

# BIG DATA

## Los principios para la protección de datos personales

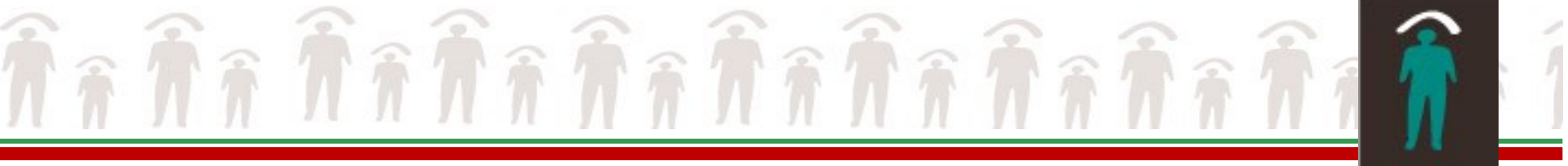
Seminario “Los nuevos retos de la privacidad.  
El tratamiento masivo de los datos personales”

Agencia Española de Protección de Datos.  
Red Iberoamericana de Protección de Datos.

Centro de Formación de AECID, Montevideo. - Noviembre 3, 2015. - Dra. Ana Brian Nougrères

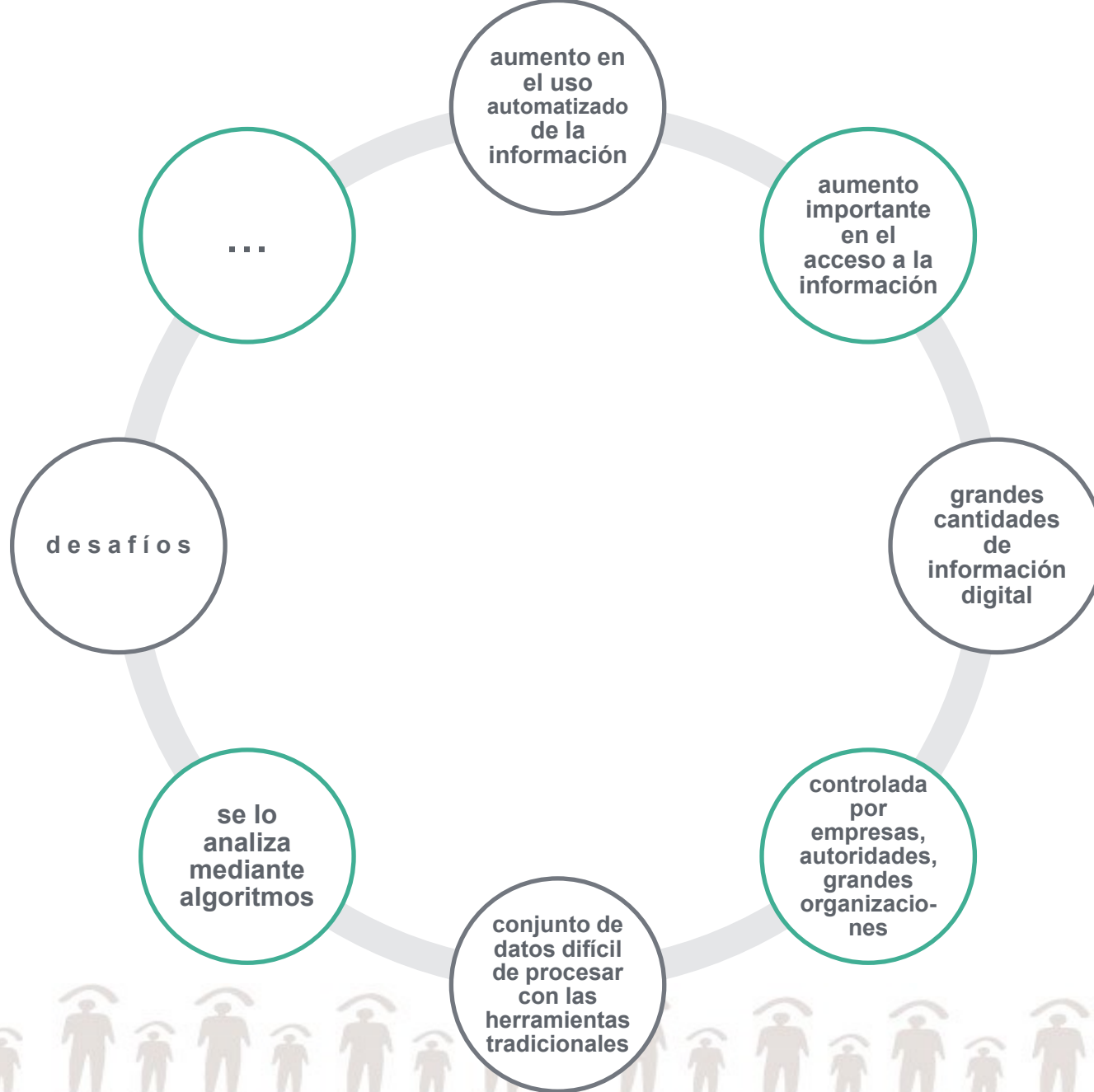


# 1



# ¿QUE ES BIG DATA?





# BIG DATA

La cantidad de datos crece a razón de un 50 % anual.

El 90 % de los datos que circulan en el mundo se generaron en el decurso de los últimos dos años.

(<http://www-01.ibm.com/software/data/bigdata>)

El Internet de las Cosas agrega nuevos elementos: se estima que para el año 2020 habrá 26.000 millones de sensores cargando a la nube información de cómo los humanos interactúan con las cosas.

(<http://www.gartner.com/newsroom/id/2636073>)

Conlleva un desafío a los principios de la protección de datos personales, que constituyen nuestra garantía de que nuestra privacidad, así como la libertad de expresión y las condiciones para el intercambio de ideas.



Los datos se transformaron en materia prima para la producción

datos como fuente de valor social y económico.

avances en minería de datos

capacidad de almacenamiento expandida

aumento en la información disponible para los negocios y gobierno

posibilidades de analizar los datos

- sin necesidad de bases de datos estructuradas y
- con independencia de las habilidades investigadores

el aumento en la cantidad de personas, dispositivos y sensores interconectados digitalmente ha revolucionado la manera de generar, compartir y acceder al dato

los datos generan valor al mundo de la economía, promueven la innovación, la productividad, la eficiencia y el crecimiento

PERO también genera problemas cuando encaramos privacidad y protección de datos, por lo cual se propende a un sistema que atienda también al individuo, a cuyos efectos se sugiere:

Proveer a los individuos de acceso a los datos

Dotar de información transparente acerca de los mecanismos del procesamiento.

# 2



# ACERCA DE BIG DATA







a favor

- Utilización del BIG DATA en forma beneficiosa para la sociedad.
- Para la Identificación y predicción de tendencias y sus correlaciones
- Por ejemplo:
  - Predicción de epidemias o de efectos de medicamentos
  - Combate de la polución en ciudades grandes

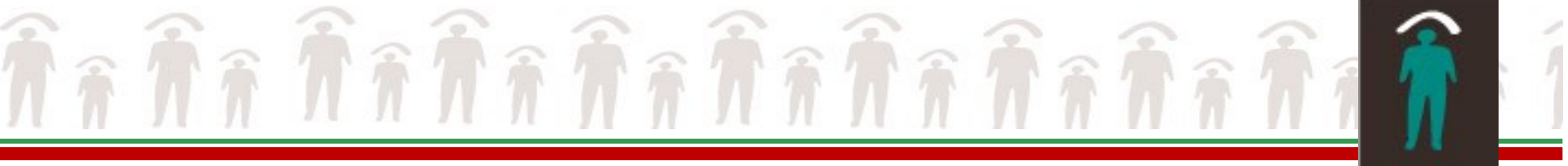


en contra

- Utilización del BIG DATA de forma que puede afectar a los individuos.
- Por ejemplo:
  - Para preparar perfiles
  - Para predecir comportamientos



# 3



# CADENA DE VALORES DEL BIG DATA





\* Hardware, Software and Operating System vendors

# 4



# DESAFIOS DEL BIG DATA PARA LA PROTECCION DE DATOS PERSONALES



# BIG DATA: PRINCIPIO DEL CONSENTIMIENTO Y PRINCIPIO DE FINALIDAD

- BIG DATA vs. uso del dato para una nueva finalidad.
- Coloca bajo presión el principio de finalidad.
- Este principio se entiende que es respetado cuando el análisis predictivo del dato se asegura que es compatible con la finalidad original, cumpliendo así con una expectativa razonable del titular del dato, que surge de un análisis caso por caso.
- Consentimiento para múltiples finalidades.
- Consentimiento como una forma de control del uso del dato por parte de su titular.
- Requisitos: libre, específico e informado.



# BIG DATA:

## PRINCIPIO DE PROPORCIONALIDAD

- La naturaleza del BIG DATA es la antítesis de los principios de relevancia y minimización, lo que se justifica en que el uso del BIG DATA está orientado hacia posibles futuros usos.
- Violenta el principio de proporcionalidad y relevancia conforme la finalidad en la colecta, y pueden mostrar una tendencia a no borrar datos.
- Una forma de cumplir con este principio es que las DPAS controlen la obligación de borrar los datos.





# BIG DATA:

## DERECHO DE ACCESO Y TRANSPARENCIA

- El derecho del titular del dato a acceder a la información sobre cómo es tratado su dato personal (manipulación, finalidad, eventual distribución) constituye uno de los más importantes principios en protección de datos personales.
  - Es muy difícil, para un usuario promedio de internet, su ejercicio en casos de marketing on line. Además se trata de herramientas que permiten identificar patrones de individualización de datos sensibles.
- Se trata de un riesgo que debe prevenirse.



# BIG DATA:

## TRATAMIENTO DE LOS DATOS SENSIBLES

- Puede suceder que se colecten datos que no son sensibles por sí mismos pero que, en un conjunto con otros datos, pueden proveer como resultado un dato sensible, sea relativo a salud, orientación sexual u otro.
- En tanto se trata de información que goza de un estatuto preferencial de protección, las autoridades de control deben estar atentas al riesgo que existe cuando se compilan y analizan datos con esas características.



# BIG DATA:

## ANONIMIZACION Y DESANONIMIZACION

- Uno de los mayores riesgos consecuencia del BIG DATA es que se desanonimicen aquellos datos que fueron anonimizados, dejando visibles medios de identificación de los titulares de los datos.
- El riesgo puede verse reducido controlando los métodos de anonimización, aunque la robustez del sistema no siempre es fácil de controlar, por dos razones:
  - Los individuos pueden ser identificados de diversas formas, sea por un dato o por información indirecta, o por información cruzada.
  - Es muy difícil para las empresas que hacen el proceso de anonimización tener conocimiento de todos los datos que son hábiles para re identificar a los titulares del dato.



# BIG DATA:

## LAS IMPLICANCIAS DE SEGURIDAD

- Los desafíos para la seguridad que trae consigo el BIG DATA tienen relación con la privacidad.
- Por ejemplo: el uso de más capas de infraestructura para procesar BIG DATA conlleva mayores riesgos, de igual manera que una nueva infraestructura para manipular el flujo de datos. El riesgo es mayor cuanto más grandes son los flujos de datos almacenados.
- Las empresas deben ser responsables por los datos que almacenan.



# BIG DATA:

## PRINCIPIO DE VERACIDAD

- Es importante que los datos en que se basan las decisiones sean veraces, en especial teniendo en cuenta el uso en gran escala de las tecnologías de minería de datos por compañías de seguros o de rating de créditos, que utilizan como fuente de información los datos en línea.
- Existe una tendencia a considerar que el contexto de la información debe ser tenido en cuenta (Danah Boyd y Kate Crawford “Critical Questions for Big Data”).
- La transparencia pasa a ser un principio clave, presupuesto para que el titular del dato pueda salvaguardar sus derechos sea mediante el derecho de acceso, de corrección o de exclusión.



# BIG DATA:

## LAS ASIMETRIAS DEL PODER

- La asimetría refiere al poder de los titulares del datos versus el poder de las corporaciones, en tanto son estas las que colectan la información sobre los individuos, que no necesariamente son quienes les proveen del dato.
- Esto implica una desventaja para el titular del dato, que carece de posibilidades de influir en el mecanismo de colecta y procesamiento de sus datos, lo cual lo hace especialmente vulnerable ante posibilidades de empleo, préstamos bancarios, opciones de seguros de salud.
- La OECD realizó un reporte en tal sentido, analizando el valor del dato personal y las metodologías para su estimación.



# BIG DATA: EL DETERMINISMO DEL DATO Y LA DISCRIMINACION

- En la era del BIG DATA la tendencia es a pensar que cuánto mayor sea la cantidad de datos colectados y con fácil acceso, las decisiones tienen a ser más razonadas y precisas.
- En esa línea de razonamiento se puede llegar a conclusiones falsas, consolidando prejuicios y estereotipando y reforzando la exclusión social y la estratificación.
- De ahí que la discriminación pasa a ser un problema de privacidad, en una sociedad en que cada vez más decisiones se toman teniendo por base análisis estadísticos que pueden resultar en la llamada “Dictadura del Dato” (Mayer.-Schonberger et al “Big Data. A revolution that will transform how we live”).



# BIG DATA: REPERCUSIONES

- De nuestra actitud depende que las decisiones sobre reportes crediticios o premios de seguros se fundamenten en información contextual que dejamos en internet (o en otros medios). De nuestro comportamiento dependerá que nuestros hijos vean denegada su cobertura de salud como consecuencia de nuestras declaraciones en redes sociales sobre desórdenes genéticos, por ejemplo. La discriminación puede ser para un trabajo, para un seguro de salud, para un préstamo.
- En cuanto al uso de BIG DATA por las autoridades sin una adecuada atención de la privacidad, debilita la democracia. Caso encuesta DPA Noruega 2014.





Muchas gracias!

