Resolución sobre
Big Data

Se afirma con frecuencia que la capacidad de almacenar y analizar grandes cantidades de datos puede ser benéfica para la sociedad. El *Big Data* (Metadatos) puede utilizarse, por ejemplo, para predecir la propagación de epidemias, descubrir los graves efectos secundarios de medicamentos y combatir la contaminación en las grandes ciudades. Algunos de estos usos no implican datos personales. Sin embargo, el *Big Data* también puede usarse en formas que generan una preocupación importante respecto a la privacidad de las personas y los derechos civiles, y a las protecciones contra la discriminación y las vulneraciones al derecho a trato igual.

El *Big Data* implica una nueva forma de ver la información, revelando aquella que antes era difícil de extraer o que estaba oculta. En gran medida, el *Big Data* implica la reutilización de la información. El valor de la información puede estar ligado a su capacidad para hacer predicciones acerca de acciones o eventos futuros. El *Big Data* puede ser percibido como un desafío para los principios clave de privacidad, en particular los principios de limitación de la finalidad y la minimización de datos.

La protección proporcionada por estos principios es más importante que nunca, sobre todo en momentos en que se recopila una cantidad cada vez mayor de información sobre nosotros. Los principios ofrecen las bases para salvaguardar la amplia creación de perfiles (*profiling*) en una creciente variedad de nuevos contextos. El debilitamiento de los principios clave de privacidad, junto con un mayor uso del *Big Data*, es probable que tenga consecuencias adversas para la protección de la privacidad y de otros derechos fundamentales.

Los miembros de la Conferencia Internacional y otros actores interesados (*stakeholders*), incluido, por ejemplo, el Grupo de Trabajo Internacional sobre Protección de Datos en Telecomunicaciones (IWGDPT, conocido como "Grupo Berlín") han considerado temas de protección de datos y privacidad relacionados con el *Big Data*. La preocupación por la privacidad en el uso de perfiles fue planteada por la Conferencia Internacional en la Declaración de Uruguay sobre Creación de Perfiles de 2012 y en la Resolución de Varsovia sobre Perfiles de 2013. Con el fin de fomentar aún más los esfuerzos para ayudar a reducir los riesgos asociados con el uso del *Big Data*

la 36ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad hace un llamado a todas las partes que utilizan el *Big Data* para:

- Respetar el principio de especificación de finalidad.

- Limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende.

- Obtener, cuando sea apropiado, el consentimiento válido del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles.

- Ser transparentes acerca de qué información se recolecta, cómo se procesa, con qué propósito serán utilizados y si será transferida a terceros.

- Dar a las personas acceso apropiado a los datos que han sido recolectados sobre ellas y a la información y decisiones que se han tomado con esos datos. Las personas deben ser avisadas de la fuente de sus datos personales y, cuando sea apropiado, de su derecho a corregir su información, así como de las herramientas para controlar esta información.

- Ofrecer a las personas, cuando sea apropiado, acceso a la información sobre los insumos principales y los criterios para la toma de decisiones (algoritmos) que se han utilizado como base para el desarrollo del perfil. La información debe presentarse en un formato claro y comprensible.

- Llevar a cabo una evaluación de impacto en la privacidad, especialmente cuando el análisis del *Big Data* implica usos novedosos o inesperados de los datos personales.

- Desarrollar y utilizar tecnologías del *Big Data* de acuerdo con los principios de la *Privacidad por Diseño*.

- Considerar cuándo los datos anónimos mejorarán la protección de la privacidad. La anonimización puede ayudar a mitigar los riesgos para la privacidad asociados con el análisis del *Big Data*, pero sólo si la anonimización está diseñada y gestionada apropiadamente. La solución óptima para anonimizar los datos debe decidirse caso por caso, posiblemente utilizando una combinación de técnicas.

- Tener mucho cuidado, y actuar cumpliendo la legislación aplicable en materia de protección de datos, cuando se comparten o se publican conjuntos de datos con seudónimos o que pueden ser identificables indirectamente. El acceso debe ser limitado y controlado cuidadosamente si los datos contienen suficientes detalles, esto es, que pueden vincularse con otros conjuntos de datos o contienen datos personales.

- Demostrar que las decisiones respecto al uso del *Big Data* son justas, transparentes y responsables. Relacionado con el uso de datos para fines de creación de perfiles, tanto éstos como los algoritmos en que están basados requieren una valoración continua. Este necesita revisiones regulares para verificar si los resultados de la creación de perfiles son responsables, justos y éticos y si son compatibles y proporcionados con el propósito para el cual los perfiles son usados. Debe evitarse la injusticia con las personas debido a resultados completamente automatizados que arrojen un falso positivo o un falso negativo. Siempre debe estar disponible una valoración manual de resultados, con efectos significativos para los individuos.