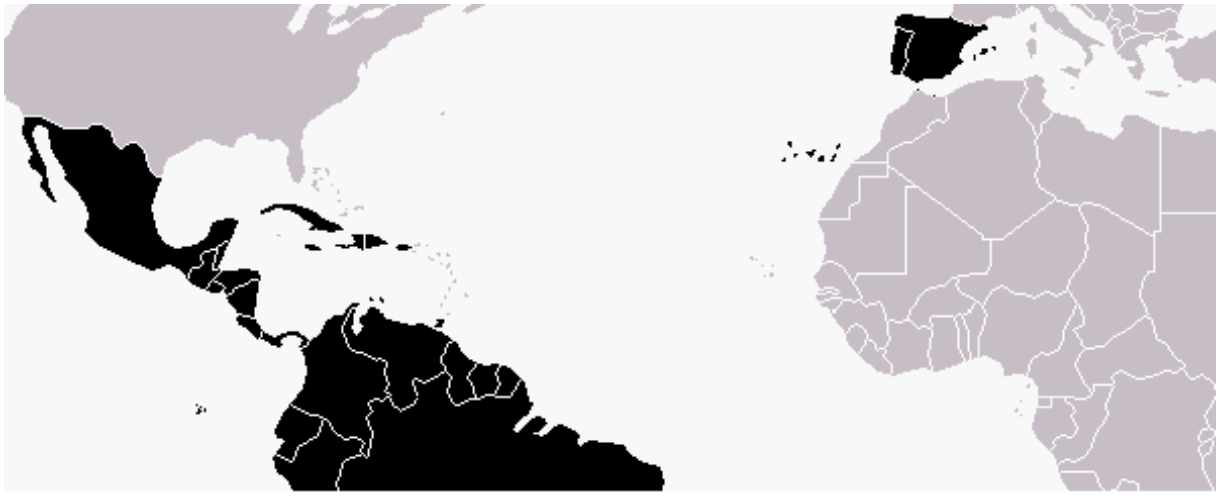

Declaración de México D. F., hacia la implantación de garantías para la privacidad en los tratamientos de Big Data [1]

Hoy en día, en un mundo digitalizado, la naturaleza de la información es diferente a la que disponíamos en el pasado. Es así debido a la abundancia de orígenes disponibles, cada uno con su peculiar variedad de datos. Un tipo de fuentes son las que se refieren a datos creados directamente por las personas, como pueden ser la informática tradicional corporativa, redes sociales, transacciones de comercio electrónico, formularios web, blogs, centros de atención a clientes, etc. y sus posibles indexaciones en motores de búsqueda. Otro tipo, que se prevé sea dentro de poco el segmento más grande de toda la información disponible, se refiere a los datos obtenidos por máquinas, como pueden ser sensores, micrófonos, cámaras de video, escáneres médicos, equipos industriales, GPS, dispositivos móviles, nuevas generaciones de electrodomésticos, electrónica para vestir (wearable devices), etc. que también puede ser indexado.

Todos estos tipos de datos forman parte del tejido de nuestras vidas más profundamente que nunca. La recolección, el almacenamiento, el procesamiento y el posterior análisis de datos se

[1] *La Declaración de México D.F., hacia la implantación de garantías para la privacidad en los tratamientos de Big Data, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada el sábado 23 de agosto de 2014 por Dulcermaría Martínez Ruíz, en el trasncurso de la Jornada académica de protección de datos personales en internet, dentro de la bienvenida para los alumnos de la cuarta generación de la Maestría en Derecho de las Tecnologías de la Información y Comunicación de INFOTEC, en la ciudad de México Ditrito Federal.*

encuentra en una fase de expansión paradigmática, impulsada por el aumento de la capacidad de procesamiento y el creciente número de tecnologías integradas en dispositivos de todo tipo.

Además se debe tener en cuenta que tanto en el presente como en el futuro, a los datos se le ha asignado un valor estratégico en varias industrias y mercados. Es decir, se han convertido en una clase de activos, esto es, lo equivalente al petróleo, sobre todo, por su fácil disponibilidad y procesamiento. Lo cual va a permitir llevar a cabo una nueva interpretación de los mismos de manera novedosa, dándoles un mayor valor agregado.

El valor de los datos no es sólo económico sino también social, científico, político y cultural. Son innegables, inimaginables y hasta inevitables las cosas que pueden alcanzarse con el trío conformado por datos personales, tecnología y análisis. A partir de ellos puede contarse con instrumentos para tomar mejores decisiones con información amplia y detallada y predecir algunas cosas.

En este contexto podemos definir Big Data como los sistemas y herramientas que son capaces de tratar ingentes cantidades de datos en un tiempo muy inferior en el que lo harían los equipos tradicionales, permitiendo su almacenamiento, búsqueda, visualización, compartición, segmentación y análisis. En la misma línea está la definición dada por McKinsey Global Institute (MGI), que lo entiende como el "conjunto de datos cuyo tamaño, y demás características, van más allá de las capacidades de captura, almacenamiento, tratamiento y análisis mediante herramientas tradicionales de gestión de base de datos".

Suele argumentarse que Big Data se encuentra intrínsecamente relacionado con el Internet de las Cosas (IoT), es decir, con el diseño de una estructura de red interconectada que permite que dispositivos físicos se comuniquen entre sí con la capacidad para transmitir, compilar y analizar datos. Ordenadores de bajo consumo, teléfonos más planos, tablets con pantallas más grandes, electrodomésticos "inteligentes" como cámaras Web con sensor de movimiento, alarmas, SmartTVs, aspiradoras robotizadas, o los famosos "wearables", entre otros, en forma de pulsera, que se encarga de medir parámetros de nuestro cuerpo: sudoración, ritmo cardiaco, calorías consumidas, horas de sueño efectivo..., elementos que forman parte de nuestra vida cotidiana, cuyo denominador común es contar con una pila TCP/IP, que les dota de conexión a un ecosistema en el que interactúan con otros dispositivos. Debido a la naturaleza ubicua de objetos conectados en la IoT, se espera que un número sin precedentes de dispositivos que se conecten a Internet,

estimándose cerca de 26 mil millones de dispositivos en el Internet de las Cosas en 2020, siendo esta última una fuente de recolección de datos que crece exponencialmente y, en consecuencia, adecuada para ser procesada mediante sistemas Big Data.

Las características principales de un sistema Big Data suelen está referido a sus 5"V" , es decir su capacidad relacionada con el volumen de la cantidad de datos para almacenar y procesar; la velocidad de transformación de los datos en información útil en el menor tiempo posible; la variedad de datos que un sistema de Big Data procesa y la heterogeneidad de sus formatos (bases de datos, HTML, XML, texto plano, imágenes, video, audio, código fuente, etc.); la veracidad de los datos y el valor del sistema Big Data en sí mismo, esto es, su capacidad para obtener valor de todos los datos disponibles a través de un almacenamiento y procesamiento eficiente y al menor coste posible.

Según lo señalado, el análisis de los datos no estructurados no es una aplicación trivial, y tratar de analizar petabytes o conjuntos de datos más grandes puede magnificar las dificultades que entrañan la extracción, transformación, carga, almacenamiento y procesamiento de datos. El análisis basado en la transmisión de grandes cantidades de datos sociales ofrece la posibilidad de crear perfiles sociales, por lo que la puerta que se ha abierto para los nuevos tipos de tratamiento pueden crear problemas legales. La creación de perfiles para la predicción de conductas, la observación y modelación del comportamiento de las personas (profiling) surgen entonces, como un alerta a la necesidad de una protección legal de los datos, su seguridad y el respeto a la privacidad cuando estas tecnologías van ligadas a contratos de adhesión o a usos delictivos de estos datos (saber por tu consumo eléctrico cuando no estás en casa). Así, estos grandes volúmenes de datos han expresado ya problemas concretos: falta de coordinación transnacional, infraestructura y financiación inadecuada, falta de expertos en información y conocimientos relacionados y un marco jurídico fragmentado y complejo. Los análisis de Big Data y su recopilación, sin un determinado marco jurídico, esgrime el surgimiento de nuevos problemas de privacidad y autodeterminación informativa.

1. TRABAJOS PREVIOS O EN PREPARACIÓN A NIVEL INTERNACIONAL

A nivel Internacional, contamos con los siguientes estudios, recomendaciones y documentos.

1. En enero de 2014, el presidente Barack Obama, presionado por las revelaciones de Edward Snowden, se vio forzado a presentar un discurso ante el Departamento de Justicia de los Estados

Unidos donde se comprometió a modificar el programa de vigilancia sobre datos telefónicos. En ese mismo discurso dispuso que un grupo de expertos confeccionara rápidamente un informe que detalle las consecuencias relevantes del Big Data y se emitieran una serie de recomendaciones.

El informe, titulado "Seizing opportunities, preserving values" (mayo de 2014), reafirma que las tecnologías de Big Data, como toda tecnología, no son per se buenas o malas, pueden ser utilizadas para el bien general de la sociedad o para producir daños. Afirma que en su faz positiva puede fortalecer la democracia, generar crecimiento económico y mejorar la calidad de vida de los ciudadanos al mejorar los servicios de salud, educación, así como la seguridad interior y nacional.

También considera que los datos generados son ahora más valiosos e invasivos. Si bien indica que el potencial positivo es enorme, también pueden darse usos perjudiciales que afecten valores básicos de justicia y equidad. Debido a que no siempre todos los agentes que acceden a grandes volúmenes de información poseen los mismos recursos para procesarlos, es esperable la aparición de nuevas asimetrías entre instituciones e individuos.

Asimismo identifica un fuerte interés del sector privado, pues esta tecnología permite crear perfiles de consumidores con mayor facilidad y precisión, que además también pueden ser comercializados. Expresamente se resalta el problema resultante de la falta de conocimiento de los consumidores, quienes, en la mayoría de los casos no son conscientes en qué medida ellos mismos son los productos que se comercializan.

Respecto de la discriminación y su relación con los derechos ciudadanos señala que el tratamiento de datos habilita a los gobiernos a realizar prácticas discriminatorias por medio de la implementación de determinadas políticas públicas, sin tomar en consideración las necesidades de grupos minoritarios. Finalmente concluye que los principales valores en peligro son los relacionados con la privacidad, por lo que es necesario preservarlos mediante la protección de toda información personal, con mejores y más actualizadas leyes de protección a los consumidores y a los ciudadanos en general, garantizando que la información recolectada sea utilizada para los fines permitidos y declarados con anterioridad.

El 23 de abril del 2014, bajo el lema "Rewards and Risks of Big Data (Recompensas y riesgos de los grandes volúmenes de datos) se presentó la 13ª edición de The Global Information Tecnology Report, documento elaborado por el Foro Económico Mundial y el INSIDE. Dicho informe recoge las

debilidades que aún subsisten en el sistema empresarial y de innovación en las Tecnologías de la Información y las Comunicaciones de 148 economías.

Entre otras cosas, en el citado informe se hace un análisis respecto a la postura que deben asumir los países frente a la madurez de los volúmenes de las grandes bases de datos; así como la manera en que deben ser tratados, a fin de obtener de los mismos mayores beneficios comerciales y organizativos. Sin dejar de lado, la necesidad de que se cuente con políticas adecuadas para que la Internet de Todo puede concretar su promesa de proporcionar inmensos beneficios económicos y sociales. La importancia de este documento radica en que a través del mismo se puede medir el impacto que puede llegar a tener el big data en la privacidad de las personas y los beneficios que podrían representar para las empresas, incluso, para los propios gobiernos. Y sin duda, puede ser un referente a la hora de buscar una armonización de los reglamentos sobre la protección de datos a nivel mundial.

2. En abril de 2013, el Grupo de trabajo internacional de Berlín sobre protección de datos en las Telecomunicaciones, presentó el "Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy". El documento expresa que uno de los fundamentos de la protección de datos es el derecho de los sujetos a controlar su propia información, teniendo el derecho a que se elimine la información procesada ilegalmente, o la producida sin su consentimiento. En este sentido, el "derecho al olvido" se presenta como esencial, en los casos en donde hay interés legítimo avalado legalmente, asegurando que no se afecte la libertad de expresión y la libertad de prensa.

En el caso de la información existente en Internet, dada su estructura, el "derecho al olvido" sería más bien un "derecho a no ser encontrado". Actualmente no hay forma técnica de identificar y localizar todas las copias disponibles de algún archivo o información específica en Internet, lo cual no obsta que la nueva información generada sea posible establecer mecanismos que funcionen como fechas de vencimiento, garantizando que dejen de estar disponibles pasadas determinadas fechas de forma automática. El grupo de trabajo alienta a los actores relevantes (sector privado, académico y gobiernos) a fortalecer sus esfuerzos para progresar en este campo. Asimismo, debe tenerse presente que puede restringirse la disponibilidad de determinada información restringiendo los resultados ofrecidos por los servicios de búsqueda, y que es posible otorgar a los usuarios herramientas para eliminar su propia información personal.

3. La Cloud Security Alliance por medio de su Grupo de Trabajo sobre Big Data emitió en marzo de 2014, un comentario sobre Big Data y el futuro de la privacidad, sintetizando que el interés por parte de los gobiernos en el tratamiento de información debería centrarse simultáneamente en cuestiones de acceso, propiedad, privacidad, transparencia y responsabilidad.

Señala que la protección de la privacidad se ha convertido en un objetivo difícil de alcanzar, ya que investigadores han demostrado que los individuos pueden ser re-identificados fácilmente mediante el cruce de diferentes bases de datos. Asimismo, el lugar en dónde se almacenan los datos, el lugar en donde se procesan y los lugares en donde se distribuyen los resultados derivados de su análisis determinan la competencia de diferentes jurisdicciones, las cuales protegen con diferente intensidad la privacidad de los sujetos.

Remarca también que nuevas tecnologías de encriptado de datos posibilitarían un uso efectivo del Big Data resguardando al mismo tiempo la privacidad de los sujetos generadores de información, aunque estas tecnologías no deberían implementarse en forma aislada sin ser acompañada por un marco de leyes adecuadas y buenas prácticas.

4. Otros antecedentes existentes en materia de seguridad de la información pueden ser examinados a la luz de la problemática específica del Big Data. El National Institute of Standards and Technology (NIST), publicó en septiembre de 2011 el SP 800 – 137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations". El documento reconoce que para garantizar la seguridad de la información se requiere de órganos específicos que identifiquen y respondan frente a las nuevas vulnerabilidades emergentes y amenazas cambiantes, en un entorno de cambio de organización e infraestructura.

El informe resalta la importancia de un control constante como parte de los procesos de administración de riesgos, para alcanzar un nivel de riesgo aceptable y es por ello que recomienda a las organizaciones públicas o privadas definir en primer lugar una estrategia de control constante sobre la seguridad de la información, establecerla en un programa de acción e implementarla para luego analizar la información resultante y las vulnerabilidades descubiertas y responder frente a ellas para así poder, en última instancia, revisar la estrategia y el programa de acción diseñado, para actualizar y mejorar el esquema general de seguridad y aumentar la calidad de la seguridad de la información al final de cada ciclo.

5. El grupo de estudio ad hoc "Next Generation Analytics and Big Data" - integrante del comité sobre gestión de datos y normas de intercambio (SC32) del JTC1 de la Organización Internacional de Normalización (ISO/CEI) - publicó en junio de 2013 su reporte preliminar sobre la gestión de grandes cantidades de datos. El documento reconoce que la protección de la privacidad es un factor a considerar, y que no tenerlo en cuenta puede derivar en temores públicos generales sobre la existencia de un "Gran Hermano", diferentes sanciones de organismos protectores de la privacidad, y acciones judiciales, incluso colectivas.

6. El reporte "Right to Privacy in the Digital Age" (junio de 2014), presentado por el Alto Comisionado para los Derechos Humanos de las Naciones Unidas, sobre la cuestión de la recolección masiva de datos vista desde el derecho a la privacidad.

El Alto Comisionado afirma que el derecho internacional de los derechos humanos contiene el marco frente al cual toda interferencia al derecho a la privacidad debe ser confrontado, aclarando que este no es el único derecho violado frente a prácticas de vigilancia masiva, intercepción de comunicaciones privadas y recolección de datos personales.

El reporte cuestiona el grado en que los consumidores son realmente conscientes de los datos que están compartiendo, de qué manera lo hacen, con quiénes y para qué fines, frente a las posiciones que sostienen que el transporte e intercambio de información personal a través de medios electrónicos es parte de un acuerdo consciente mediante el cual los individuos entregan voluntariamente información sobre sí mismos y sus relaciones, a cambio de acceso digital a bienes, servicios e información.

También definen como no convincente a la distinción entre datos y metadatos. Cualquier captura de datos de comunicación interfiere potencialmente con la privacidad, y la recolección y el almacenamiento de estos datos conforman una injerencia en la vida privada, sean esos datos posteriormente consultados o no. Incluso la mera posibilidad de que esa información pueda ser interceptada crea una injerencia en la vida privada por el potencial efecto negativo sobre varios derechos, incluidos los de la libertad de expresión y de asociación.

Nadie puede ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Las injerencias permitidas por leyes nacionales pueden ser ilegales si

aquellas leyes están en conflicto con el derecho internacional de los derechos humanos. Los estados deben probar que las injerencias son necesarias, proporcionales y que respetan los principios de legalidad.

El reporte reconoce que estamos presenciando la emergencia de una práctica de los estados que consiste en externalizar las tareas de vigilancia masiva en terceros. Reconocer la existencia de fuerte evidencia de una creciente dependencia de los gobiernos para con el sector privado, en cuanto a llevar a cabo y facilitar tareas de vigilancia digital.

Cuando una compañía suministra los datos o la información de un usuario a un estado en respuesta a una solicitud que contravenga el derecho a la privacidad según el derecho internacional, o una empresa ofrezca tecnología de vigilancia de masas o equipos a los estados sin salvaguardas adecuadas, o cuando la información se utiliza de alguna manera en violación de los derechos humanos, las empresas corren el riesgo de ser cómplices o verse involucrados en violaciones de los derechos humanos.

Cuando las empresas se enfrentan a demandas de gobiernos para acceso a datos que no cumplan con las normas internacionales de derechos humanos, se espera que traten de honrar los principios de los derechos humanos en la mayor medida posible y que sean capaces de demostrar sus continuos esfuerzos en ese sentido.

7. El 28 de julio de 2014 el Information Commisioner´s Office del Reino Unido ha publicado un informe titulado "Big Data and Data Protection". Para el ICO operar dentro de la ley no debería considerarse como una barrera a la innovación. El Informe expone cómo se aplica la ley cuando Big Data utiliza la información personal. Detalla que aspectos de la ley necesitan considerar particularmente las organizaciones para poder innovar sin situarse al margen de la ley. Las organizaciones necesitan pensar en formas innovadoras para decir a los clientes lo que quieren hacer y lo que esperan lograr. El informe también aborda las inquietudes planteadas por algunos comentaristas que no encajan la actual ley de protección de datos con Big Data. Para el ICO los principios de protección de datos básicos ya establecidos en la ley del Reino Unido y la Directiva 95/46 son lo suficientemente flexibles para cubrir Big Data. Los principios todavía son aptos para el propósito, pero las organizaciones necesitan innovar al aplicarlos. También valora positivamente las nuevas herramientas previstas en la Propuesta de Reglamento General de Protección de Datos de la UE para este tipo de tratamientos.

2. BIG DATA COMO SERVICIO DE TI

Big data es uno más de los servicios que ofrece el área de Tecnologías de la Información (TI) a la organización con el objetivo de poder obtener valor a partir de la información. Esa finalidad se consigue mediante el análisis de los datos, obtenidos a partir de múltiples orígenes y con diferentes formatos, mediante técnicas analíticas implementadas en sistemas informáticos especializados.

En consecuencia Big Data debe ser administrado, con el mismo rigor que el resto de servicios de la organización, integrándose bajo el paraguas de las estructuras de Gobierno y Gestión de TI.

Para comprender el alcance de esta necesaria integración, podemos aproximarnos a una definición de gobierno y gestión que clarifique los conceptos: mientras que la gestión únicamente pretende mejorar la eficacia y la eficiencia de los servicios, y de los procesos en que éstos se sustentan, el gobierno pretende asegurar unos objetivos, partiendo de unos recursos y en base a la estrategia corporativa acordada, manteniendo el riesgo a un nivel aceptable. Y es en este último concepto de riesgo donde, desde el punto de vista de la protección de datos, debemos prestar especial atención.

El riesgo puede incidir en la privacidad como la probabilidad de que se materialicen las diferentes amenazas que representan un impacto negativo de seguridad en los datos personales, pudiendo comprometerse la confidencialidad, la integridad o la disponibilidad de los mismos. Pero también, desde un punto de vista jurídico, el riesgo puede surgir de la adopción inadecuada o insuficiente del marco normativo y regulatorio o debido a la ausencia, en determinados países, de legislación aplicable sobre protección de datos personales.

En algunas legislaciones Iberoamericanas, las acciones y los avances que permiten identificar un marco regulatorio adecuado para "hacer frente" al Big Data que involucra datos personales, que para su completa comprensión y aplicación podría adoptar un axioma general: "Lo importante no es la cantidad de datos personales tratados, sino que son datos personales".

De esta forma, de la misma forma que es recomendable atender a la realidad económica y organizativa de todos aquellos sujetos que tratan datos personales, y por lo tanto bienvenida la elaboración y difusión de textos como el "Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas", también resulta recomendable (quizás, indispensable) el

análisis de Big Data como servicio de TI y sus implicaciones con la protección de datos personales y la privacidad de las personas.

3. LA SEGURIDAD DE LOS DATOS

Los tres atributos básicos de la seguridad de la información, pueden llegar a verse comprometidos en los tratamientos de Big Data:

En relación a la confidencialidad existe la posibilidad real, a partir de un análisis basado en volúmenes de datos que pudieran llegar a correlacionarse con algún dato identificativo personal, del trazado de perfiles de conducta de los afectados. Precisamente el volumen de datos es una de las características esenciales de Big Data, junto a la aplicación de la analítica adecuada. Es en este punto donde se considera fundamental la determinación, previa a ese tipo de tratamientos, de la finalidad de los mismos. El principio de finalidad, además del de consentimiento, debería ser la estrella polar de la protección de datos referida a Big Data. Otras actitudes, como es el permitir un acceso individualizado o granular a los grandes volúmenes de datos almacenados en los sistemas de Big Data, puede representar elevado riesgo para la privacidad si los datos se almacenan sin la debida anonimización o están insuficientemente protegidos mediante controles de acceso ineficaces.

En cuanto a la integridad de la información, representada en un sentido más amplio por la calidad de los datos, debe considerarse que si el objetivo principal de Big Data es facilitar ayuda para la toma de decisiones, la falta de integridad provocará la obtención de conclusiones erróneas y, en consecuencia, decisiones también erróneas.

Y, por último, sin el atributo de disponibilidad no será posible dar en todo momento el debido cumplimiento al derecho de acceso, considerado como un mecanismo de verificación y control de los propios datos por parte del interesado, amparado por la legislación aplicable en materia de protección de datos. En él se incardinan relacionados todos los demás derechos de rectificación, cancelación y oposición.

Una peculiaridad del derecho de acceso, en entornos de Big Data, no es solo posibilitar el conocimiento de todos los datos personales, en sí mismos, de que dispone una organización relacionados con el interesado. También sería deseable un acceso transparente a los diferentes perfiles que el sistema haya podido construir del propio afectado de forma automatizada y, a ser

posible, una descripción de la lógica de los algoritmos empleados para obtenerlos, conocer para qué han sido obtenidos esos perfiles y, si procede, a quién se han facilitado.

En México, como en otra legislaciones Iberoamericanas, la normativa vigente cuenta con las disposiciones necesarias para obligar a los responsables que tratan datos personales en un entorno de Big Data a la adopción de las medidas de seguridad que garanticen los tres atributos anteriormente identificados.

Bajo un enfoque neutral (y por ello positivo para los objetivos perseguidos) el art. 19 de la LFPDPPP dispone que "todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado". Se establece, además, que "los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."

La generalidad y neutralidad de estas disposiciones, en relación con Big Data, requerirá que cada tratamiento de datos personales sea valorado (e.g. mediante un "Privacy Impact Assesment") para tomar en cuenta, precisamente, el riesgo existente sobre el tratamiento de los datos, las posibles consecuencias del mismo para los titulares, la sensibilidad de los datos tratados y el desarrollo tecnológico que se utiliza para tratar los datos de forma masiva pero con objetivos definidos.

En Peru, la Ley de Proteccion de Datos Personales, Ley N° 29733, define un dato personal a toda información que identifique o pueda volver identificable a un individuo, cuyo Reglamento de la Ley, Decreto Supremo N° 003-2013-JUS, en su articulo 24. Complementa que es toda información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados, definición que comprendería la protección de los datos obtenidos a partir del Big Data dado que estos datos a partir de sistemas de gestión de información pueden elborar un perfil de un individuo.

La ley peruana regula la información que debe ser comunicada cuando el titular de un dato ejerce su derecho de acceso, en cual sea titular del banco de datos personales o responsable del tratamiento la información relativa a sus datos personales debe proporcionar todas las condiciones y generalidades del tratamiento de los mismos. Ademas se recalca que la respuesta debe ser amplia y comprender la totalidad del registro correspondiente al titular de datos personales, aun cuando el requerimiento sólo comprenda un aspecto de dichos datos. Es decir, si existiera la aplicación de una herramienta como el de Big Data se debe poner en concimiento este procedimiento con toda la información correspondiente al tratamiento llevado a cabo por este tipo de análisis de datos personales, que en el caso del Big Data comprendería señalar el método y tipo de análisis de la obtención o generación del dato personal

4. LA CALIDAD DE LOS DATOS

Hay dos formas de abordar la calidad de los datos en entornos de Big Data: Desde un punto de vista jurídico y desde otro más tecnológico. La conjunción de ambos nos garantizará el marco adecuado para confiar en la certeza de los resultados obtenidos a partir de los tratamientos y contribuir a la protección de los derechos fundamentales de los afectados.

La mayoría de normativas de protección de datos disponen que los responsables del tratamiento deberán observar, entre otros, el principio de calidad de los datos. Se cumplirá con este principio cuando los datos personales tratados sean exactos, completos, pertinentes, necesarios, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. El responsable deberá establecer los mecanismos que considere necesarios para preservar esos atributos evitando así que se altere la veracidad de la información. Ya hemos visto que en entornos de Big Data la calidad de los datos es algo sustancial a la vez que, debido a los grandes volúmenes de datos tratados y su variedad, se requerirán mayores esfuerzos para lograrlo.

Vemos que el principio de calidad de los datos debe contemplarse como un binomio indisociable del principio de finalidad, que limita el alcance de los tratamientos a la finalidad concreta, o compatible, para la que éstos fueron recabados y los interesados informados.

Partimos de la presunción de que en todo tratamiento de datos personales existe la expectativa razonable de privacidad, entendida como la confianza que deposita el titular de esos datos, respecto de que los datos personales que ha proporcionado serán tratados conforme a lo que

acordaron las partes. El valor de esa expectativa es lo que, amparado por la legislación aplicable en materia de protección de datos, proporciona confianza y seguridad jurídica. En consecuencia es imprescindible en tratamientos de Big Data un análisis basado en el principio de limitación de finalidad en relación a aquello que se le informó al interesado y éste aceptó y que los datos tratados son los irrescindibles para logar esa finalidad: derecho de información, minimización de datos y principio de consentimiento. Siempre debería informarse al interesado sobre la finalidad con que se recaban sus datos y el posible alcance de los tratamientos posteriores.

El grupo de trabajo consultivo europeo conocido como del Artículo 29 (GT29) ya se ha pronunciado mediante el análisis de diferentes posibilidades en su opinión wp203. Según esa opinión el principio de limitación de la finalidad es una piedra angular de la protección de datos.

No obstante, los datos que ya han sido recogidos pueden ser realmente útiles para otros propósitos, que no han sido previstos inicialmente. Por lo tanto, también hay valor en permitir, dentro de límites cuidadosamente equilibrados, un cierto grado de uso adicional. Así, consideran que el principio de limitación de la finalidad está diseñado para ofrecer un enfoque equilibrado: De una parte tiene como objetivo conciliar la necesidad de la previsibilidad y la seguridad jurídica en relación con los fines del tratamiento que deben ser explícitos, legítimos y determinados y, por otra, la necesidad pragmática de proporcionar flexibilidad sin incurrir en tratamientos incompatibles con dichos fines.

El procesamiento adicional para un propósito diferente no significa necesariamente que sea incompatible, pero la compatibilidad debe evaluarse caso por caso, teniendo en cuenta todas las circunstancias, lo que no siempre será una tarea fácil y dificulta la tutela por parte de las autoridades de control al desplazarse desde el plano basado en el derecho objetivo hacia el plano de lo subjetivo en función de las circunstancias.

A nivel ilustrativo cabe citar el artículo 7.f de la Directiva europea 95/46/CE, que establece dos únicos requisitos acumulativos para legitimar un determinado tratamiento no consentido explícitamente: La necesidad de satisfacer un interés legítimo y que no prevalezcan derechos y libertades fundamentales de los afectados.

También adquiere esencial relevancia en el principio de calidad de los datos el ejercicio de derechos y la posibilidad de revocación de los consentimientos otorgados por los afectados.

Desde un punto de vista más tecnológico, en relación a la calidad de los datos, habitualmente se hacen clasificaciones basándose en diferentes atributos de ellos: Éstos deben ser íntegros en el sentido que los datos, que en Big Data deben conciliarse procedentes de múltiples orígenes y diferentes formatos, continúen siendo completos, precisos y preservados de cambios no autorizados; completos, evitando truncamientos que los desvirtúen durante el almacenamiento y demás tratamientos y permaneciendo vinculados los conjuntos de datos complementarios entre sí; actuales, manteniendo la trazabilidad desde cuando la información fue dada de alta o modificada en el sistema de Big Data y su fecha real o estimada de prescripción; consistentes, que describe la coherencia lógica de la información; la validez de los datos, que obliga a que sean confiables en su origen y acordes a la situación actual que representan; precisos, que consiste en mantener la exactitud de los datos de entrada en los sistemas de Big Data, con independencia de los diferentes orígenes, ya sean humanos, informáticos, sensores, etc.

Como en otras tantas jurisdicciones, México ha adoptado el principio de calidad como parte de aquéllos otros rectores de la protección de datos personales y que, materializado, debe garantizar que los datos tratados sean exactos, completos, pertinentes, correctos y actualizados, según se requiera para el cumplimiento de la finalidad para la cual son tratados por el responsable (art. 36 del RLFPDPPP).

Cabe señalar que la redacción adoptada por la Ley mexicana de protección de datos en relación con este principio abre la puerta a diversas interpretaciones en relación con su cumplimiento. En el entorno Big Data, la necesidad de interpretar lo dispuesto por el artículo 11 de esta Ley se anticipa como inevitable, pues no cabe duda que al disponer este numeral que "el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados", si bien es cierto se atiende a una realidad en relación con la posibilidad material de mantener datos correctos y actualizados de los interesados, también es cierto que se abren posibilidades indefinidas para flexibilizar en determinados escenarios la rigurosidad de esta obligación.

Por lo anterior, es recomendable, como para tantos otros principios, invitar al análisis, estudio y difusión de las particularidades de Big Data y su enorme vinculación con la protección de datos personales y la privacidad de las personas, procurando en todo momento que tanto la generalidad de los principios como la especialidad de los entornos en que estos deben respetarse,

garantice la protección de los bienes jurídicos protegidos por la normativa y la viabilidad de las actividades económicas de los "responsables Big Data".

Lo anterior cobra mayor sentido a la luz de la reciente sentencia emitida por el Tribunal de Justicia de la Unión Europea en el Asunto C-131/12 (ya conocida como la "sentencia del derecho al olvido"), que entre otros varios aspectos se pronuncia sobre el cumplimiento del principio de calidad por parte de los gestores de motores de búsqueda en Internet, concluyendo que dichos gestores son "responsables" del tratamiento de los datos personales que efectúan estos motores de búsqueda y que, por lo tanto, están obligados al cumplimiento de las disposiciones establecidas en la Directiva europea 95/46/CE (entre otras, las relativas a la calidad de los datos que tratan en el ámbito de sus actividades e intereses económicos).

5. BIG DATA Y PRIVACY BY DESIGN (PbD)

Una de las herramientas que se demuestran más útiles a la hora de respetar la privacidad en los tratamientos de Big Data es el Privacy by Design, que podría definirse como abordar la privacidad de forma temprana, especialmente en proyectos complejos como pueden serlo los de Big Data, representando una mayor efectividad a un coste menor. Por eso cabe considerarla desde la fase de diseño (Privacidad por diseño).

El principio de privacidad por diseño fue creado por la Comisaria de Privacidad de Ontario, Canadá, Ann Cavoukian y puede ser aplicado a cualquier tipo de datos. Se fundamenta en 7 principios básicos:

1. Proactivo no reactivo / preventivo no correctivo: la privacidad por diseño se anticipa a los riesgos antes de que se produzcan. Se trata de adoptar medidas que impidan que estos riesgos se materialicen y por tanto, tiene un carácter preventivo, se trata de actuar antes, no después.

2. Privacidad por defecto: cualquier sistema ha de estar configurado de forma que, por defecto otorgue una mayor protección a la privacidad de las personas, de modo que, no se comparta la información del usuario salvo que éste realice una acción o cambie su configuración.

La privacidad por defecto otorga un mayor control sobre la propia información ya que, el usuario está protegido aunque no haga ninguna acción y decide libremente cuándo, cómo y con quién, comparte sus datos.

3. Privacidad integrada en el diseño: la protección de la privacidad ha de estar integrada en el sistema desde el momento en que se diseña, sin que ello disminuya su plena funcionalidad. No se trata de una opción que se añade a posteriori sino que, es uno de sus componentes integrales.

4. Funcionalidad: seguridad y privacidad no han de ser características excluyentes sino que, ambas han de estar garantizadas e integradas en cualquier sistema.

5. Protección durante todo el ciclo de vida de los datos: la protección de la información se ha de configurar desde el momento en que se recaban los datos, durante todo su ciclo de vida hasta que son destruidos, garantizando también que se eliminen de forma segura y confidencial, respetando los periodos de retención establecidos.

6. Transparencia: la entidad que trate los datos ha de estar sujeta a los términos y condiciones informados desde un principio que, no podrán modificarse, sin el previo consentimiento del afectado. También podrá estar sujeto a una verificación independiente.

7. Velar por los intereses del usuario como objetivo: el interés del individuo siempre ha de estar presente en el diseño y configuración de sistemas y aplicaciones por ejemplo, mediante fuertes medidas de seguridad (encriptación, verificación en dos pasos, etc.), información completa y comprensible, opciones "user-friendly", privacidad por defecto.

Ann Cavoukian ha elaborado un nuevo principio basado en aquellas entidades que disponen de grandes y complejos sistemas informáticos que ya están creados y que, por tanto, no han aplicado desde el principio la privacidad por diseño. Se trata de "Privacy by ReDesign" (rediseño) que se basa en las 3 Rs: "Rethink, Redesign and Revive" (repensar, rediseñar y revivir):

- *Rethink: consiste en que las organizaciones reviesen sus estrategias de mitigación de riesgos, procesos y sistemas considerando opciones que, otorguen una mayor protección a la privacidad. Revisar periodos de retención de datos, controles de acceso a los datos, etc.*

- *Redesign: consiste en implementar mejoras en el funcionamiento de los sistemas desde un punto de vista de respeto a la privacidad y permitiendo obtener los mismos objetivos. Por ejemplo, valorar la disminución en el tipo de datos recabados, etc.*

- *Reviving: revivir el sistema en base a un nuevo enfoque más protector de la privacidad.*

Para cumplir con estos cometidos, podemos utilizar diferentes principios y herramientas, que pasamos a analizar a continuación y que creemos que deben presidir cualquier sistema de Privacy by Design.

Los derechos de acceso y rectificación junto con el principio de transparencia son pilares básicos que han de gobernar el Big Data y por tanto, también se han de configurar desde el inicio. Igualmente, siempre se ha de facilitar un derecho de oposición fácil y gratuito, especialmente para la utilización de los datos con fines comerciales y de publicidad.

El principio de transparencia también exige que la información sea facilitada en un lenguaje sencillo y accesible, para todos los sectores de población. Y la utilización de sistemas como la información por capas, permiten al usuario localizar la información que necesita de forma más rápida.

Es importante que, los términos y condiciones de cualquier producto y servicio sean vinculantes para la entidad que los ofrezca, obligando a recabar el consentimiento de los usuarios antes de su modificación.

Conviene tener presente el carácter internacional de muchos de los productos y servicios que se ofrecen en la sociedad de la información y la dificultad jurídica que puede representar determinar las leyes que resultan de aplicación a un determinado producto o servicio. Por ello, el principio de transparencia es de suma importancia, conviene que los productos o servicios que se ofrezcan a los ciudadanos de un país permitan conocer de entrada cuál es su expectativa de privacidad al utilizarlo y cuáles son sus derechos reales. Ello le permitirá al menos, poder discriminar entre diferentes proveedores y escoger con propiedad el que más le convenga.

Con carácter previo puede ser conveniente realizar una evaluación de impacto de la protección de datos (Privacy Impact Assessment. PIA). En esta evaluación de impacto a la privacidad es necesario tener muy en cuenta las finalidades concretas del tratamiento con el fin de determinar si es posible obtener el mismo resultado mediante información anónima.

Además, la finalidad del tratamiento nos ayudará a definir periodos de retención y tipo de datos que sean estrictamente necesarios para el cumplimiento de la finalidad. De este modo, se podrán definir plazos a partir de los cuales la información puede eliminarse y cuando sea posible, se permitirá disociar la información de carácter identificativo.

Este punto es especialmente importante teniendo en cuenta el impacto energético que resulta del actual consumo de datos y de asegurar su permanente accesibilidad. Es necesario poder discriminar entre la información relevante y estrictamente necesaria para el cumplimiento de la finalidad, de la que resulta no adecuada, irrelevante u obsoleta para poder facilitar la eliminación segura de esta última.

Otro punto que será necesario tener en cuenta es el concepto de "dato de carácter personal" ya que, depende del país de que se trate, dicha definición tendrá un carácter más o menos amplio.

Será conveniente determinar qué se consideran "datos sensibles" teniendo en cuenta que, con el Big Data se podrán relacionar diferentes tipos de datos que, si bien en un principio puedan ser considerados de nivel básico, valorados en su conjunto permitan crear perfiles detallados de personas, hábitos y comportamientos que merezca una mayor protección por pertenecer al ámbito íntimo de la persona.

También es importante instaurar mecanismos de control de acceso a la información ya sean por terceros o por los responsables del tratamiento que sean estrictos, especialmente cuando se trate de datos sensibles, partiendo de la regla generalque solo podrian acceder o conocer aquellos que previamente han obtenido el consentimiento del titular del dato personal o que exista una normativa de alto rango como la ley que contemple excepciones en mérito del interés público.

En relación al tratamiento de datos de menores con carácter general, se intentará adoptar medidas que impidan o restrinjan su tratamiento. Cuando sea necesario, ya sea a nivel educativo, de salud o social se procurará que el tratamiento cumpla especiales cautelas, sirva para el cumplimiento de unas finalidades concretas y en beneficio del menor, contando siempre con el consentimiento de sus padres o tutores. Ha de procurarse que, no se produzcan consecuencias negativas para el menor (evaluaciones, notas, ayudas, becas, temas de adopción, custodia, etc.) derivadas de un tratamiento automatizado de datos, siempre ha de existir mecanismos que aseguren un tratamiento y evaluación individualizada, con un trato humano y personal.

En lo que respecta a la relación entre el Big Data y el Internet de las Cosas o la interconexión de datos entre máquinas (M2M) obliga a tener muy presentes la transparencia, la privacidad por diseño y por defecto.

El usuario debe saber cuándo compra determinados productos de este tipo cuáles son sus reales expectativas de privacidad, ha de poder gestionar con facilidad sus preferencias y determinar qué información, para qué finalidad y con quién la quiere compartir. También ha de conocer los periodos de retención de los datos y tener garantizados sus derechos de acceso, rectificación, oposición y cancelación.

En lo que respecta a la utilización de las técnicas de análisis de sentimientos (sentiment analysis) que sirven para analizar los sentimientos de los usuarios para intentar determinar sus preferencias a la hora de comprar un producto u opinar sobre una decisión, al tener una connotación muy invasiva, solamente se deberían poder utilizar con el consentimiento inequívoco del usuario. Evidentemente, deberían de gobernar el resto de principios (transparencia, retención limitada de datos, derechos de acceso, cancelación, etc.).

6. MARCO DEL GOBIERNO DE LOS DATOS

El gobierno de los datos es un "marco de organización que armoniza la estrategia, define objetivos y establece políticas para la información corporativa", el cual engloba la elaboración de un marco normativo al interior de las organizaciones enfocado en la protección y gestión de los datos personales, abarcando por ejemplo la definición de los procesos y políticas internas que reglamenten la gestión de los datos personales.

Una vez definido el modelo de gobierno de datos, será importante el proceso de implementación, capacitación y adaptación, ya que la implementación de dicho modelo no tendrá impacto únicamente en la definición de los procesos y políticas internas, sino que se tendrá que empapar a la organización e incluso en su cultura organizacional.

Es por lo anterior que se habla de generar en las organizaciones una estructura de gobierno de datos que entre otros contemple temas como la calidad, ciclo de vida de los datos, seguridad y cumplimiento legal en materia de protección de datos personales, y más aun tratándose de empresas que están en contacto, procesan o generan información mediante Big Data, ya que por los grandes volúmenes de información que manejan una adecuada gestión de los datos es indispensable.

En alguna de las legislaciones iberoamericanas ya se contempla el que los responsables puedan allegarse de estos modelos de gobierno de datos para el cumplimiento de las obligaciones a su cargo, ya que se establece que el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo adecuado para tales fines.

En lo que respecta a la calidad de los datos, dentro de las organizaciones y como parte de los puntos de control de las políticas y procesos que se establezcan en los modelos de gobierno de datos, se deberán contemplar los riesgos que implican factores como los registros manuales de los datos, errores humanos, flujo de información entre departamentos, errores en procesos o incluso en los mismos sistemas, ello incluso cuando hablemos de entornos controlados donde las cantidades de datos o el flujo de los mismos sea muy poco.

Pero si este tipo de errores los trasladamos a entornos globales de información como lo es el uso de herramientas de Big Data que utilizan como fuente de información los datos generados o circulantes en plataformas Web y dispositivos móviles, los errores se pueden disparar exponencialmente, no sólo por los errores que se pueden dar al interior de la organización sino también por lo complicado que es saber si tales datos son confiables o verídicos.

En pro de que el uso de los datos utilizados mediante Big Data sean lo más confiables posibles, existen algunos modelos que ofrecen técnicas para mejorar la calidad de los datos como por ejemplo, el perfilamiento, estandarización, mapeo, categorización o anonimización de los datos.

Al principio la implementación de estos modelos podría ser vista por las empresas como muy costosa, pero en realidad a la larga se convierte en una ventaja, ya que al utilizar las técnicas de Big Data se busca el que los equipos de marketing o ventas puedan realizar por ejemplo campañas dirigidas a sus clientes de una forma más efectiva, pero si partimos del hecho de que muchos de los datos pueden ser falsos, en realidad los esfuerzos empleados no obtendrán resultados certeros.

Por el contrario, si se emplean las suficientes medidas que permitan eliminar datos inexactos, incompletos o no estandarizados, aunque la muestra sea menor el resultado será más exacto. Es decir, al final lo importante no es tener más y más datos personales sino que los mismos sean de calidad.

El velar por la calidad de los datos personales no sólo es importante para lograr la satisfacción de las preferencias de los clientes, para optimizar la labor de los departamentos de ventas y de mercadotécnica, o incluso para mejorar el procesamiento de los datos en las áreas de tecnologías de la información, sino que también es importante para el cumplimiento de las disposiciones legales aplicables en materia de protección de datos personales.

Siendo por ejemplo el caso de la legislación mexicana en la materia y la Directiva 95/46/CE, que establecen como obligación para los responsables el dar cumplimiento y garantizar el principio de calidad de los datos personales, por medio del cual los datos deberán:

- *Sean exactos, completos, pertinentes, correctos y actualizados.*
- *Si los datos personales son proporcionados por el titular, se presume que se cumple con la calidad en los datos, hasta que se manifieste o acredite lo contrario.*

Estableciéndose además que el responsable adoptará los mecanismos que sean necesarios para cumplir con los dos puntos anteriores, aún y cuando la información no se obtenga directamente del titular.

Es por ello que al ser un problema el que el Big Data no pueda garantizar que los datos sean veraces, que mejor que dentro del modelo de gobierno de datos de las empresas se empleen técnicas que nos ayuden a deputar los datos para quedarnos únicamente con los datos que cumplan con el principio de calidad.

En lo concerniente al ciclo de vida de los datos, en un modelo de gobierno de datos es elemental el considerar el ciclo de vida de los datos o livecycle management, ello sobre todo para las organizaciones que procesan datos mediante plataformas de Big Data, ya que como se ha mencionado, los volúmenes de información que procesan son muy grandes.

Dentro del ciclo de vida de los datos se deben considerar tanto aspectos técnicos como el volumen, velocidad y complejidad, así como aspectos legales que tienen que ver con la creación, almacenamiento, tratamiento, transferencia, remisión, archivado definitivo o destrucción de los datos personales, así como las finalidades del tratamiento de dichos datos.

En algunas legislaciones Iberoamericanas, se establece que los plazos de conservación de los datos personales no deberán exceder de los que sean necesarios para el cumplimiento de las finalidades del tratamiento, ello tomando en cuenta la legislación aplicable en casos especiales como los datos financieros, de salud, contables, fiscales e históricos, los cuales por sus características y particularidades suelen tener plazos de conservación especiales (normas sectoriales).

Cuestión no menos importante es la relativa a la seguridad ya que como se analizó en el apartado de seguridad de los datos, existen diversos riesgos que pueden poner en peligro la seguridad, la confidencialidad, la integridad, la disponibilidad e incluso la privacidad de los datos, es así que la seguridad no sólo debe estar contemplada en las plataformas y elementos de las tecnologías de la información y comunicaciones, ya que agentes diversos como el descuido de una persona o por el mal acondicionamiento y seguridad de las instalaciones, también se pueden poner en riesgo los datos personales.

Es por ello que adicional a las medidas de seguridad técnicas, se deben implementar también las administrativas y las físicas, entre las que destacan:

La capacitación, actualización y concienciación de las personas que intervienen en temas de seguridad y protección de datos al interior de la organización.

Esto se puede realizar mediante programas de capacitación, ya que incluso, al realizar tales capacitaciones de manera periódica se evita el que por cambios o rotación de personal lo impartido quede en el olvido o que las nuevas personas no tengan los conocimientos necesarios.

El empleo de técnicas de anonimización, mediante las cuales se logra que los datos personales no puedan ser asociados con su titular, es decir, después de aplicar una técnica de anonimización deberá ser irreversible el ligar a un dato con su titular.

Se deberá realizar el análisis de riesgos que consiste detectar la diferencia entre las medidas de seguridad existentes y las faltantes que resulten necesarias para la protección de los datos personales.

La importancia de este análisis de riesgos reside en que no sólo se quede en la detección de los elementos ausentes, sino que se realice un plan de trabajo que permita su implementación en la organización, precisamente para subsanar las deficiencias detectadas.

Se deberá contemplar el procedimiento y las acciones a realizar en caso de sufrir vulneraciones o brechas de seguridad, se debería tener en cuenta:

- *Se entiende como vulneración a la seguridad de datos personales la pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizados.*

- *Cuando el responsable detecte vulneraciones de seguridad, informará al titular cuales fueron las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales (Informe sobre Vulneraciones).*

- *El informe sobre vulneraciones se realizará en cuanto se confirme que ocurrió la vulneración y se hayan tomado las acciones para detonar la revisión exhaustiva de la magnitud de la afectación.*

Esto con la finalidad de que los titulares afectados puedan tomar las medidas adecuadas para proteger sus datos e información con ellos relacionada.

El responsable deberá analizar las medidas que correspondan para que la vulneración detectada no vuelva a ocurrir.

En lo referente a la protección de los menores, los datos personales deben recibir una protección y tratamientos especiales. Es así que las empresas pueden establecer lineamientos en donde se estipule si existe o no la necesidad de recopilar datos de menores de edad, los límites o rangos de edad de los menores respecto de los cuales se recopilen datos, así como los productos y servicios a los que tendrán acceso, lo anterior ayudará a su vez a la definición de las finalidades del tratamiento de los datos.

Una vez definidos los casos en los que será procedente la recopilación de datos de menores de edad, se tomarán medidas para:

- *Informar en el aviso de privacidad sobre la recopilación de los datos de los menores y sobre las finalidades de su tratamiento.*

- *Establecer los mecanismos mediante los cuales los padres o tutores otorgarán su consentimiento para el tratamiento de los datos personales de los menores de edad,*

así como para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales, ello también a través de sus padres o tutores. De otorgar el consentimiento el propio menor, al ser por ejemplo español mayor de 14 años, se deberá utilizar un lenguaje adecuado a su edad.

- *Decidir si es indispensable que los datos personales de menores de edad sean tratados mediante las técnicas de Big Data, y en su caso, establecer medidas como la anonimización o depuración de los datos personales, de manera que no se causen afectaciones a los menores y se utilicen únicamente los datos que sean indispensables.*

La obligación de transparencia en estos tratamientos de Big Data conlleva a que entre la información que debería contener el aviso de privacidad, se encuentre el dar conocer las finalidades del tratamiento de los datos personales recopilados, lo que en caso de que se realice el procesamiento de información mediante las técnicas de Big Data, tal finalidad también deberá ser informada al titular.

En el Aviso de Privacidad también se debería informar respecto a las medidas de seguridad físicas, administrativas o técnicas que limiten el uso, acceso o divulgación no autorizada de los datos personales, así como en los casos en los que se realiza el procesamiento de información mediante Big Data se informarán sobre de las técnicas especiales utilizadas, tales la anonimización de los datos.

Es también importante que la información contenida en el aviso de privacidad y sobre toda la referente a las finalidades del tratamiento y medidas de seguridad utilizadas, sea redactada de una forma clara, sencilla y que se enfoque al tipo, grupo o sector al que van dirigidos los productos o servicios, en caso la explicación comprenda inevitablemente algún nombre técnico también se deberá dar una breve explicación de este, elemento que podría ser problable dada las aplicaciones tecnológicas de la herramientas de Big Data.

En lo que respecta a los derechos de acceso, rectificación, cancelación y oposición (ARCO), el análisis sobre el ejercicio de los derechos, se puede realizar en dos partes: respecto de los datos personales obtenidos de fuentes de Internet en las cuales cualquier persona tiene acceso, y respecto de los datos obtenidos directamente de su titular, o cuando se obtienen de manera indirecta pero que es posible localizar al titular:

- *Sobre en plataformas o sistemas de Big Data alimentadas por datos personales obtenidos de fuentes de Internet accesibles al público, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, es realmente complicado y desproporcionado al ser casi imposible saber cuántos responsables de tratamiento los han utilizado.*

- *Respecto de los datos obtenidos directamente de su titular, o de manera indirecta pero cuando es posible localizar al titular, desde el aviso de privacidad se deberá dar a conocer al titular de los datos que los mismos serán tratados para el procesamiento de información mediante Big Data, dando oportunidad al titular para otorgar o no su consentimiento.*

Una vez obtenido el consentimiento para el tratamiento de los datos mediante Big Data, se deberá establecer el procedimiento y medidas necesarias al interior de la organización para garantizar la atención de los derechos de acceso, rectificación, cancelación y oposición, ello cuando exista la posibilidad de identificar al titular. Ya que respecto a datos estadísticos o datos cuya disociación se haya realizado de manera previa y plena, no hay posibilidad de identificar a sus titulares.

Para finalizar indicaremos que en base al principio de accountability, al igual que el resto de las empresas, personas u organizaciones que recopilan, tiene acceso o tratan datos personales, quieres recopilen o procesen información mediante Big Data están obligados al cumplimiento con las obligaciones que conforme a la legislación les sean aplicables, debiendo justificar su actuación conforme a la legalidad vigente y respondiendo en caso de incumplimiento.

7. BIG DATA Y CLOUD COMPUTING

Cuando las empresas no pueden costearse la infraestructura física necesaria para analizar grandes volúmenes de datos desestructurados, recurren al sistema conocido como Cloud Computing.

Muchos proveedores de almacenamiento de datos se erigen en Cloud Services Provider (CSP) directamente o mediante acuerdos y ofrecen soluciones basadas en Cloud Computing como parte de su actividad de negocio (catálogo de servicios además del catálogo de productos) y las comercializan entre los clientes como soluciones mas asequibles y accesibles.

En esencia, las empresas cliente alquilan espacio de almacenamiento y potencia de proceso en servidores virtuales, a los que pueden acceder en línea. Estos servidores están equipados con sofisticadas aplicaciones que han sido diseñadas especialmente para manejar y analizar grandes volúmenes de datos.

La ventaja para los clientes es que pueden conseguir resultados rápidamente a un coste razonable. Además pueden acceder al asesoramiento y soporte del proveedor como apoyo al diseño y a la ejecución de los proyectos.

Desde el punto de vista de la protección de la privacidad, lo primero que tenemos que tener en cuenta a la hora de contratar una herramienta de estas características es que se va a producir un acceso a datos y por ello, se deben reflejar en el contrato que nos ofrece el proveedor las estipulaciones sobre el acceso a datos reguladas en las diferentes legislaciones nacionales que se han tomado en serio esta materia.

Es por ello que antes de contratarla, se nos debe facilitar información transparente que posteriormente debe quedar plasmada en el contrato sobre los usos, finalidades y alcance del acceso a datos, la implantación de medidas de seguridad, la devolución o destrucción de los datos cuando finalice el servicio, las subcontratas previstas y, en el caso de no conocerse en ese momento, la manera de solicitar autorización previa al responsable del tratamiento.

Otro aspecto vital del Cloud Computing es la ubicación del servidor, (o alguna de sus copias de seguridad) puesto que según en qué lugar del mundo esté ubicado nuestro servidor virtual en el Cloud Computing, cuando introduzcamos datos personales en él, podrá considerarse una simple cesión (que puede resolverse mediante la suscripción del preceptivo contrato entre responsable y encargado del tratamiento) o bien una Transferencia Internacional de Datos (TID) que conlleva obligaciones legales adicionales en los países que cuentan con legislación en protección de datos.

El tercer aspecto a considerar en los servicios de Cloud Computing es la necesidad de garantizar la disponibilidad, la integridad y la seguridad de la información. Adquieren especial relevancia en este tipo de tratamientos, aunque por el nivel de seguridad no se esté obligado a implantarlas, la posibilidad de permitirnos la realización de backups o copias de seguridad externas a la aplicación, la posibilidad de configurar perfiles de usuarios que delimiten los recursos a los que se puede acceder y con qué privilegios de acceso, la gestión de una política de renovación periódica de

contraseñas y que estas sean robustas (incluyendo mayúsculas, minúsculas, números y símbolos especiales), la aplicación de mecanismos de cifrado sobre todo si estas herramientas utilizan la funcionalidad del Cloud Computing o si se realizan continuas importaciones o exportaciones de datos, la de poseer un registro de incidencias en la que se puedan consignar aquellas que afectan a la seguridad o a la integridad de los datos y la de tener activado el registro de accesos al sistema con revisión periódica del mismo.

También son más que recomendables para estos tratamientos masivos de datos la limitación y registro de las importaciones y exportaciones de datos desde o hacia la herramienta al personal debidamente autorizado y la monitorización de esas actividades, ya que en caso contrario sería recomendable la eliminación o capado de sitios Web de correo electrónico o Cloud Computing, de grabadoras de CD-DVD o puertos USB y la instalación de herramientas de monitorización de equipos y correos electrónicos a los usuarios de estas herramientas.

En el dictamen 05/2012, de 1 de Julio de 2012 sobre la computación en nube, el Grupo de Trabajo del Artículo 29 (GT29) analiza todas las cuestiones pertinentes en materia de Proveedores de Servicios de Cloud Computing (CSPs) que operan en el Espacio Económico Europeo (EEE) y sus clientes, especificando todos los principios aplicables de la Directiva europea sobre protección de datos (95/46/CE) y de la Directiva sobre privacidad 2002/58/CE (modificada por la Directiva 2009/136/CE), según proceda.

El GT29 advierte que a pesar de las claras ventajas de la computación en nube, tanto en términos económicos como sociales, el despliegue a gran escala de los servicios de computación en nube puede provocar diversos riesgos para la protección de datos, principalmente la falta de control sobre los datos personales, así como la insuficiente información en relación a cómo, dónde y por quién son los datos tratados o subtratados.

Los organismos públicos y las empresas privadas deben evaluar estos riesgos cuidadosamente al contratar los servicios de un CSP.

En el Dictamen examina cuestiones relacionadas con:

- *La puesta en común de recursos con otras partes.*

- *La falta de transparencia de una cadena de externalización compuesta por múltiples encargados del tratamiento y subcontratistas.*

- *La inexistencia de un marco común general de portabilidad de datos.*

- *La incertidumbre con respecto a la admisibilidad de la transferencia de datos personales a los proveedores establecidos fuera del EEE.*

Del mismo modo se aborda en el dictamen, como cuestión preocupante, la falta de transparencia en cuanto a la información que un responsable del tratamiento puede proporcionar a los interesados sobre la manera en que se tratan sus datos personales. Los interesados deben ser informados de quién trata sus datos y para qué fines, a fin de poder ejercer los derechos que tienen a este respecto.

Una de las principales conclusiones es que las empresas y las Administraciones Públicas que deseen utilizar la computación en nube deben efectuar, como un primer paso, un análisis de riesgos completo y riguroso.

Los proveedores en el EEE deben proporcionar al cliente toda la información necesaria para evaluar adecuadamente los pros y los contras de la adopción de tal servicio.

Los principales impulsores de la oferta de servicios de computación en nube para los clientes deberán ser:

- *La seguridad*

- *La transparencia*

- *La seguridad jurídica*

Por lo que respecta a las recomendaciones contenidas en el dictamen, se subrayan las responsabilidades de un cliente de servicios de computación en nube como responsable del tratamiento y se recomienda, por tanto, que el cliente seleccione un proveedor de servicios de computación en nube que garantice el cumplimiento de la legislación de la UE sobre protección de datos.

El dictamen aborda las salvaguardias contractuales apropiadas estableciendo la condición de que todo contrato entre el cliente y el proveedor deberá ofrecer garantías suficientes en términos de medidas técnicas y organizativas. También es importante la recomendación de que el cliente de servicios computación en nube deberá verificar si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos.

8. OTROS ASPECTOS A CONSIDERAR

Las incertidumbres sobre los potenciales impactos negativos que pueda generar el tratamiento masivo de información aconsejan adoptar posturas garantistas, especialmente en relación al derecho a la protección de los datos de carácter personal, la privacidad o la intimidad, pero también respecto de la salvaguarda de otros derechos y libertades, tanto individuales como colectivos, que pudieran verse afectados por el conjunto de actividades que se ocultan bajo el concepto Big Data.

Todo y que el punto de partida sea de una cierta desconfianza y recelo, a priori generada por los propios agentes relacionados con el Big Data, en base a la opacidad con la que llevan a cabo sus actividades, sin duda pueden encontrarse puntos de encuentro entre:

- *Las necesidades, ya sean públicas o privadas, del tratamiento masivo de la información y*
- *Las condiciones y límites que necesariamente deben imponerse a ese tipo de tratamientos y a los usos posteriores.*

A título de ejemplo como comentamos anteriormente, el estudio "Big Data: aprovechar las oportunidades, preservando los valores", publicado el 1 de mayo de 2014, por la Casa Blanca, elaborado a petición del presidente Obama, que encargó a sus asesores que elaboraran un informe que dictaminara sobre la manera en que el Big Data podía afectar a la vida las personas, ponen de relieve la preocupación que el Big Data suscita en los poderes públicos; estos deben tomar partido, y adoptar políticas adecuadas para minimizar los riesgos que puedan derivarse del tratamiento masivo de información.

No hay duda de los potenciales beneficios que para la sociedad en su conjunto pueden derivarse del Big Data, entre ellos su aportación al crecimiento y desarrollo económico, pero hay que

estar alertas respecto de los nuevos retos y riesgos que el Big Data puede suponer tanto para la privacidad, como para otros derechos y libertades individuales y colectivos.

En ese sentido, las políticas públicas y las tecnologías, juegan un papel importante en la protección de los derechos y libertades que puedan verse afectados por el tratamiento masivo de información y, especialmente, respecto del uso que se pueda hacer del resultado del procesamiento de esa información.

Las actividades relacionadas con el Big Data no siempre implican el tratamiento de datos de carácter personal, por tanto no siempre se va a dar la componente de impacto sobre la autodeterminación informativa, ahora bien, no debemos perder de vista que la información relacionada con las personas, una vez tratada, es la que puede llegar a aportar más valor a los procesos de negocio, a la investigación científica, o a las necesidades de inteligencia de los estados en tanto garantes de la seguridad pública o para la definición y aplicación de políticas públicas.

Los datos personales pueden estar presentes de dos maneras, una de tipo indirecto, cuando en origen los datos eran de carácter personal, y han sido sometidos a tratamientos de disociación -aparentemente dejan de ser datos personales, pero existe el riesgo de re-identificación-, y por tanto, a priori, los resultados de su tratamiento no aplican a personas concretas identificadas o identificables, o bien de manera directa, cuando el tratamiento Big Data se lleva a cabo directamente sobre datos personales.

Por tanto podemos afirmar que si bien hay situaciones en que Big Data y privacidad van en paralelo, no es menos cierto que pueden existir abundantes casuísticas en que se crucen, por tanto en que aparezcan puntos de contacto o fricción que hay que gestionar convenientemente.

Desde el punto de vista del uso social de la tecnología, en un primer momento esta suele provocar en las personas un estado de cierta "fascinación", de ahí su rápida adopción, que suele al poco tiempo llevar a una fase de "deslumbramiento", en el que se producen efectos hasta cierto punto contradictorios, por un lado lo último siempre es lo mejor, de manera que las tecnologías emergentes son rápidamente adoptadas, pero a la vez se impone el "discurso tecnológico dominante" que gana adeptos de manera continuada, solo por el hecho de ser dominante, sin que como individuos entremos en otras consideraciones o reflexiones respecto de la utilidad o conveniencia de su uso.

Del "deslumbramiento" se pasa a la siguiente etapa, de la más absoluta "ceguera digital", y es en ese estado en el que emergen los riesgos. ¿Aceptamos una sociedad con un conocimiento filtrado y mediatizado? En definitiva sociedades controladas. ¿Estamos dispuestos a que ciertas las tecnologías limiten el libre desarrollo de la personalidad? ¿Sólo vamos a atender a los riesgos individuales, dejando de lado a los riesgos colectivos derivados del Big Data?

El uso de Big Data para llevar a cabo predicciones es más que conocido, pero tal vez el futuro nos depara otros usos, por ejemplo el de la inducción o modificación de comportamientos; o acabemos en un escenario donde impere el determinismo del dato, en el que solo el "análisis mecánico" de los datos vaya a mover las decisiones, llevándonos a un "estado totalitario del dato", en el que decisiones transcendentales que afecten a las personas, de manera colectiva o individual, se vayan a tomar exclusivamente en base al análisis de datos, lo que puede llevar a la aparición de nuevos modos de discriminación en base a esos análisis de información masivos.

Tal vez como rechazo a esos riesgos empecemos a hablar en un futuro no muy lejano de "la objeción de conciencia digital", es decir, tener la capacidad de oponernos a que nuestros datos sean utilizados, incluso aunque sea de manera anonimizada, pero eso sí, sin renunciar a los beneficios de las tecnologías.

Conviene plantearse la necesidad de regular esas actividades, y ante el escenario descrito pueden adoptarse diferentes posturas desde la perspectiva regulatoria:

- *Optar por la postura de que en tanto exista tratamiento de datos personales se aplica la regulación vigente, y cuando no hay dato personal se deja de aplicar, con lo cual nos encontramos en una situación de desregulación del Big Data, con la inseguridad jurídica que ello puede generar para todas las partes, de hecho este es el estado actual de la cuestión.*

- *O si bien hay que ampliar el alcance de la regulación de los datos personales a situaciones en que ya no hay datos personales, lo que supondría una excepción más que relevante por lo que respecta al ámbito de aplicación material de la regulación del derecho a la protección de los datos de carácter personal y*

- *Si tal vez debe de ser una actividad regulada de manera específica, a la que apliquen unos límites, garantías y condiciones propios, en virtud de los riesgos colectivos que puede implicar.*

Lo "peligroso" no es el Big Data en sí mismo, si no dejarlo exclusivamente en manos del mercado y sin ninguna regulación. Una regulación que debería desarrollarse en base a unos principios claros, tales como:

- *El "principio de inocuidad", por el que los usos del Big Data bajo ninguna circunstancia deben perjudicar ni a los individuos, ni a la humanidad" y que, en todo caso, las excepciones a este principio deben ser establecidas por los legisladores desde una perspectiva restrictiva y garantista.*

- *El "principio de objeción", por el que las personas puedan oponerse, de manera previa o a posteriori, a que su datos sean tratados, incluso de forma anonimizada, y sin que ello les impida usar las tecnologías.*

- *El "principio de seguridad", las actividades de Big Data deben estar especialmente protegidas, a fin de evitar incidentes accidentales o malintencionados que pongan en riesgo a la información.*

- *El "principio de respeto al libre desarrollo de la personalidad", deben prohibirse usos del Big Data que impliquen la modificación de comportamientos y el determinismo del dato.*

- *El "principio de responsabilidad", por el que en todo momento debe poder atribuirse una determinada actividad de Big Data a una persona física o jurídica y, en su caso, exigirle responsabilidades.*

- *El "principio de transparencia", por el que deben articularse mecanismos que permitan que las personas afectadas sean conocedoras del uso que se hace de sus datos.*

9. ESPECIALIDADES DE BIG DATA

9.1 OPEN DATA, SMART CITIES Y ADMINISTRACIONES PÚBLICAS

Si Big Data se define por su tamaño y el Open Data por su utilidad. Open data es el concepto utilizado para los datos abiertos y accesibles al público, compañías y organizaciones que los pueden utilizar para lanzar nuevos productos o servicios, analizar patrones, tomar decisiones, etc.

La estrategia Open Data nació el año 2009 en Washington y se refiere a la posibilidad de que, el ciudadano acceda a los datos del gobierno que, antes sólo eran analizados en el interior de las administraciones públicas. Actualmente el concepto se ha extendido a los países europeos a través de la Agenda Digital Europea y también a algunos países Iberoamérica como Argentina, Chile, Colombia y Perú.

En el modelo Open Data los datos deben ser accesibles a cualquier persona y se han de facilitar de modo que, permitan su utilización con fines comerciales o no comerciales. Estos datos han de ser accesibles de forma gratuita o a un coste mínimo. Y esto es así porque entienden que en nuestra sociedad de redes y bajo el gobierno de la información, el derecho a acceder a la información pública se erige como un derecho humano fundamental, en virtud del cual las personas pueden tomar conocimiento de la información que elaboran o poseen los órganos del Estado. Se basa esto, y lo reafirma a la vez, en el aporte relevante que puede generar esta información al conocimiento, expresión, reflexión y debate público de las ideas.

De ahí que, la información que se públique no debe ser definitiva, en virtud de que puede contener diversos estudios, informes, etc., que han servido como base para la prestación de un servicio por parte de la entidad pública. De esta forma, la imagen de la administración publica de cara a la sociedad serà percibida de manera distinta y no como un ente cerrado y opaco.

Open Data no sólo se ha de referir a los datos de los gobiernos, también podría abrirse por parte de empresas de transporte, bibliotecas, universidades, museos, arte y cultura, consumo energético, geología, astronomía, temas de educación, etc. y se han de facilitar en un formato electrónico normalizado.

El uso avanzado de información de la administración se ha de construir sobre una base que permita, no sólo mejorar la transparencia, eficiencia y eficacia de las Administraciones Públicas sino también, garantizar los derechos y garantías jurídicas de los ciudadanos. Producto de la ejecución de una política pública previamente diseñada, las legislaciones deben contener disposiciones para garantizar fortalecer e incentivar la transparencia y publicidad de la información pública que

permitan erradicar las asimetrías de información entre el Estado y los ciudadanos existentes bajo la cultura de la opacidad.

Por este motivo, es importante revisar y adaptar la normativa jurídica vigente, teniendo en cuenta las características específicas de cada materia o archivo (datos históricos, datos de salud, antecedentes penales, etc.) y redefinir las relaciones con los ciudadanos y empresas y sus derechos.

Hay que tener en cuenta que, aunque la información relativa a una persona identificada o identificable esté a disposición del público, debe seguir estando protegida por la legislación sobre protección de datos, garantizando los derechos, libertades y dignidad de las personas interesadas.

A la hora de determinar en cada caso, si la información se facilita, la entidad pública deberá:

- *No incluir datos personales, por ejemplo, facilitando datos estadísticos, lo cual excluiría limitaciones referentes a la normativa de protección de datos como la necesidad de consentimiento, finalidad determinada, proporcionalidad, etc.*

- *Anonimizar, en este caso, se deberá garantizar que se han empleado las técnicas y evaluaciones necesarias para evitar que estos datos puedan ser reidentificados. Se deberá evaluar y realizar pruebas sobre el riesgo de reidentificación reidentificaicón. Si el resultado de estas valoraciones no es positivo, la Autoridad competente debería establecer limitaciones, de acuerdo con el apartado siguiente o bloquear su publicación.*

- *En el supuesto de incluir datos personales, las garantías de protección de datos e intimidad de las personas resultan plenamente aplicables y por tanto se requerirá:*

O que la publicación de estos datos sea compatible con las finalidades determinadas en el momento de su recogida (evitar finalidades incompatibles, por ejemplo mensajes comerciales no solicitados, etc.).

O deberá existir una base jurídica sólida para la publicación (basada en el consentimiento del afectado o en el complimiento de una ley claramente definida con un objetivo legítimo).

O la divulgación de estos datos ha de ser siempre necesaria y proporcionada al objetivo legítimo perseguido por la normativa.

O establecer condiciones específicas y salvaguardas para su utilización.

La Administración deberá aplicar un criterio de prudencia antes de decidir cómo publicará la información ya que, una vez los datos se han puesto a disposición del público y son accesibles a través de internet, es muy difícil limitar su uso y garantizar el cumplimiento de las normas sobre protección de datos.

También convendrá revisar las normativas sectoriales y específicas, con el fin de evitar resultados incompatibilidades o contradicciones. Por ejemplo que, al relacionar datos publicados por la administración, con otros datos accesibles a través de internet, pueda resultar en finalidades incompatibles.

La limitación de la finalidad ha de estar siempre presente en el modelo de Open Data, para garantizar un tratamiento compatible con la recogida inicial.

Para la evaluación del tratamiento ulterior de los datos se tendrá en consideración:

- *La relación entre los fines para los que se recogieron los datos personales inicialmente y los fines de su tratamiento ulterior*
- *El contexto en el que se recogieron estos datos y expectativas razonables de los interesados de su posterior uso*
- *Naturaleza de los datos personales e impacto del tratamiento ulterior en los interesados*
- *Medidas de salvaguardia para garantizar un tratamiento leal y evitar repercusiones indebidas al interesado.*

Deberá aplicarse un principio de proporcionalidad y de minimización de datos, solo publicar los datos estrictamente necesarios para cumplir con una finalidad concreta y determinada.

También se deberá de tener en cuenta como se accede a estos datos y garantizar que los datos personales de los afectados quedan protegidos incluso si se trasladan a otros estados o países. Para ello deberán establecerse garantías adecuadas.

En lo que respecta a la conveniencia de realizar de manera previa una evaluación e impacto de la protección de datos, antes de que la administración pública decida abrir determinados archivos o información al público en base al concepto de Open Data podría entenderse como una buena práctica, ya que serviría para:

- *Evaluar los riesgos derivados de la apertura de esta información e impacto en la intimidad de los afectados, especialmente teniendo en cuenta que, la información incluso si se publica de forma anónima, puede llegar a identificar a una persona si se relaciona con otra información pública o disponible en internet.*

- *Aplicar los principios de privacidad por diseño y por defecto.*

- *Determinar en qué condiciones y garantías se puede permitir su utilización. Valorar el establecimiento de una licencia de uso que determine limitaciones en la utilización, así como responsabilidades y sanciones en caso de incumplimiento.*

- *Fijar una base jurídica para su divulgación que establezca finalidades determinadas y actuaciones prohibidas.*

- *Aplicación de los principios básicos de protección de datos: limitación de la finalidad, proporcionalidad, calidad, minimización de datos.*

- *Escuchar a todas las partes interesadas y tenerlas en consideración, para poder equilibrar los riesgos en juego, antes de decidir la publicación de estos datos (autoridad pública titular de los datos, entidades privadas que interesa acceder a dichos datos y representantes del colectivo de personas afectadas).*

- *Contar con el soporte y consejo de las autoridades de protección de datos.*

También es importante que, se fomente la cooperación entre diferentes organizaciones públicas con el fin de que se compartan buenas prácticas y códigos de conducta relativos a la apertura de datos entre las diferentes entidades públicas, a nivel estatal, provincial o local.

En lo que respecta al uso de tecnologías de Big Data por parte de las Administraciones Públicas, al poderse procesar no sólo información obrante en varias Administraciones Públicas, otras empresas o terceros sino también, información disponible en Internet (por ejemplo, redes sociales,

blogs, foros, webs...), estos tratamientos pueden tener una especial relevancia en las actuaciones inspectoras de la administración, actuaciones policiales, en el control de subvenciones, prestaciones por bajas médicas, subsidios de desempleo, etc.

En un contexto internacional, países como Estados Unidos, han declarado la utilización del Big Data en la administración pública como una prioridad gubernamental, particularmente por la reducción de costo y tiempo que implica el procesamiento de la información. Esto, a través de diversas iniciativas: DoD USA (2011), D2D Data to Decission y la Iniciativa Big Data de la Casa Blanca (2012).

La Comisión Económica de las Naciones Unidas para Europa (UNECE) también ha incluido el aprovechamiento estadístico de los Big Data entre sus temas de interés estratégico para este año.

Actualmente algunas Instituciones y Administraciones Iberoamericanas han declarado que utilizará los beneficios del Big Data para la obtención de indicadores que permitirán tomar decisiones de política pública, y es justo en este punto en donde se centra el desarrollo de la presente opinión.

El Big Data utilizado por las administraciones públicas será suministrado de información, particularmente sensible: datos de todos los ciudadanos, que concentrado en una sola plataforma de información, resulta peligroso, particularmente en relación a la privacidad y la protección de datos personales de los ciudadanos.

Por todo ello, el uso del Big Data en el ámbito de la administración ha de configurarse sobre un principio de transparencia más elevado pues mucha información que se obtenga podrá provenir de terceros o sin el conocimiento del afectado.

En el tratamiento de esta información es importante tener presentes los derechos básicos del ciudadano en materia de protección de datos basados en el consentimiento para el tratamiento de datos, el principio de finalidad y en los derechos de acceso, rectificación, cancelación u oposición. Y todo ello, sin olvidar un derecho de indemnización a favor del afectado en caso de que, la actuación de la administración haya vulnerado dichos principios y con ello haya causado daños y perjuicios que deban ser reparados.

Debe recordarse que, en general las legislaciones de protección de datos excepcionan para las administraciones públicas el consentimiento para el tratamiento de los datos personales cuando desarrollan sus funciones en el ejercicio de las funciones que les son propias.

El derecho de los ciudadanos a resarcirse de los daños y perjuicios causados por un defectuoso tratamiento o vulneración de los procedimientos y garantías básicas por parte de la administración, puede ayudar a conseguir un mejor equilibrio y funcionamiento del sistema, en el sentido de que, la administración no se verá tentada a tratar información de forma indiscriminada y a basar sus decisiones estrictamente en un tratamiento automatizado. No obstante, para su efectividad es necesario que el acceso de los ciudadanos a este resarcimiento no se vea desnaturalizado por procedimientos demasiado burocráticos y costosos.

Si la administración pública desea adoptar decisiones basadas en información que no ha sido facilitada por el propio usuario hay que preguntarse donde se sitúan los límites ya que, esta información podría traer graves consecuencias contra el usuario (por ejemplo, inicio de una actuación inspectora) y estas consecuencias podría tener su origen en información falsa, incorrecta u obsoleta.

En este sentido, se podría valorar un sistema que estableciera una serie de garantías, tales como:

- *Limitación en las finalidades, esta información solamente se puede utilizar por determinados sujetos y para finalidades concretas "numerus clausus".*

- *En relación a datos de salud (o datos sensibles en general) exigir la adopción de medidas más estrictas, consentimiento reforzado y relevancia para su tratamiento.*

- *Calidad en los datos (completos, actualizados y exactos), no se pueden recabar datos de forma indiscriminada sino, los que son relevantes para la concreta finalidad que han de cumplir.*

- *Un importante derecho de acceso y rectificación, incluyendo un procedimiento para permitir al usuario poner en duda la información de que dispone la entidad cuando no es correcta, y permitir rectificarla. Todo ello, con carácter previo a que se pueda utilizar esta información para evaluar al sujeto. Igualmente, el afectado ha de disponer de un derecho de acceso a obtener esta información siempre que lo interese, de forma fácil y accesible. Este derecho de acceso debería permitir conocer*

el origen de la información para facilitar un mejor control sobre los propios datos. En el caso de las administraciones públicas el derecho de acceso debería facilitarse de forma gratuita.

- *Igualmente las administraciones deberían hacer accesibles los criterios en base a los cuales adoptan decisiones basadas en esta información.*

- *Transparencia y "accountability": la actuación de las administraciones públicas deberá estar gobernada por un principio de transparencia y sujetas a una obligación de responsabilidad de sus actuaciones y debiendo rendir cuentas frente los ciudadanos.*

El respeto a los derechos de privacidad e intimidad de las personas, a la libertad de expresión y el derecho a la legítima defensa no deben verse mermados por la utilización del Big Data en la administración pública puesto que, su finalidad es servir a sus ciudadanos, regular y mejorar el buen funcionamiento de la sociedad, no convertirse en un estado policial o en un Big Brother.

En lo que respecta al uso del Big Data y su contribución al desarrollo de "Smart Cities" ciudades inteligentes, basadas en un modelo de sostenibilidad y eficiencia respondiendo a las necesidades básicas de sus habitantes, instituciones y empresas:

- *Contribuyendo a una gestión más eficiente y sostenible de los recursos naturales. Creando patrones de consumo que permitan mejorar la planificación y utilización de las energías alternativas, promoviendo la sostenibilidad y el ahorro. Por ejemplo, con una gestión eficiente del alumbrado público, sólo en las horas que no hay luz natural.*

- *Fomentando la participación ciudadana para conocer sus necesidades y mejorar los servicios. También para permitir valorar los servicios o denunciar situaciones de forma fácil y ágil, a través de Internet o mediante aplicaciones móviles y de este modo, poder obtener una solución más rápida y eficaz a través de la demominada Administración electrónica.*

- *Contribuyendo en una planificación más eficaz del transporte público a partir de múltiples sensores ubicados estratégicamente y de dispositivos móviles de los*

ciudadanos, para por ejemplo mejorar la gestión de aparcamientos, evitar retenciones o mejorar la circulación.

- *Mejorando y optimizar las redes de telecomunicaciones garantizando su continuidad y calidad.*

- *Utilizando de sensores en los trenes para detectar actividad sísmica y en caso de advertir una actividad inusual, enviar una mensaje para desactivar los trenes. Este sistema ya se está utilizando en los trenes de alta velocidad de Japón.*

- *Mejorando la calidad de vida y medio ambiente a mediante sensores de polución (mejorar la calidad del aire con reducción de emisiones de CO_2, del agua, ruido, residuos, espacios públicos, etc.).*

- *Mejorando la eficiencia energética en edificios públicos y privados (organizaciones públicas, universidades, escuelas, etc.).*

- *Optimizando los recursos destinados a la salud pública: Muchos seguimientos de pacientes podrían realizarse sin que éste acudiera físicamente al centro médico, ayudando de este modo a descongestionar las consultas.*

- *Gestionando eficiente de residuos y reducción de emisiones, contaminantes, etc.*

- *Desarrollando redes inteligentes (Smart grid) que permitan el control del consumo energético, lectura de datos en tiempo real (mediante "Smart meters" o medidores inteligentes), facturación automática y facilitar acceso a los ciudadanos de aquella información que pueda servir para el ahorro, eficiencia y mejora (facilitando el acceso al ciudadano sobre los datos de su consumo energético, permitiendo que los pueda gestionar, visualizar por internet, ver estadísticas sobre su consumo y solicitar cambios de consumos y tarifas; reduciendo el tiempo de solución de averías y reclamaciones).*

La información, tal como se ha indicado, no solamente ha de ser accesible y gestionada por las administraciones públicas sino que, es importante mejorar y fortalecer el concepto de "open government" ya que, de otro modo se produciría un desequilibrio pues, muchos de estos datos

provienen justamente de los mismos ciudadanos. Por ello el uso de estos dispositivos debe adecuarse a las medidas garantistas mencionadas con anterioridad.

9.2 BIG DATA Y SANIDAD

El aprovechamiento de los grandes volúmenes de información que se recaban en las instituciones de salud como resultado de la consulta, tratamiento y hospitalización de pacientes para la atención de enfermedades y padecimientos, bajo un esquema de análisis y disociación adecuado, constituye un material que permita asegurar la mejora constante de los servicios de salud.

La incorporación de una estrategia de Big Data para administrar los grandes volúmenes de datos estructurados y no estructurados, combinado con la posibilidad de aplicar algoritmos que permitan correlacionar datos provenientes de diferentes fuentes para apoyar la investigación y desarrollo de respuestas que favorezcan un mayor acceso a los servicios de salud, es una de las alternativas que las tecnologías de la información ofrecen para fortalecer la investigación científica en materia de salud.

Los avances en la investigación científica relacionada con la salud y bienestar humano ofrecen la posibilidad de contar con nuevos esquemas de tratamiento para atender enfermedades y mitigar sus efectos, esta innovación se fundamenta en gran medida por la capacidad tecnológica disponible para comprender la biología de la enfermedad, que además permita el desarrollo de nuevos medicamentos, diagnósticos y servicios preventivos de sanidad.

Esta visión contrasta con los métodos tradicionales utilizados por las compañías farmacéuticas, que pueden implicar plazos de hasta 10 años para desarrollar e introducir un nuevo producto al mercado.

El esquema considerado para disminuir el proceso de desarrollo e introducción de productos incluye compartir esfuerzos mediante esquemas de alianzas con otras empresas farmacéuticas o con las instituciones de salud administradas por los Estados, para la consolidación de un sistema de sanidad más eficiente que permita trasladar los resultados de la investigación científica en aplicaciones de salud, resultado de compartir recursos y conocimientos entre los participantes.

En este contexto se identifica que un recurso valioso para apoyar la investigación científica está referido con la posibilidad de aprovechar la información que se recaba de los pacientes

atendidos en el sector salud como parte de una estrategia para obtener conocimiento útil en la detección de enfermedades y su curación.

Las características de la información de salud existentes en los sistemas de información y las condiciones en que se busca su aprovechamiento posicionan a Big Data como una estrategia tecnológica adecuada para los fines de investigación científica, pues satisface las condiciones de las cinco V:

- *Volumen. Sin duda los datos de salud son un buen ejemplo de cantidad incremental de información, tanto estructurada como no estructurada, y que además se produce por la intervención humana y por el uso de diferentes dispositivos que la recolectan.*

- *Velocidad. Como se ha expuesto, el aprovechamiento de la información contenida en los sistemas de salud es una alternativa para disminuir el tiempo dedicado a la investigación y desarrollo de nuevos productos que mitiguen o alivien las enfermedades.*

- *Variedad. La información de salud tiene además la particularidad de recabarse en diferentes procesos y formatos.*

- *Verificación. Por el impacto potencial que representa a la salud general esta cualidad es crítica en su aplicación para fines científicos de sanidad.*

- *Valor. El resultado esperado de la aplicación de una estrategia de Big Data es la contribución general al bienestar poblacional en materia de salud.*

Si bien las consideraciones anteriores abonan en favor de la aplicación del Big Data, no debe omitirse que la titularidad de los datos contenidos en los sistemas de información de salud pertenece a los pacientes y está sujeta a los principios reconocidos para su tratamiento, incluyendo la condición de excepción de su aprovechamiento por el Estado aduciendo situaciones de salud general y el tratamiento para fines científicos, considerando la aplicación de un proceso de disociación.

Esta necesidad de aprovechar la información en posesión de los Estados para fines científicos de salud, puede confluir en conflicto de interés entre la protección del derecho del titular de los datos personales, y el establecimiento de esfuerzos de colaboración con las empresas farmacéuticas para la

aplicación del conocimiento científico en la investigación del que se derivarán nuevos productos médicos, cuyo beneficio económico directo recaerá en ellas.

Un segundo riesgo entre privacidad y datos disociados para fines científicos se tiene entre los datos sensibles que incluyen la información genética de los pacientes y las investigaciones que se realizan en el genoma humano como parte de los avances médico-biológicos, siendo que la consideración de la información genética resulta necesaria para profundizar en el estudio de la biología humana y sus enfermedades, considerando inclusive patrones hereditarios para el desarrollo de tratamientos médicos específicos.

El aprovechamiento colectivo que ofrece una estrategia de Big Data dirigida al sector salud, no limita la consideración del beneficio individual, principalmente en situaciones que hacen necesario que un paciente reciba un trato personalizado, y pueda vincularse electrónicamente con otras fuentes de información para recibir atención médica, realizando intercambio de información con otros prestadores de servicios de salud.

Desde la perspectiva del interés general, es importante salvaguardar el derecho de los titulares a la protección de sus datos personales, para hacerlos accesibles a la colectividad, bajo la tutela del Estado, que en ejercicio de sus obligaciones de proteger los derechos individuales deberá tener la capacidad y habilidad de administrar la información confiada en forma responsable, estableciendo los mecanismos y políticas que aseguren la protección y aprovechamiento responsable de la información contenida en los sistemas de salud, para la investigación científica en el área de salud.

9.3 BIG DATA Y ENTIDADES FINANCIERAS

Sabido es que la ingeniería aplicada para perfilamiento y conocimiento de clientes se utiliza en el sector analizado desde hace mucho tiempo, incluso antes de considerarse algún tipo de protección a los datos personales. Tampoco tenía ésta actividad un nombre apetecible para una época tan tecnologizada como la actual, era simplemente la labor de analistas de información de muy diversas fuentes para el ofrecimiento de determinados productos para determinados clientes y una pretensión de calificación de riesgo, considerando los antecedentes de cumplimiento de las obligaciones económicas de las personas en general.

Otra condición era que la información o datos que se analizaban se encontraban dispersos en muy diversas fuentes, tanto privadas como públicas, y ciertamente ninguna de ellas contaba con las autorizaciones que los titulares hoy, en términos generales deben dar o conocer a quienes las manipulan, como es el caso de las llamadas sociedades de información crediticia, entidades que refiriéndome al caso mexicano que es muy representativo de los países en los que existe, tienen por objeto fundamental el recopilar y manejar datos bancarios, financieros y otros relativos al historial crediticio y otras operaciones de naturaleza análoga de personas y empresas, mantenerlo y acrecerlo con aquellos datos que les proveen sus propios participantes (bancos, operadores financieros, casas comerciales y autoridades) así como información de operaciones crediticias fraudulentas con objeto que los mismos sean entregados a los participantes y usados por éstos para llevar a cabo distintas actividades, la mayoría vinculada al explotación mediante el análisis del conocimiento de quienes ahí aparecen.

Al respecto del tema, consideremos al Big Data como tendencia y consecuencia en el avance de la tecnología, es la fórmula perfecta para el análisis de una gran cantidad de información para su posterior explotación por aquellos que la realizan y contar con una herramienta científica para la toma de decisiones. Dicho conocimiento puede poner en jaque la privacidad, la honra, la reputación y por supuesto el derecho a la protección de los datos personales, ya que todos tenemos información y datos por evidente consecuencia del desarrollo, actas de nacimiento, registros escolares, antecedentes laborales, historia social y por supuesto bancaria y financiera.

El derecho a la protección de datos personales viene garantizando un principio de calidad de los datos y el ejercicio de derechos ARCO, que no es más que la garantía de que la información inadecuada, incompleta o excesiva que se contenga en medios sea eliminada o rectificada.

Precisamente en el ejercicio de éste derecho radica una disposición creada dentro del sector y circunscrita en las sociedades de información crediticia. En el caso mexicano, como en otros como el español, transcurridos seis años en términos generales aplicamos un "reseteo" de aquellos incumplimientos o desviaciones que se hubieran realizado para el cumplimiento de obligaciones y en consecuencia, aquellos análisis que se realicen contendrán una historia parcial de la realidad en el cumplimiento y perfilamiento que se realice con el Big Data.

De lo anterior surge la inquietud de que ocurre en países donde la legislación no contempla estas figuras y se producen tratamientos relativos a solvencia patrimonial y crédito mediante

técnicas de Big Data, pudiendo aparecer información sobre insolvencias crediticias o impagos con una antigüedad sin límite.

9.4 BIG DATA Y LA PUBLICIDAD COMPORTAMENTAL

El GT29, a través de su Dictamen 2/2010 sobre publicidad comportamental en línea, la identifica como aquella actividad que "implica la identificación de los usuarios que navegan por internet y la creación gradual de perfiles que después sirven para enviarles publicidad que corresponde a sus intereses."

Conforme a lo anterior, para este Grupo de Trabajo los siguientes elementos son definitorios de este tipo de publicidad son:

- *Permite la identificación de "usuarios" (personas físicas, titulares de datos personales).*
- *La identificación de éstos se efectúa a partir de su navegación por internet.*
- *Esta identificación permite, a su vez, la creación gradual de perfiles (profiling).*
- *La creación de estos perfiles tiene por objeto el envío de publicidad que correspondería "a los intereses" de los usuarios.*

Claramente, nos encontramos frente a una actividad especializada que hace uso de Big Data; sin embargo, cabría analizar si, dentro de esta definición, el interés de los usuarios por recibir este tipo de publicidad constituye en sí mismo un elemento que la defina o si, por el contrario y como puede también deducirse, "el interés" radica en aquellos que generan publicidad comportamental.

Esta observación no pasa inadvertida para el GT29, que "no cuestiona los beneficios económicos que la publicidad comportamental pueda aportar a los que la practican" a la vez que establece claramente que esta práctica "no debe realizarse a expensas de los derechos a la intimidad y a la protección de datos de las personas". Consideramos que la misma posición debe ser adoptada por las diferentes autoridades nacionales y difundida entre responsables y titulares.

Por otro lado, es necesario tomar en cuenta que el uso de medios electrónicos para la definición de perfiles (tecnologías de rastreo) como elemento esencial de este tipo de publicidad, se ha convertido en un elemento diferenciador entre las diversas legislaciones que regulan su uso.

Existen aquellas que requieren que el uso de dichas tecnologías sea informado a los usuarios y que éstos puedan aceptarlas de forma previa a su instalación en sus propios equipos, con opción a su rechazo; otras requieren de información previa y obligatoria para los usuarios, que les permita rechazar (a posteriori) la instalación de este tipo de tecnologías. Otras simplemente exigen que se proporcione información a los usuarios, sin que necesariamente deba ser previa o accesible antes de su instalación.

En todo caso, es necesario establecer qué legislaciones cuentan con las disposiciones necesarias para salvaguardar los derechos de los titulares de datos personales que pueden ser objeto de publicidad comportamental, así como su expectativa razonable de privacidad.

Identificamos como esencial el cumplimiento del principio de información, que en relación con las finalidades de mercadotecnia, publicidad y prospección comercial, deben encontrarse expresamente recogidos en los Aviso de Privacidad, de forma que aquellos responsables que traten datos personales para dichas finalidades, deban comunicarlo expresamente a los afectados, dando opción a su negativa cuando esta finalidad no resulta necesaria para la relación jurídica existente entre ambas partes.

El uso de tecnologías de rastreo también está expresamente regulado por algunas normativa nacionales. En este sentido, es necesario recordar que bajo la rubrica "Política de cookies, web beacons u otras tecnologías similares", las normativas nacionales aludidas disponen (de manera análoga a la mexicana) que cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos.

Por lo anterior, en el contexto de Big Data y la publicidad comportamental, se hace necesario emprender acciones de formación y concienciación sobre el uso de las tecnologías de rastreo que la normativa vigente ya regula, pero que su propia novedad parece alejar de su cumplimiento integral.

En esencia, se considera que la especialidad de actividades de Big Data (como la publicidad comportamental) debe dar lugar a su identificación, estudio y definición de actividades de cumplimiento, para que cada una de ellas se desarrolle con respeto de los derechos fundamentales de las personas, en relación con el tratamiento de sus datos personales y de su privacidad.

9.5 BIG DATA Y EDUCACIÓN

Hoy en día existe una cantidad ingesta de información que está chocando en nuestra sociedad y que en la mayoría de las ocasiones es imposible o insostenible de tratar o analizar con herramientas de base de datos. Consolidando un entorno donde es común la proliferación de webs, apps de imagen y sonido, redes sociales, dispositivos móviles, sensores,….

Por lo que, debemos de ser conscientes de la realidad en la cual vivimos e irnos adaptando a ella. Para ello, es bueno conocer y comprender las tendencias actuales y futuras, sobre modelos basados en Big Data. De esta forma se ayudará a que las instituciones educativas puedan adaptarse e identificar a estudiantes en riesgo, de forma que puedan intervenir con el fin de reducir la deserción y aumentar las tasas de graduación de los alumnos/as.

Este tipo de medidas dentro del ámbito académico, se pueden abarcar desde dos perspectivas: una centrada en la propia institución, y otra en el aprendizaje. Siendo mucho más efectiva la primera, ya que propone modelos educativos centrados en Big Data que optimizan la deserción en el ámbito educativo (centro e instituciones), así como también realiza un seguimiento más exhaustivo de los alumnos/as.

Una forma de logarlo, es mediante el análisis y comprensión de la información disponible en la web, como son: redes sociales, sistemas educativos, webs institucionales,…

Esta innovación educativa está en auge actualmente, gracias a los conocidos cursos MOOCs (Massive Online Open Courses), que ofrecen cursos de formación abiertos, masivos y gratuitos. Nacieron en el año 2008, y tenían como iniciativa el acercamiento de conocimiento de nivel superior a todos los internautas, sin tener que ser estudiantes de universidad. Es una formación globalizada e

internacional, que busca un público más amplio, con el objetivo de liberar conocimiento. Cuenta con un sistema de evaluación propio, que valorar a cada uno de los estudiantes en función de los conocimientos adquiridos.

Además, este tipo de enseñanza no sólo ayuda en la lucha de la brecha digital; sino que también proporciona una serie masiva de información (Big Data) muy importante para la mejora de la enseñanza en todos los niveles educativos: social, cognitivo y emocional, a nivel individual, grupal e institucional. Al mismo tiempo que, facilita y mejora el apoyo que se ofrece en tiempo real a cada uno de los alumnos/as de estos cursos.

Toda esa información recogida, tiene un gran valor educativo para las instituciones, ya que ayudará a mejorar el diseño curricular de muchas de las materias adaptándose, aún si cabe, a las necesidades reales de los alumnos/as. De esta forma se podrán solucionar algunas de las necesidades que se requieren en las universidades, como son: módulos más adaptados, módulos actualizados, platear tareas, recoger el feedback y diseñar una formación más relevante que constituya un aprendizaje más efectivo y mejore la enseñanza.

Por último y sin menor relevancia, un punto a considerar dentro de esta problemática, son los aspectos éticos, morales y legales de dicho uso de la información. Un elemento crucial en la privacidad de datos. Las herramientas analizadas a lo largo de la presente Declaración (como la evaluación de impacto) se manifiestan imprescindibles a la hora de realizar este tipo de tratamientos, sobre todo si son de menores.

10. EL CONCEPTO DE PORTABILIDAD DE LOS DATOS E INTEROPERABILIDAD

En una época en donde la migración de servicios hacia soluciones de Cloud Computing y aplicaciones es cada vez más común, la protección de datos se vuelve fundamental, pero también la posibilidad de estandarizar los procesos de portabilidad de los datos de usuarios asociados a diversos servicios de Cloud Computing.

Se debe implementar una política de portabilidad e interoperabilidad como política de contratación. La portabilidad de datos representa el mayor riesgo operativo para los usuarios del Cloud Computing, ya que ante la ausencia de regulación que establezca los formatos, parámetros, términos y condiciones bajo los cuales un proveedor de Cloud Computing portará los datos a otro en caso de terminación del contrato del primero, como si ha ocurrido en el caso de los servicios

telefónicos, la posibilidad de hacer efectivo éste derecho radica en la inclusión de una cláusula contractual que precisamente se encargue de lidiar con éste tema.

Desafortunamente para el crecimiento de la industria de servicios de Cloud Computing, la obligación de permitir la portabilidad del dato es una cláusula que el cliente o usuario debe buscar incluir en el contrato, y es que no solamente se trata de hacer que el proveedor del servicio entregue un soporte magnético u óptico que contenga la información del usuario, sino que además el cliente debe buscar garantía de que esos datos entregados puedan ser leídos y procesados por su nuevo proveedor y que la información en poder del proveedor primigenio sea destruida dentro del plazo legal aplicable. Dicho proceso debe ser verificable, en el entendido que no debe existir ninguna información adicional o derivada de la información original que pueda ser utilizada o considerada propia por el proveedor.

Es importante hacer notar que la creciente configuración de nubes pone en peligro el principio de neutralidad de la Red, ya que el hecho de que un cliente o usuario de servicios en nube no pueda portar sus datos entre uno u otro proveedor, pone en entredicho la libertad de contratación, el derecho protección y uso de sus datos, razón por la cual diversos expertos ya han comenzado a elaborar el concepto denominado cloud neutrality, estableciendo la necesidad de establecer la portabilidad de los datos como un derecho legalmente previsto en los contratos en cuestión, y aceptado por el proveedor, mismo que deberá sujetarse a reglas básicas que permitan portar los datos y supervisar la debida realización de los mismos.

Por lo anterior, es muy importante establecer que en la actualidad dentro de las diversas opciones que ofrecen los proveedores de Cloud Computing se pueden encontrar soluciones abiertas a la portabilidad de datos y soluciones sin portabilidad.

Aunque como se ha señalado anteriormente, la idea es que se generen en un futuro parámetros internacionales que permitan a los usuarios de soluciones de Cloud Computing requerir y exigir a los proveedores de las mismas reglas que de portabilidad de datos sin restricciones, actualmente los usuarios deben buscar solución abierta a la portabilidad, en el entendido que las mismas permiten con mayor facilidad transferir todos sus datos y aplicaciones del usuario desde un proveedor de Cloud Computing a otro (o a los sistemas propiedad del cliente), garantizando la disponibilidad de los datos y la continuidad del servicio.

Es vital tener en cuenta que los contratos de Cloud Computing pueden terminarse no sólo en el caso de rescisión de contrato por parte del cliente, sino por otras circunstancias ajenas al mismo, como podría ser el fin de la prestación de algún tipo de servicio por parte del proveedor, el cambio de su política comercial o cambios en el marco regulatorio existente, razón por la cual, el usuario debe tener en cuenta que tipo de contrato tiene firmado, ya que entre más restringido esté el derecho de portar sus datos, mayor será la dificultad de transferir sus datos.

Es fundamental que los usuarios de soluciones de Cloud Computing celebren acuerdos con proveedor reconocidos por su calidad en el servicio y que reconozcan los derechos de portación de los datos y apliquen la legislación local de protección de datos. El usuario de soluciones de Cloud Computing debe tener la opción de exigir a su proveedor la portabilidad de la información a sus propios sistemas de información o a un nuevo prestador de Cloud Computing, lo anterior, siempre de acuerdo con las condiciones y términos acordados para tal efecto.

La portabilidad de datos debe también generarse y adecuarse para resolver los casos de transferencias internacionales, que podrían generar afectaciones de derechos y conflictos entre legislaciones, en el entendido, que dicha situación pudiera lugar a transferencias de datos a proveedores situados en jurisdicciones con menos medidas de protección y protección a los datos personales de los usuarios y requerir, en su caso, autorización previa de la Autoridad de Control.

El debido establecimiento de los procedimientos de portabilidad de datos, y la subsecuente entrega de información a un nuevo proveedor hará mas sencillo el proceso de migración de bases de datos, sin afectar, dañar o impedir dicha migración, resguardando la integridad de los datos. El proveedor debe garantizar por escrito dicha obligación de portar de manera adecuada e integra la información y detallar los procedimientos aplicables. No obstante lo anterior, la determinación de normas y parámetros técnicos aplicables respecto a la migración y recepción de bases de datos entre proveedores de soluciones de Cloud Computing son necesarias para generar interoperabilidad entre los mismos y sus sistemas para asegurar la portabilidad de datos de los usuarios.

Las Partes deben establecer procedimientos, con la finalidad de que una vez concluida la portabilidad, el proveedor anterior garantice al usuario el borrado seguro de los datos entregados bajo el contrato anterior. Dichos procesos de borrado seguro pueden ser realizados y/o validados por terceros designados previamente en el contrato.

La interoperabilidad debe en todo momento aligerar la carga del cumplimiento de las funciones básicas de las soluciones de Cloud Computing, al asignar el quién, qué y dónde para mantener organizados los datos no estructurados. Estas tareas deben ser ejecutadas sobre servidores que formen parte de las soluciones de Cloud Computing como una tarea en segundo plano, virtualmente invisible para los usuarios, manejando archivos sin interrumpir el flujo de trabajo.

La interoperabilidad de redes debe permitir a los proveedores desarrollar una interacción segura y fluida entre centros de datos de la nube y crear centros de datos mucho más sencillos con una infraestructura más ágil que mejores los procesos de gestión.

Por lo anterior, la interoperabilidad debe ayudar a alcanzar la eficiencia global del Cloud Computing mediante las mejores prácticas de la infraestructura. Para facilitar lo descrito, los proveedores debe proporcionar y estandarizar las mejores prácticas, modelos de uso, diseños de referencia y sólidas herramientas para planificar e implantar estrategias de la nube garantizando la interoperabilidad de las redes y soluciones utilizadas. La creación de estándares para soluciones de interoperabilidad en Cloud Computing debe incluir elementos relacionados con las redes definidas por el software, innovaciones en almacenamiento y avances en arquitectura de redes utilizadas.

Para finalizar, se deben tener en cuenta algunas de las responsabilidades que los proveedores de servicio deberían asumir:

- *Responsabilidad por daños por Interrupción en el Servicio. Independientemente de establecer los parámetros mínimos de servicios, los proveedores deben reconocer expresamente en los contratos que contengan soluciones los niveles de responsabilidad directa por la interrupción que afecten los servicios. Es cierto que el cómputo en la nube establece un problema práctico para determinar la responsabilidad de los proveedores de servicios por fallas en los mismos, ya que el cómputo en la nube consiste en la mezcla de recursos e infraestructuras para poder brindar a los usuarios movilidad, disponibilidad y funcionalidad; por tanto es importante que los proveedores de Cloud Computing determinen y delimiten las partes de su red e infraestructura en las cuales aceptan control y responsabilidad ante el usuario por fallas en los servicios prestados. Determinado lo anterior, es muy*

importante establecer no solamente procesos de falla, sino procesos de aceptación de responsabilidad y las penalidades aplicables por dichas fallas.

- *Acuerdo de Niveles de Servicios.- Ya antes hemos hablado de la importancia de un acuerdo de niveles de servicio o SLA (Service Level Agreement) por lo que en este punto vale la pena recordar que el Contrato de Cloud Computing debe contener un anexo que detalle de manera eficiente los parámetros, niveles y términos de servicios que permitan la funcionalidad de acuerdo con lo requerido por el cliente, dentro de dicho Acuerdo de Niveles de Servicio se deben incluir por lo menos los siguientes elementos:*

  i) Disponibilidad Mínima de los Servicios e Infraestructura.

  ii) Tabla de penalidades por incumplimiento en la disponibilidad

  iii) Detalle de los parámetros técnicos a medir durante la prestación de los servicios.

  iv) Tipos y periodicidad para la entrega de reportes.

  v) Tiempos máximos para reparación de fallas

  vi) Procesos de escalamiento.

  vii) Detalle sobre los procesos de seguridad aplicables.

  viii) Detalle de Monitoreo.

Es muy importante señalar que una de las obligaciones claves del cómputo en la nube es la funcionalidad de servicios en tiempo real y la garantía de protección y resguardo eficiente de la información, transmitida, intercambiada y/o almacenada a través de recursos de cómputo en la nube.

No basta agregar niveles de servicios, ya que si estos no garantizan la disponibilidad y funcionalidad de los mismos, no puede garantizarse que los servicios de cómputo en la nueve sean prestados de forma eficiente ni que otorguen las ventajas ofrecidas al usuario de manera efectiva.

- *Responsabilidad de Garantizar la disponibilidad del Dato.- Es indispensable que los proveedores de Cloud Computing garanticen la disponibilidad y seguridad del dato almacenado, transmitido e intercambiado, ya que más allá de la forma en que pueda funcionar o estar conformada la infraestructura utilizada o el servicio prestado, la capacidad del usuario de recuperar, modificar o eliminar su información en tiempo real no puede ser limitada. La capacidad para utilizar los datos almacenados, en tiempo real y en cualquier dispositivo, debe ser la premisa del prestador de servicios de cómputo en la nube. Adicionalmente a lo antes referido, la responsabilidad por afectar la disponibilidad en el acceso a los datos de usuario, debe ser una responsabilidad que el proveedor reconozca en los contratos en cuestión.*

- *Localización del Dato.- Este punto en particular puede generar muchas confusiones y discusiones entre los especialistas, ya que si bien es cierto, la posibilidad de resguardar un solo dato o bases de datos en diferentes lugares de forma simultanea es una de las características principales del cómputo en la nube, los proveedores defienden la idea de mantener en secreto los diversos lugares en donde se guarda la información, siempre por cuestiones de seguridad y protección del usuario y el proveedor. Uno de los problemas que puede generar la ubiquidad de los datos es sin duda la determinación de la jurisdicción aplicable para el caso de un conflicto entre las partes o que se provoque una transferencia internacional de datos.*

Si bien es cierto que el secreto de los datos es importante por temas de seguridad, también lo es que debe existir compromiso expreso del proveedor de señalar al usuario el lugar físico principal en donde se guardará la información, además de borrar y hacer constar la eliminación de datos de cualquier registro y lugar del proveedor al finalizar el contrato.

Por lo anteriormente expuesto entendemos,

Que siendo los datos personales la moneda de oro de la economía digital y el motor de la economía del siglo XXI. Los datos son el negocio de los negocios.

Que como quiera que los datos personales son un activo y generan valor para las organizaciones y el Estado, no cesarán los esfuerzos para, de una parte, flexibilizar su uso, especialmente frente a regulaciones que siguen, en buena medida, el modelo europeo sobre

tratamiento de datos personales, y de otra parte, exigir el debido tratamiento de esa información para evitar la eventual vulneración de los derechos de las personas cuando su información es tratada indebidamente.

Que los beneficios o maleficios del Big Data dependerán del uso ético y responsable que haga quien posee enormes cantidades de datos sobre diversos aspectos de millones de personas alrededor del mundo.

Que debido a que con la tecnología se puede hacer casi todo. La pregunta que surge es la siguiente: ¿todo lo tecnológicamente posible, es social y humanamente deseable?

Que ante el desarrollo de estas tecnologías que indudablemente tienen consecuencias altamente positivas para la humanidad, con grandes posibilidades en sectores como la sanidad, los diferentes Estados, las entidades y las empresas se deben implicar para que el uso de estas tecnologías no se utilicen con fines invasivos de la privacidad de las personas.

Que corresponde a los Estados adaptar las legislaciones y unificarlas, desarrollando nuevas herramientas que mejoren la privacidad de los individuos cuando se usan estos sistemas, y corresponde alas empresas y entidades implementarlos.

Que estos sistemas, herramientas y garantías deben ir encaminados a los principios de transparencia, objeción al tratamiento, inocuidad para el afectado, calidad de los datos, minimización de los mismos y responsabilidad en lo que respecta a las relaciones con los individuos, debiendo obligar las diferentes legislaciones a la implantación de medidas de índole técnica y organizativa que prevean la evaluación de impacto en privacidad, el privacy by design, la adopción de medidas de seguridad, la anonimización de los datos, el ejercicio de derechos de acceso, rectificación, cancelación y oposición y la disponibilidad, integridad y confidencialidad de la información.

Que hay que preguntarse en que clase de sociedad queremos vivir, qué tipo de información estamos dispuestos a que se recabe diariamente sobre lo que hacemos, donde vamos, sobre como nos comportamos y durante cuanto tiempo ha de ser analizada y accesible.

Que la tecnología y la información no son por sí solas el problema. Todo radica en su uso. Si se puede hacer algo con la información, alguien lo va a hacer (o lo está haciendo): Hacia dónde vamos a seguir y a dónde vamos a parar?

Que es bienvenida la innovación y es bienvenido el Big Data, pero también bienvenida la reflexión crítica sobre los riesgos del big data. No podemos ser espectadores ingenuos y ciegamente maravillados por lo que nos dicen sobre el big data. Como todo en la vida, no es positiva la "tecnofobia" ni la "tecnofascinación" pero si la tecnoreflexión y sobre todo la ética.