948
 - Convenio 108– 1981
 - Directiva 95/46/EC- 1995
 - Directiva 2002/58/EC – 2002



LEYES QUE REFIEREN A PROTECCION DE LOS DATOS PARA ACTIVIDADES SECTORIALES



- Algunos países tenían leyes que atendían la situación de determinados tipos de datos, tales como:
 - Datos en salud
 - Datos genéticos
 - Datos estadísticos
 - Datos de menores
 - Datos crediticios
 - Secreto profesional



EL CASO URUGUAY AÑO 2000



- La Constitución de la República carecía de regulación específica en protección de datos personales.
- Los artículos 72 y 332 de la Constitución declaran que la lista de derechos que aparece en la Constitución no excluye otros derechos que son inherentes a la condición humana o que derivan de la forma republicana de gobierno, y que sus normas pueden ser aplicadas aún en el caso en que no exista regulación específica teniendo en consideración las normas análogas, los principios generales del derecho, los principios de justicia y las doctrinas más recibidas. Sistema de numerus apertus.
- Disposiciones sectoriales que regulan datos médicos, datos estadísticos.



2



Hacia el sistema europeo en protección de datos personales



2003 – Primer hito



XIII CUMBRE IBEROAMERICANA DE JEFES DE ESTADO Y GOBIERNO SANTA CRUZ DE LA SIERRA NOV.2003

“45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad”.



2003 - Segundo Hito



DECLARACIÓN DE LA ANTIGUA GUATEMALA – II EIPD 2003

“1º Valoran el creciente interés, preocupación y compromiso que en el ámbito de los Países Iberoamericanos se ha puesto de manifiesto con la protección de datos personales.

2º Reiteran la consideración de **la protección de datos personales como un auténtico derecho fundamental** de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos.

5º Constatan la necesidad de *impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos*, así como la idoneidad de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes, en el respeto a los derechos fundamentales y en los intereses de sus respectivos países, garanticen una protección adecuada en todos los Países Iberoamericanos. Tales marcos normativos deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los instrumentos nacionales. En este sentido, consideran muy positivas las iniciativas regulatorias que se han puesto en marcha en diversos Países Iberoamericanos.

6º Resaltan la importancia de *potenciar las iniciativas de intercambio de experiencias* entre los Países Iberoamericanos, estableciendo canales permanentes de diálogo y colaboración en materia de protección de datos.

7º Con este fin, y al objeto de reforzar la mutua y continua colaboración entre ellos, avanzando en base al Foro Permanente creado con ocasión del Primer Encuentro, se constituyen en la **Red Iberoamericana de Protección de Datos**, abierta a la incorporación de representantes de todos los Países Iberoamericanos.



2004 – Tercer hito



DECLARACIÓN DE CARTAGENA DE INDIAS III EIPD 2004



La Declaración de Cartagena de Indias (2004):

- Considerando el importante rol informativo de la Red Iberoamericana de Protección de Datos, útil para entender cómo opera la protección de datos en cada país
- Deciden que la Red asumirá una actitud más proactiva, en procura de logros más concretos.

- **INTERCAMBIO DE INFORMACION:** Así se trate de leyes, sentencias, eventos de adecuada credibilidad, información relevante, la idea es promover el intercambio.
- **CONSEJO PERMANENTE:** asistencia recíproca con relación a leyes o cuestiones de carácter práctico.
- **COOPERACION** en la creación de documentos y propuestas en común (como es el caso de los documentos sobre acceso, sobre dpas, sobre telecomunicaciones, gobierno electrónico o estrategia de la Red, directrices).



3



Sistema actual de protección de datos personales en América Latina



PAISES DE AMERICA LATINA

➤ PAISES CON LEYES GENERALES DE PROTECCION DE DATOS

Argentina – 2000

Uruguay - 2008

México – 2010

Perú – 2011

Costa Rica -2011

Nicaragua – 2012

Colombia – 2012

República Dominicana-2013

➤ PAISES CON PROYECTOS DE LEY SOBRE PROTECCION DE DATOS A ESTUDIO EN EL PARLAMENTO

Brasil

Chile



Sólo
ARGENTINA (2003)
y **URUGUAY** (2012)
fueron
declarados

países con un adecuado nivel de
protección de datos según la
Directiva 95/46
del Parlamento Europeo y del
Consejo



URUGUAY

RATIFICO ASIMISMO LA CONVENCION
108
DEL CONSEJO DE EUROPA
Y SU PROTOCOLO ADICIONAL

- 1.- por Ley 19030 de enero de 2013
Uruguay ratifica el C108,
en efecto desde el 1 de Agosto de 2013.
- 2.- 45º país en ser parte del C108
- 3.- primer país no europeo



4



Novedades 2017



ARGENTINA

- Por Decreto de Necesidad y Urgencia N° 746/2017 se incorporó como función del Jefe de Gabinete de Ministros la de garantizar el efectivo ejercicio del derecho de acceso a la información pública y controlar la aplicación de la Ley de Protección de Datos Personales.
- Por Decreto N° 899/2017 se declara que la Agencia de Acceso a la Información Pública tiene por función fiscalizar la protección integral de los datos personales para garantizar el derecho al honor y a la privacidad de las personas, convirtiéndose en la nueva autoridad de aplicación de la Ley.
- Por Decreto 685/2017 el ex Director de la DPA argentina pasó a ser el Director de la Agencia de Acceso a la Información pública, por 5 años, con rango y jerarquía de secretario.



PERÚ

- El Decreto Legislativo N° 1353 de 2017 en su artículo 1º manifiesta que tiene por finalidad:
 - Crear la Autoridad de Transparencia y Acceso a la Información Pública
 - Fortalecer el régimen de protección de datos personales
 - Regular la gestión de los intereses entre ambos
- El Decreto Supremo N° 019-2017-JUS de 2017 reglamenta el Decreto Legislativo y en su artículo 2º establece:
 - La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, es el órgano de línea encargado de ejercer la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y depende jerárquicamente del Despacho Viceministerial de Justicia



5



URUGUAY



NORMATIVA:

- 2008 – Ley 18331
- 2012 – Declaración de Adecuación
- 2013 – Ley 19030 Ratificación del C108



URUGUAY

Ley 18331, 2008



- 1.- protección de datos personales como un derecho fundamental
- 2.- principios
- 3.- obligaciones
- 4.- derechos de los ciudadanos y residentes
- 5.- Agencia de Protección de Datos autónoma e independiente



07.04.2014

DECRETO 92/2014
NOMBRES DE
DOMINIO EN LOS
ORGANISMOS DE LA
ADMINISTRACIÓN
CENTRAL

- Regula la seguridad de la información en el sector público, con relación al uso de los nombres de dominio.
- Su OBJETIVO es estandarizar los nombres de dominio para garantizar la transparencia y la seguridad.
- Obliga al uso de nombres de dominio "gub.uy" o "mil.uy".
- Prohíbe el uso de cualquier otro nombre de dominio.
- Los sistemas informáticos deberán estar alojados en centros de datos seguros situados en Uruguay
- Otorga un plazo de 90 días para presentar a AGESIC un Plan de Acción.



27.12.2010

28.09.2009

Ley 18719 artículo 149

Decreto 451/2009

**INCIDENTES DE
SEGURIDAD**

- Siguiendo la estrategia del ex Presidente José Mujica, se creó un centro para atender incidentes de seguridad informática.
- Su OBJETIVO es estandarizar acciones a seguir en caso de incidentes de seguridad.
- CERTuy, dependiente de AGESIC, es el encargado de registrar, clasificar, realizar diagnósticos, actuar e informar.
- 2014: el primer resultado fue informado en la página web de AGESIC.



27.12.2013

Ley 19179

SOFTWARE ABIERTO, ESTÁNDAR Y LIBRE

- En los organismos del Estado se preferirá licenciamientos de software libre.
- Se considera de interés general que el sistema educativo promueva el uso de software libre.
- En caso de que el Estado contrate o desarrolle software, el mismo al ser distribuido, se licenciará como software libre.
- La reglamentación de las condiciones, tiempos y formas en que se efectuará la transición se hará en 180 días.



27.02.2014

Resolución 64/2013

de la URCDP

POLÍTICA DE PRIVACIDAD DE PROTECCIÓN DE DATOS

- Establece que todas las páginas web que procesen datos en Uruguay deben publicar sus Políticas de Privacidad, y que las mismas deben adecuarse a la Ley 18.331.



14.03.2013

Resolución No. 13/2013

**ACLARATORIA CON
RESPECTO A
ATRIBUCIONES DE LA
URCDP**

- Declara que la URCDP actúa dentro de su competencia cuando exige que la presentación de la información requerida a entidades públicas o privadas se cumpla en forma completa.



27.02.2014

**Resolución 1040/2013
de la URCDP**

**ATRIBUCIONES DE LA
URCDP SOBRE
MOTORES DE
BÚSQUEDA DE
INTERNET**

- Recomienda que, previamente a la publicación de datos en páginas web públicas, deben resolverse los problemas concernientes a la privacidad de los datos.
- Para honrar el derecho al olvido, en algunos casos ciertos datos no deberían ser incluidos, y en otros los datos pueden ser eliminados posteriormente.
- El objetivo del Decreto es prevenir que los datos eliminados permanezcan en el índice de motores de búsqueda como Google, Bing, Yahoo.



URUGUAY



Estamos conscientes y preocupados por:

- La expansión de la vigilancia
- La colaboración entre el gobierno y los vendedores de tecnologías de vigilancia
- Las decisiones tomadas analizando el comportamiento
- Datos abiertos en datos personales de salud
- Protección de datos en organismos públicos
- Amenazas a la privacidad de las comunicaciones
- Falta de control social
- Amenazas a la libertad de expresión
- Amenazas al acceso a la información
- Amenazas que inducen a la discriminación



6



Generalidades



AMERICA LATINA

- La protección de datos personales ha cambiado su panorama en los últimos 20 años.
- Europa aparece con un importante grado de integración, como líder en América Latina, actuando proactivamente.
- América Latina debe asumir la necesidad de integración y de trabajar en este desafío.
- EE.UU. intenta ejercer influencia en América Central y América Latina. Aspectos como el consentimiento y las transferencias internacionales marcan una gran diferencia.



7



Principales dificultades



PRIMERA DIFICULTAD

- Las Agencias de Protección de Datos deben trabajar para ser más autónomas e independientes.
- Esto ayudará a las Agencias de Protección de Datos a tener más recursos económicos y humanos.
- Sólo la autonomía otorgará a las Agencias de Protección de Datos la autoridad para hacer cumplir el régimen de protección de datos.
- Sólo la autonomía otorgará a las Agencias de Protección de Datos los medios para organizar nuevas formas de cooperación.



SEGUNDA DIFICULTAD

- El sistema de protección de datos es diferente en EE.UU. y en la Unión Europea.
- Ambos regímenes tiene una importante influencia en América Latina.



8



Desafíos



PARA LAS EMPRESAS

- Asumir un rol proactivo.
- Clarificar el uso que hacen las empresas de los datos personales.
- Cumplir con la normativa.
- Ir más allá del estricto cumplimiento.
- Crear una reputación.
- Generar confianza en su producto, su servicio y su marca.
- Sacar una ventaja sobre los competidores.
- Obtener recomendaciones de los asesores locales y globales.



PARA AMÉRICA LATINA

- Trabajar en nuevas formas de integración.
- Siempre estar conscientes de las dimensiones legales de la seguridad de la información y lo que esto implica en términos de la protección de datos.



PARA LOS PAISES

- Ofrecer un claro marco normativo.
- Dar a las Agencias de Protección de Datos los medios para trabajar autónomamente y con independencia, para tener verdadera autoridad para hacer cumplir la normativa.
- Educar y concientizar a los individuos.



¿Qué necesita el sistema Latinoamericano de Protección de Datos?



Educación
Concientización
Imponer multas
Juicios civiles y penales
Cooperación
Integración y armonización



Muchas gracias!



ana.brian@estudiojuridicobriann.com.uy

