Laurant

Law Firm / Abogados

La protección de los datos personales en redes sociales y respecto al uso de la minería de datos y datos de gran tamaño ('big data') en Internet: retos y recomendaciones para los sujetos obligados en México

Cédric Laurant

Laurant Law Firm/Abogados

ICHITAIP: Conferencia en celebración del Día Internacional de Protección de Datos Personales 2018

(Chihuahua, Estado de Chihuahua, México, 30 enero 2018)

Laurant

Law Firm / Abogados

La protección de datos personales en redes sociales y respecto al uso de la minería de datos en Internet: retos para los sujetos obligados en México y recomendaciones

- Introducción.
- 1. La protección de los datos personales en redes sociales:
  - 1.1. Retos para los sujetos obligados.
  - 1.2. Recomendaciones a los sujetos obligados.
- 2. El uso de los 'big data' en Internet:
  - 2.1. Retos para los sujetos obligados.
  - 2.2. Recomendaciones para los sujetos obligados.
- Conclusión.

La protección de datos personales en redes sociales y respecto al uso de la minería de datos en Internet: retos para los sujetos obligados en México y recomendaciones

- Introducción.
- **1. La protección de los datos personales en redes sociales:**
  - 1.1. Retos para los sujetos obligados.
  - 1.2. Recomendaciones a los sujetos obligados.
- 2. El uso de los 'big data' en Internet:
  - 2.1. Retos para los sujetos obligados.
  - 2.2. Recomendaciones para los sujetos obligados.
- Conclusión.

1. La protección de los datos personales en redes sociales

- Objetivo: considerar los beneficios y riesgos por la privacidad generados por el uso de redes sociales en sitios de entidades gubernamentales y del sector público en general.

1.1. Retos para los sujetos obligados

- Reto principal: promover la transparencia de la información disponible al ciudadano mientras su privacidad es protegida efectivamente.
- Las redes sociales ofrecen un medio por el cual la entidad pública puede acercarse de otras maneras a sus administrados.
- Las redes sociales también permiten a esos administrados involucrarse más directamente y fácilmente en las actividades y consultas de las entidades públicas.
- Existe una **desconexión** entre la percepción que tiene el usuario de redes sociales de la protección de su privacidad en ese ámbito y la protección actual de su privacidad.

1.1. Retos para los sujetos obligados

- Mientras el uso de redes sociales por entidades pública tiene por propósito transparentar sus actividades con el público, no es claro qué información se recopila, cómo se usa y cómo limitar su diseminación, no sólo por parte de los proveedores de redes sociales, sino por parte de la propia entidad.

- La actividad de recopilación de datos de navegación e interacciones, entre el administrado usando redes sociales y el sitio de gobierno usándolas, es regulada por la LGPDPPSO federal y las leyes estatales correspondientes. El reto es saber cómo aplicar esas leyes de manera efectiva.

1.1. Retos para los sujetos obligados

- Las redes sociales deben fomentar la participación democrática, no ser usadas para monitorear al ciudadano: el usuario de redes sociales no puede ser obligado a revelar información sobre él a la entidad gubernamental por usar la red social que usa la entidad gubernamental en su sitio.

1.2. Recomendaciones a los sujetos obligados

- Recomendaciones generales:
  - Es necesario que el uso de las redes sociales en sitios de entidades públicas se haga de manera diferente de cómo se implementa en la mayoría de sitios web de particulares.
  - De manera general: debe ser prohibido que entidades gubernamentales puedan rastrear y monitorear las actividades de sus usuarios en sus sitios sitios web.

1.2. Recomendaciones a los sujetos obligados

- Recomendaciones generales:
  - Debe ser prohibido que entidades de gobierno comercialicen la información sobre esas interacciones.
  - Entidades de gobierno tienen que impedir el uso y comercialización de esa información de navegación por empresas de redes sociales: el ciudadano no debería someterse al monitoreo de terceros (las empresas de redes sociales) sólo porque quiere acceder a servicios públicos y a información que proveen entidades gubernamentales sobre sus actividades.

1.2. Recomendaciones a los sujetos obligados

- Recomendaciones generales:
  - Los sitios de entidades gubernamentales deben incluir en sus avisos de privacidad, las reglas aplicables a su uso de redes sociales y explicar al visitante cómo protege su navegación y actividades en el sitio de cualquier forma de vigilancia, que sea por la propia entidad y por la red social que se usa. También tiene que informar sobre los datos que recopila, porque los recopila (finalidades) y cómo los va a utilizar.
  - El uso de redes sociales debería ser limitado a proveer información y dirigir a los visitantes a los sitios oficiales donde podrán acceder a la información sobre la entidad gubernamental.

1.2. Recomendaciones a los sujetos obligados

- Recomendaciones generales:
  - La información que provee entidades tiene que estar disponible en su sitio web y no sólo vía las redes sociales que utiliza.
  - Las entidades gubernamentales deberán establecer acuerdos con redes sociales sobre cómo implementar estas recomendaciones.

1.2. Recomendaciones a los sujetos obligados

- Unas recomendaciones específicas:
  - Encuestas promovidas vía redes sociales deben explicar sus finalidades y limitar la información que obtiene de los encuestados a esas finalidades.
  - Si la entidad gubernamental utiliza una red social para informar al público de consultas públicas, no puede usar redes sociales para recibir respuestas a la consulta sino sólo dirigir al visitante al sitio oficial donde se recibirán sus comentarios.
  - Si una entidad gubernamental implementa herramientas de analíticos en su sitio web, no puede rastrear y monitorear a sus usuarios de manera individualizada; no puede por ejemplo usar los cookies cuya función lo permite.

La protección de datos personales en redes sociales y respecto al uso de la minería de datos en Internet: retos para los sujetos obligados en México y recomendaciones

- Introducción.
- 1. La protección de los datos personales en redes sociales:
  - 1.1. Retos para los sujetos obligados.
  - 1.2. Recomendaciones a los sujetos obligados.
- **2. El uso de los 'big data' en Internet:**
  - 2.1. Retos para los sujetos obligados.
  - 2.2. Recomendaciones para los sujetos obligados.
- Conclusión.

2. El uso de los ‘big data’ en Internet

- **2.1. Retos para los sujetos obligados.**
- 2.2. Recomendaciones para los sujetos obligados.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los ‘big data’ (‘grandes datos’).
  - Concepto:
    - Selección de Alemania en el Mundial de Futbol de Brasil 2014: según algunos hubiera ganado por su uso de minería de datos.
    - Tendencia tecnológica en la ciencia, la industria, los negocios o la gestión pública; afecta a la mayor parte de los aspectos de la actividad humana; se combina con otras tecnologías como el cómputo en la nube, el Internet de las cosas y la analítica predictiva.

2.1. Retos para los sujetos obligados

Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Concepto:
    - Se basa en el enorme incremento en la generación de datos en el mundo y permite aplicar nuevas formas de gestión específicas y especializadas (captura de datos, almacenamiento, búsqueda, compartición, análisis, etc.) y generar valor a partir de su análisis. Incremento en volumen, velocidad y variedad de los datos. Cfr Web 2.0, redes sociales, conexión de dispositivos y sensores a la Red (IoT), teléfonos móviles generando su ubicación vía GPS.

2.1. Retos para los sujetos obligados

Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Ejemplos de aplicaciones de la minería de datos:

    En el sector público:
    - Entender los comportamientos y preferencias de los administrados para ofrecerles servicios y productos personalizados o más enfocados a sus necesidades.
    - Mejoras en los servicios públicos (gestión del tráfico, servicios sanitarios, etc.).
    - Mejoras de la seguridad y el cumplimiento de la Ley (prevención de ciberataques, identificación preventiva de transacciones fraudulentas).

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Ejemplos de aplicaciones de la minería de datos:

    En otros sectores:
    - Entender y optimizar los procesos de negocio internos de las organizaciones.
    - Aplicaciones personales (dispositivos wearable).
    - Mejoras en la ciencia y la investigación.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - 2 definiciones de "big data":
    - "Serie de recursos de información de gran volumen, velocidad de generación/actualización y variedad, que requieren métodos y formas innovadoras y rentables de procesado para un conocimiento y toma de decisiones mejoradas." (Gartner)
    - "Big data se establece en el límite de la habilidad de una organización para almacenar, procesar y acceder a todos los datos que necesita para operar eficazmente, tomar decisiones, reducir riesgos y ofrecer servicios a sus clientes o usuarios." (Forrester)

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Características esenciales:
    - Procesamiento de grandes **V**olumenes de datos, estructurados y no estructurados;
    - generados a gran **V**elocidad; y
    - de una gran **V**ariedad;
    - para extraer **V**alor de esos datos; y
    - asegurar una elevada **V**eracidad entre la información obtenida y los datos originales.

2.1. Retos para los sujetos obligados

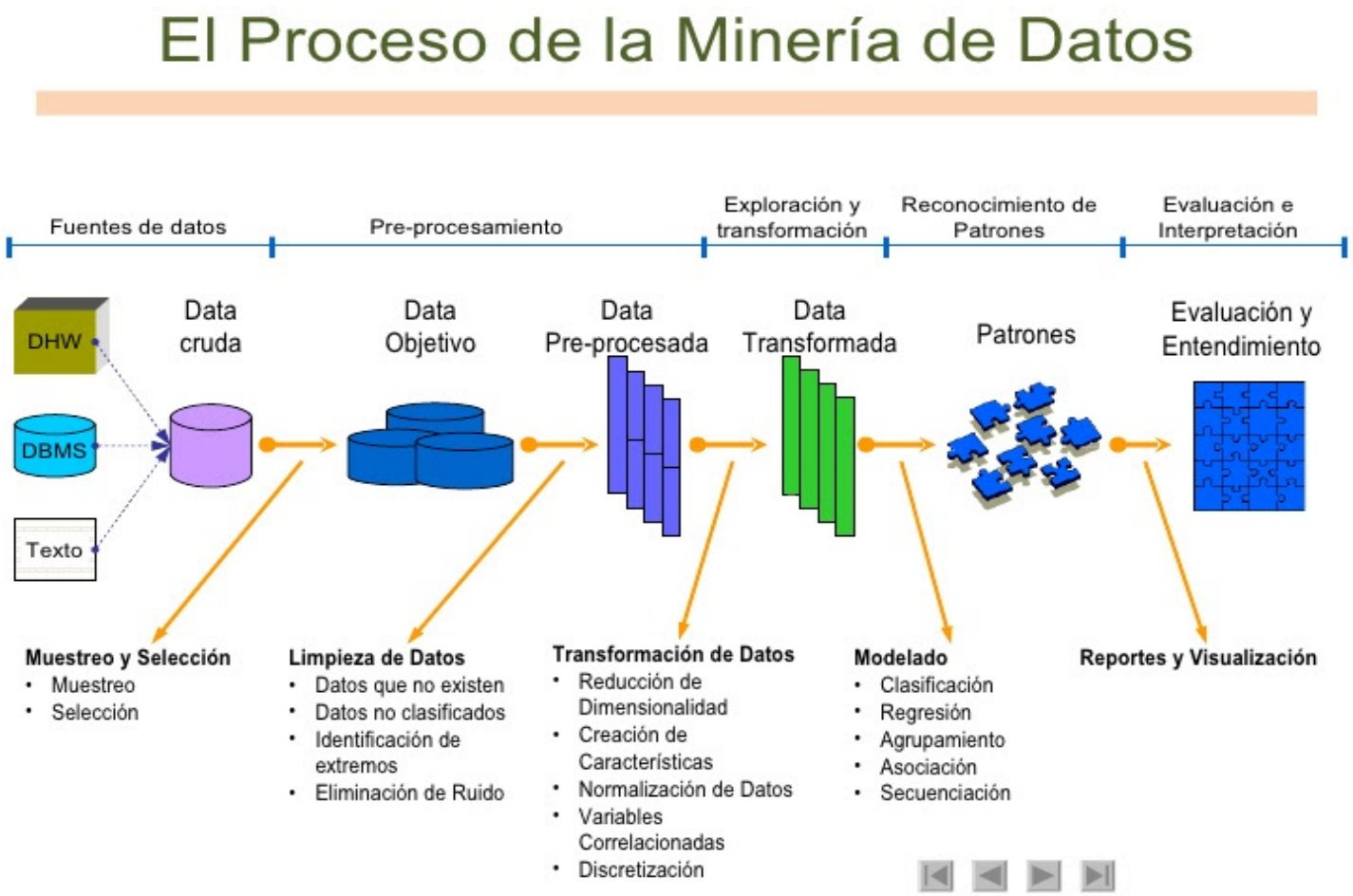
- Retos derivados del uso de los 'big data' ('grandes datos').
  - 2 definiciones de "minería de datos":
    - Conocida como exploración de datos, se define como el analista de (a menudo grandes) datos que se establece para encontrar relaciones insospechadas, intentando descubrir patrones para resumir los grandes volúmenes de éstos en formas novedosas que sean comprensibles y útiles para el titular de los datos.

2.1. Retos para los sujetos obligados

2.1. Retos para los sujetos obligados

Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados



2.1. Retos para los sujetos obligados

- Diferencias entre “big data” y “minería de datos”:
  - “Los ‘grandes datos’ (‘big data’) hacen referencia a grandes cantidades de datos que superan la capacidad de procesamiento habitual del software informático existente. Por lo que Big Data es la tecnología capaz de capturar, gestionar y procesar en un tiempo razonable y de forma veraz estos datos, a través de herramientas (software) que identifiquen patrones comunes como definir características específicas de los consumidores, generar parámetros, métricas o procesos específicos que cambian por completo la forma de hacer negocios, encontrando nuevos nichos, aumentando la rentabilidad y productividad de las compañías.”

2.1. Retos para los sujetos obligados

GRANDES DATOS

(BIG DATA)

PANORAMA GENERAL

MUCHAS RELACIONES

MINERÍA DE DATOS

(DATA MINING)

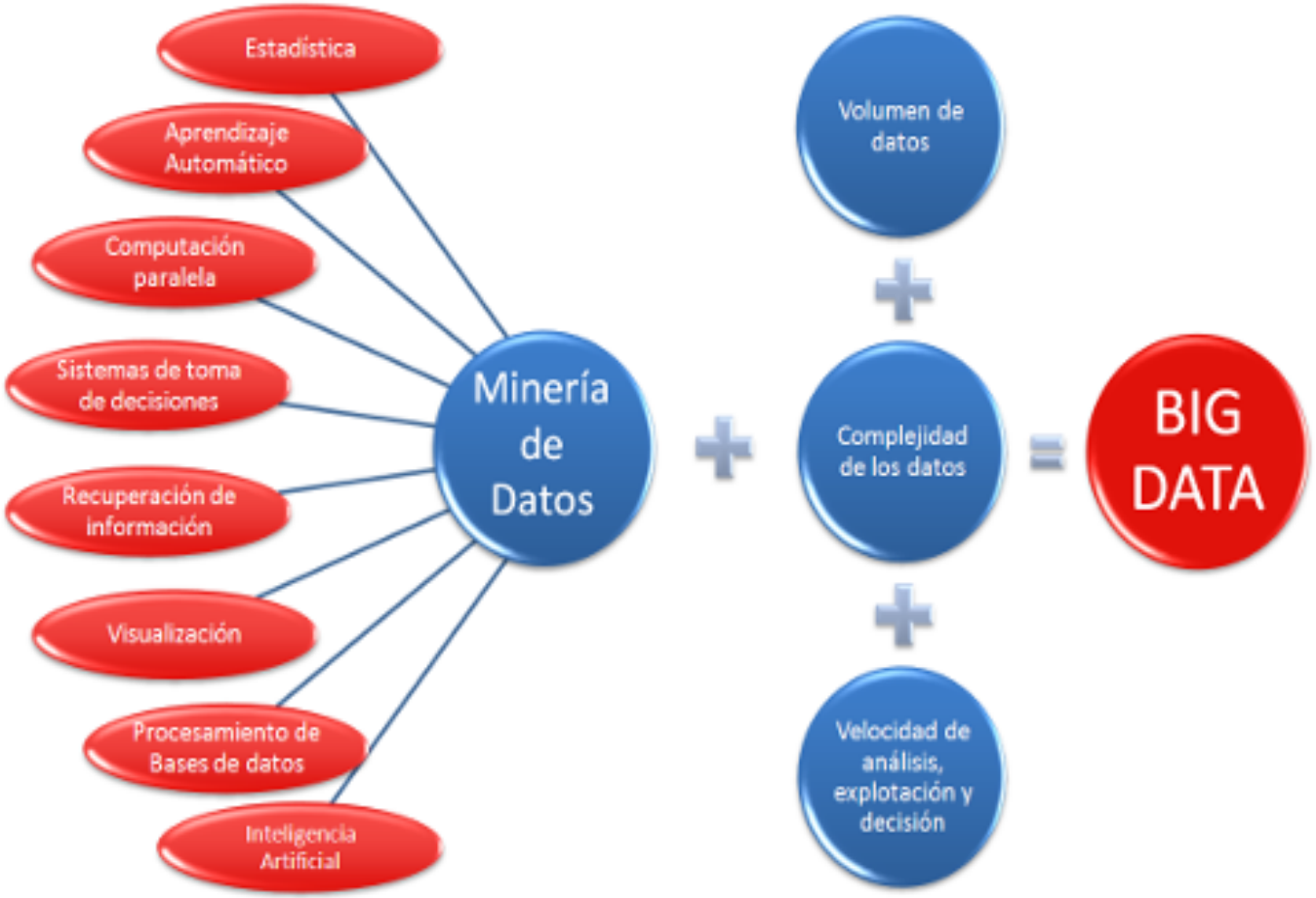
PRIMER PLANO

MUCHOS DETALLES

2.1. Retos para los sujetos obligados

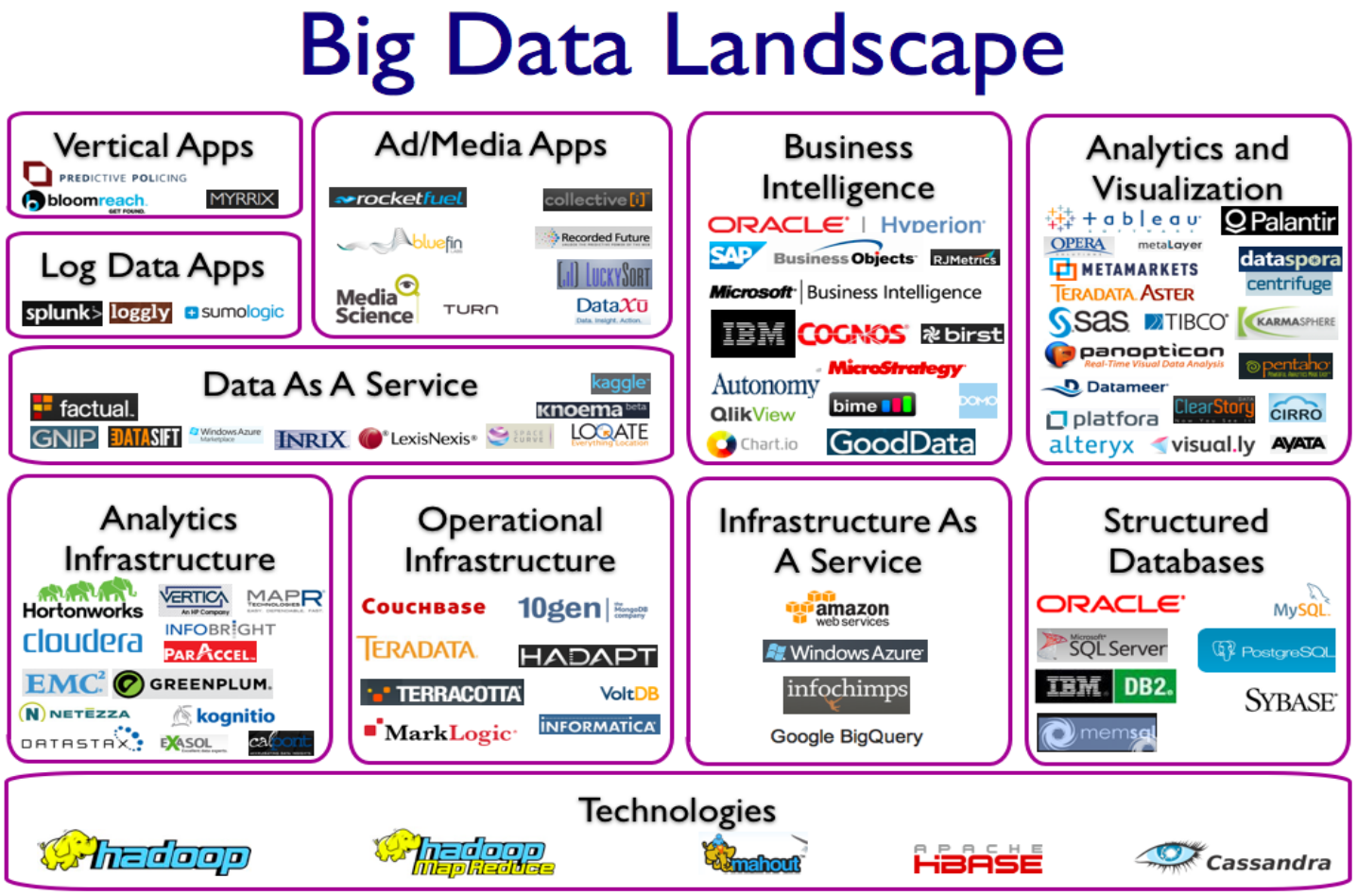
- Diferencias entre “big data” y “minería de datos”:
  - “Big data” es un término para un conjunto de datos de gran tamaño: aquellos que superan el simple tipo de arquitecturas de bases de datos y manejo de datos que se utilizaron en los primeros tiempos, cuando el procesamiento de los grandes datos era más caro y menos factible.
  - Mientras la “minería de datos” se refiere a la actividad de pasar por los conjuntos de grandes datos para buscar información pertinente u oportuna. Este tipo de actividad es realmente un buen ejemplo del viejo axioma "buscar una aguja en un pajar".

2.1. Retos para los sujetos obligados



Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados



dave@vcdave.com

blogs.forbes.com/davefeinleib

BIG DATA LANDSCAPE 2017

V2 – Last updated 5/3/2017

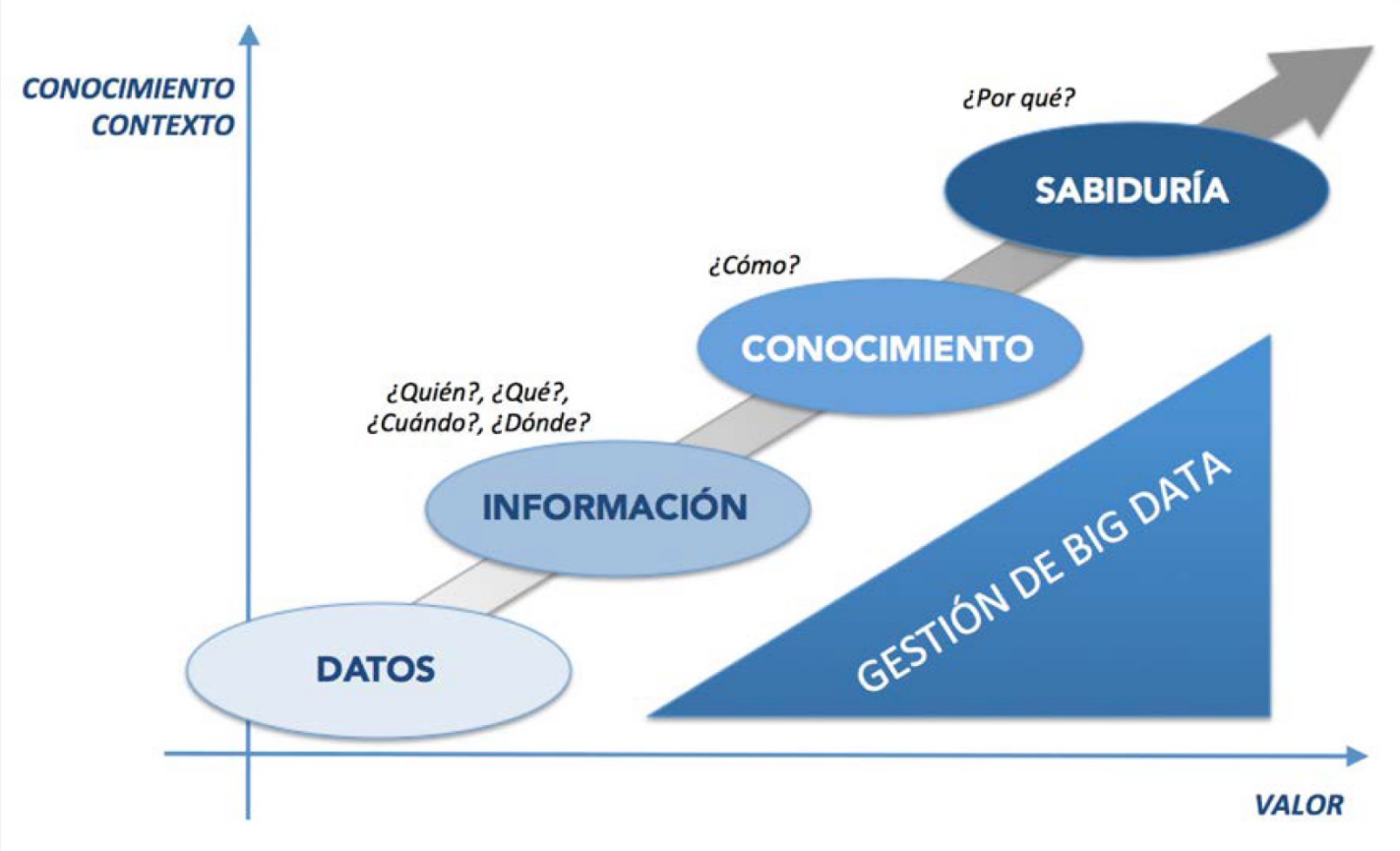
 mattturck.com/bigdata2017

FIRSTMARK
EARLY STAGE VENTURE CAPITAL

2.1. Retos para los sujetos obligados

Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados



Cadena de gestión del conocimiento.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Objetivos de los retos:
    - Maximizar el valor que general su uso mientras se protegen adecuadamente los datos personales de los titulares.
    - Lograr que la protección de los datos en el uso de la minería de datos se vuelva una ventaja competitiva.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Beneficios de la minería de datos para las entidades del sector público como administraciones públicas:

    Analizar y explotar 'big data' permite a las administraciones:

    - Tomar mejores decisiones, al basarlas en un mayor número de fuentes de información y en su combinación.
    - Ofrecer servicios más personalizados a los usuarios.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Retos del uso de la minería de datos para que sea posible lograr todo su potencial:
    - En cuanto a la infraestructura tecnológica: necesario desarrollar e implantar nuevos modelos de bases de datos, almacenamiento, etc.;
    - En cuanto a la metodología de análisis: en tiempo real y de correlación de eventos y datos;

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los 'big data' ('grandes datos').
  - Retos del uso de la minería de datos para que sea posible lograr todo su potencial:
    - En cuanto a seguridad de la información y protección de datos: debido a la dimensión mucho mayor de las consecuencias de un ataque afectando la seguridad de la información de bases de datos resultando de proyectos de minería de datos, los retos son a nivel de la infraestructura de seguridad, de la gestión de los datos, de la protección de la confidencialidad (autenticación, control de acceso, cifrado, anonimización, etc.).

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los ‘big data’ (‘grandes datos’).
  - Reto fundamental: proteger los datos de los titulares para asegurar el valor de los ‘big data’.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los ‘big data’ (‘grandes datos’).
  - ¿En qué la minería de datos amenaza la privacidad?

2.1. Retos para los sujetos obligados

- Caso Netflix:
  - Con un conocimiento acerca de alguna característica de un usuario de Netflix, es posible identificar qué valoraciones de películas ha escrito ese usuario.

2.1. Retos para los sujetos obligados

- Caso de la reidentificación del Gobernador de Massachusetts:
  - Listas de datos anonimizados de los empleados estatales del estado de Massachusetts, incluyendo información de salud para que sirva a investigadores. Una científica de datos pudo reidentificar los datos anonimizados. Conclusión: un 87% de los estadounidenses podían ser inequívocamente identificados sólo con su código postal, fecha de nacimiento y sexo.

2.1. Retos para los sujetos obligados

- Caso Target:
  - Adolescente embarazada.

➔ Cualquier solución de ‘big data’ tiene que tomar en cuenta los aspectos de privacidad.

2.1. Retos para los sujetos obligados

- Retos derivados del uso de los ‘big data’ (‘grandes datos’).
  - ¿Cómo la minería de datos ha modificado la definición de los “datos personales”?

2.1. Retos para los sujetos obligados

- ¿Cómo la minería de datos ha modificado la definición de los "datos personales"?
  - Concept de "identificación indirecta". Combinación del metadato con otros datos puede identificar a una persona indirectamente.

2.1. Retos para los sujetos obligados

- ¿Cómo la minería de datos ha modificado la definición de los "datos personales"?
  - Tipos de datos personales:

    Según la forma en que los datos se obtienen:
    - Compartidos por titular de forma voluntaria.
    - Datos observados: capturados por una organización a raíz de las acciones de las personas (p.ej. datos de localización).
    - Datos inferidos/agregados: obtenidos del análisis de otros datos voluntarios, observados o también inferidos.

2.1. Retos para los sujetos obligados

- ¿Cómo la minería de datos ha modificado la definición de los "datos personales"?
  - Tipos de datos personales:

    Según su capacidad para suponer vulneraciones de la privacidad:
    - Datos identificativos:
      - Directos: permiten identificación inequívoca de una persona.
      - Datos biométricos.
      - Datos de identificación débil: potencialmente podrían identificar individuos, pero para lo cual deberán combinarse con otros y acompañarse de un trabajo de análisis. P.ej. direcciones IP, pseudónimos, etc.

2.1. Retos para los sujetos obligados

- ¿Cómo la minería de datos ha modificado la definición de los "datos personales"?
  - Tipos de datos personales:

    Según su capacidad para suponer vulneraciones de la privacidad:
    - Datos distintivos:
      - Datos de comportamiento: localización, hábitos de compra, patrones de navegación en Internet, etc.
      - Datos de opiniones (caso Netflix).
      - Información sensible: médica, salud, situación financiera.

2.1. Retos para los sujetos obligados

- ¿Cómo la minería de datos ha modificado los principios de protección de datos personales que han permitido asegurar la protección de la privacidad hasta ahora?
  - Los principios fundamentales de protección de la privacidad (*Fair Information Privacy Practices*, o "FIPP"):

2.1. Retos para los sujetos obligados

- Los principios fundamentales de protección de la privacidad (*Fair Information Privacy Practices*, "FIPP"):
  - 1. limitación en recopilación de datos / minimización;
  - 2. calidad e integridad de datos;
  - 3. determinación explícita de la finalidad de tratamiento;
  - 4. limitación de uso;
  - 5. seguridad;
  - 6. transparencia;
  - 7. participación individual;
  - 8. responsabilidad y auditoría.

2.1. Retos para los sujetos obligados

Laurant
Law Firm / Abogados

2.1. Retos para los sujetos obligados

- Los FIPP deben evolucionar para adaptarse a las especificidades por los problemas específicos que genera la minería de datos:
  - Maneras de abordar la reutilización de información para finalidades diferentes; difícil determinar a priori esas finalidades.
  - Uso combinado de datos de distintas fuentes, algunos son personales, algunos no al principio.
  - Evaluación o segmentación de individuos por su perfil (para propósitos que van desde marketing hasta decisiones de contratación).

2.1. Retos para los sujetos obligados

- Los FIPP deben evolucionar para adaptarse a las especificidades por los problemas específicos que genera la minería de datos:
  - Consentimiento no necesario al momento de empezar la minería de datos; una vez que se identifica a personas, se vuelve difícil de obtener del titular. Consentimiento tampoco puede ser completamente informado cuando se trata de minería de datos.
  - Principio de participación individual puede volverse inviable si se trata de obtener acceso a todos los datos que se usaron para generar a nuevos datos personales sobre el titular; tampoco va a ser fácil de permitir al titular el acceso al algoritmo que lo generó por razones de protección de los secretos empresariales.

2.1. Retos para los sujetos obligados

- El modelo de notificación y consentimiento: se ha vuelto impráctico e inefectivo para realmente proteger al titular.
- El consentimiento es un enfoque poco apropiado para legitimar muchos aspectos del tratamiento de datos en Internet.

2.1. Retos para los sujetos obligados

- Retos para la protección de la privacidad:
  - Pensar en soluciones que permitan a la minería de datos de asegurar su cumplimiento con el marco legal aplicable;
  - Incorporar 2 objetivos: utilidad de la herramienta de minería y grado de protección del conjunto de datos personales que se mina. (Cfr solución de Facebook.)
  - Necesidad de reformar los marcos legales de protección de datos que todavía están en su mayoría enfocados en legitimar el tratamiento de datos en la notificación de la información sobre el tratamiento y el consentimiento).

2.1. Retos para los sujetos obligados

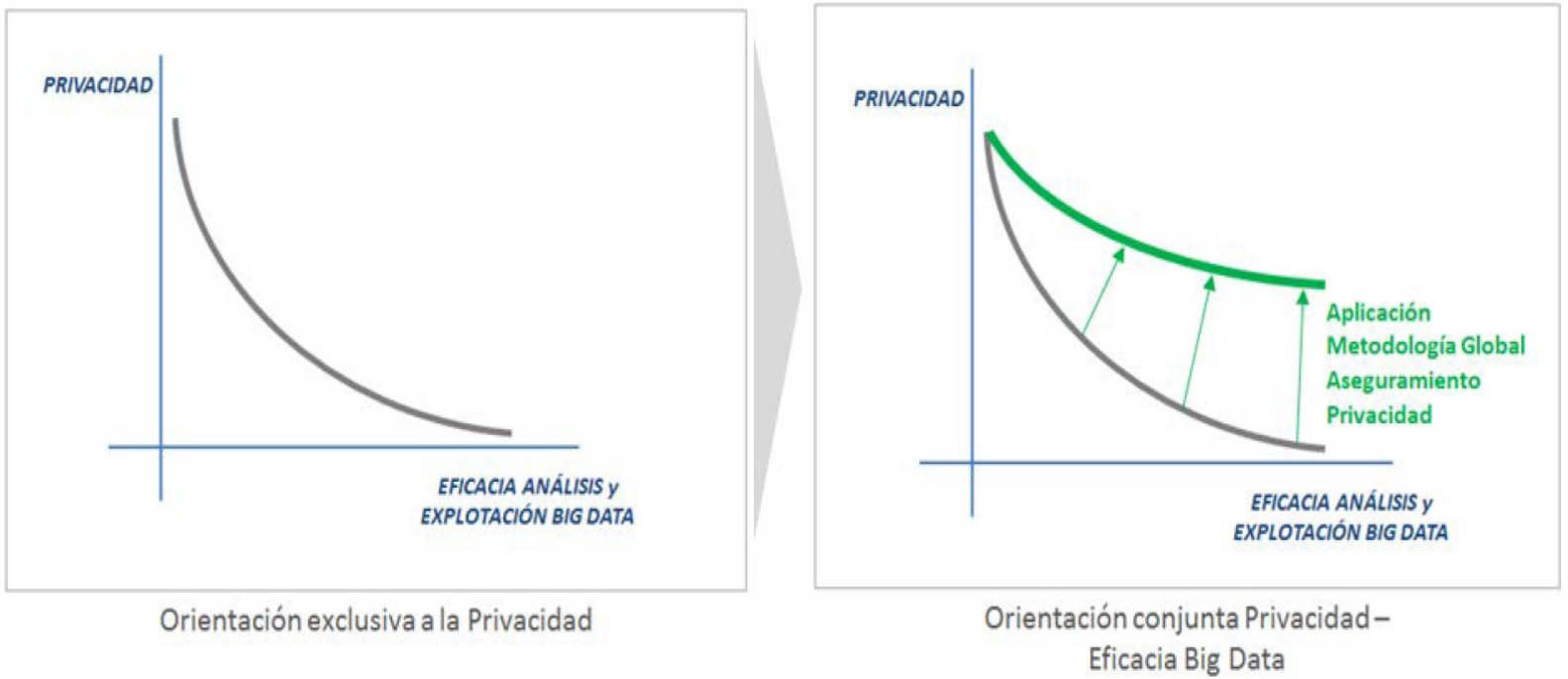
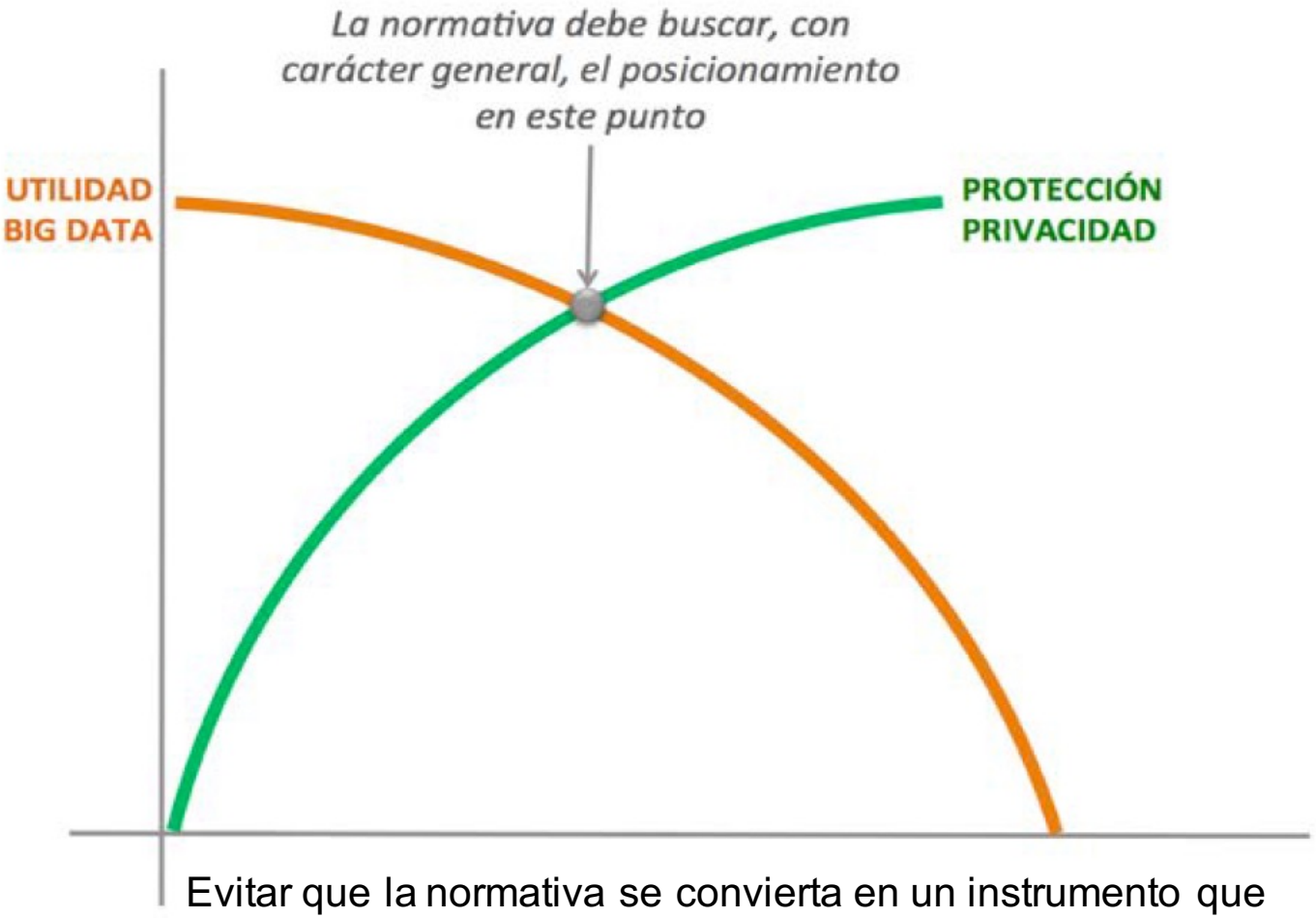


Imagen I-4 – Gráficas ilustrativas tendencia compromiso Utilidad – Protección Privacidad
(Elaboración propia)

2.1. Retos para los sujetos obligados



Evitar que la normativa se convierta en un instrumento que impida aprovechar todos los beneficios de la minería de datos, pero tampoco que se vuelva un trámite que no permita ningún tipo de protección).

2.1. Retos para los sujetos obligados

FIPP	Impacto de los Big Data
1. Limitación en la recopilación de datos / Minimización de datos.	ALTO Se trata de un aspecto cuyo mantenimiento en los términos actuales no es compatible con la naturaleza de los Big Data.
2. Garantía de la Calidad e Integridad de los datos.	BAJO La redacción actual de este principio seguiría en principio siendo válida en el contexto de los Big Data.
3. Determinación explícita del Propósito para el que	ALTO No es posible a priori determinar todos los propósitos para

se recopilan los datos.	los que una serie de datos personales se recopilan en un contexto de gestión de Big Data.
4. Limitación de uso.	**ALTO** Dada la relación con el principio anterior, también se trata de un principio que debería ser revisado para asegurar su aplicación en entornos Big Data.
5. Seguridad.	**BAJO** La redacción actual de este principio seguiría en principio siendo válida en el contexto de los Big Data.
6. Transparencia.	**BAJO** La redacción actual de este principio seguiría en principio siendo válida en el contexto de los Big Data.
7. Participación Individual.	**ALTO** En muchas ocasiones es imposible que los usuarios puedan saber los propósitos para los que serán usados sus datos, así como analizar detalladamente los algoritmos que se usarán en su procesado.
8. Responsabilidad y Auditoría.	**MEDIO** La redacción original se centra en el cumplimiento de los principios y de la normativa en vigor, si bien debería orientarse más hacia la administración responsable de datos y al uso de mecanismos (como las evaluaciones de impacto de privacidad) para asegurar el cumplimiento y demostrar el mismo a las autoridades responsables.

2.1. Retos para los sujetos obligados

- Soluciones:
  - La utilidad del principio de notificación y consentimiento pierde terreno.

2.1. Retos para los sujetos obligados

- Soluciones:
  - Se puede sustituir por asegurarse que la organización que usa minería de datos lo haga de forma responsable, no sólo al momento de recopilar datos personales del titular, con o sin su consentimiento, sino en todas las etapas de tratamiento y con obligaciones que implica el principio de responsabilidad comprobada: (cfr Regul. Gen. de Prot. de Datos de la U.E. ("RGPD")):
    - Documentación de procesos;
    - Evaluaciones de impacto en la protección de datos; y
    - Mecanismos de protección de datos por diseño y por defecto.

2.1. Retos para los sujetos obligados

- Soluciones:
  - También el RGPD prevé:
    - Más control para el titular como el "derecho al olvido" y el derecho a la portabilidad de datos.
    - Aplicabilidad más amplia a responsables de tratamiento (tratan datos personales de titulares que residen en la U.E. y las actividades de tratamiento afectan a la prestación de bienes o servicios a titulares de datos de la U.E. o se monitoriza su comportamiento).

2.1. Retos para los sujetos obligados

- Retos para los sujetos obligados en México:
  - Nueva ley (LGPDPPSO): todavía se basa en el paradigma de los FIPPs y de la notificación y consentimiento. ➔ El uso de 'big data' se hace parcialmente en violación al marco legal.
  - No existe ningún lineamiento (que hayamos encontrado) del INAI u otra autoridad en México que explique cómo desarrollar un tratamiento con 'big data' en cumplimiento de la LGPDPPSO.

2. El uso de los ‘big data’ en Internet

- 2.1. Retos para los sujetos obligados.
- **2.2. Recomendaciones para los sujetos obligados.**

2.2. Recomendaciones para los sujetos obligados

- 1. La LGPDPPSO hace referencia a varios conceptos que consagró la Regulación General de Protección de Datos de la U.E.:
  - Privacidad por defecto y privacidad por diseño;
  - Evaluación de impacto a la privacidad;
  - Responsabilidad comprobada.

  Varios de estos conceptos ponen énfasis en la necesidad de documentar sus procesos para demostrar que la empresa ha hecho su trabajo de debida diligencia.

2.2. Recomendaciones para los sujetos obligados

- Implementar la LGPDPPSO y su futura ley estatal prestando particular atención a las obligaciones de **documentación de procesos y** (en aplicación del principio de responsabilidad comprobada).

Gracias.

Laurant

Law Firm / Abogados

Cédric Laurant

★ *Dueño*, Laurant Law Firm/Abogados

twitter @cedric_laurant

E-mail: info [arroba] cedriclaurant [punto] com

Website: http://cedriclaurant.com

Blogs: https://blog.cedriclaurant.org
https://blog.security-breaches.com

Laurant
Law Firm / Abogados

Fuentes de información

- Wilma Arellano Toledo, "Gobierno abierto y privacidad: la problemática del Big Data y el Cómputoen la Nube", Revista Virtualis, Tecnológico de Monterrey, año 5, No. 10, julio-diciembre 2014, pp 33-60.
- Lilie Coney, Amie Stepanovich & Colin Irwin (Electronic Privacy Information Center), Workshop comments to the Privacy Office of the Department of Homeland Security at the Government 2.0 Workshop: Privacy and Best Practices, Docket No. DHS-2009-0020, 1 junio 2009.
- J. Ignacio Criado y Francisco Rojas-Martín (eds), *Las redes sociales digitales en la gestión y las políticas públicas. Avances y desafíos para un gobierno abierto*, Escola d'Administració Pública de Catalunya, Barcelona, diciembre 2013.
- Electronic Privacy Information Center, "Privacy and Government Contracts with Social Media Companies", https://epic.org/privacy/socialnet/gsa/.
- *Big Data & Privacy – Making Ends Meet*, Future of Privacy Forum & The Center for Internet and Society, Stanford Law School, septiembre 2013.
- Gang-Hoon Kim, Silvana Trimi & Ji-Hyong Chung, "Big-Data Applications in the Government Sector", Communications of the ACM, Vol. 57, No. 3, marzo 2014, pp 78-85.
- Ley de Protección de Datos Personales del Estado de Chihuahua, Periódico Oficial del Estado No. 51, 28 junio 2013.
- Julia Manske, David Sangokoya, Gabriel Pestre, Emmanuel Letouzé, "Oportunidades y requerimientos para aprovechar el uso de *Big Data* para las estadísticas oficiales y los Objetivos de Desarrollo Sostenible en América latina", Data-Pop Alliance Harvard Humanitarian Initiative, MIT Media Lab y Overseas Development Institute), White Paper Series, mayo 2016.
- *Manual sobre utilidades del big data para bienes públicos*, Goberna América Latina, Escuela de Política y Alto Gobierno, Instituto Universitario de Investigación Ortega y Gasset, y Entinema, Madrid, 2017.
- Katina Michael & Keith W. Miller, "Big Data: New Opportunities and New Challenges", *Computer*, IEEE Computer Society, junio 2013.
- Alberto Quiñones Layos, "Protección de la privacidad en la gestión de big data. Una visión multidimensional: tecnología y normativa", proyecto de fin de carrera, Universidad Carlos III de Madrid, versión 1.0, 15 octubre 2015.
- Hervais Simo, "Big Data: Opportunities and Privacy Challenges" (working draft paper), Fraunhofer-Institut für Sichere Informationstechnologie, Alemania, sin fecha.

Laurant
Law Firm / Abogados