COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Estrasburgo, 23 de enero de 2017 T-PD(2017)01

COMITÉ CONSULTIVO DEL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS EN RELACIÓN CON EL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL

(T-PD)

DIRECTRICES[1] SOBRE LA PROTECCIÓN DE LAS PERSONAS EN RELACIÓN CON EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL EN UN MUNDO CON BIG DATA[2]

Director General de Derechos Humanos y Estado de Derecho

[1] Emanados de los 50 miembros con derecho a voto consultados mediante procedimiento escrito: Dinamarca, Liechtenstein, y Luxemburgo se abstuvieron, Alemania e Irlanda presentaron su objeción.
[2] El borrador inicial, así como las versiones posteriores fueron redactadas por Alessandro Mantelero, Profesor Agregado Permanente en el Instituto Politécnico di Torino (Italia).

I. Introducción

Los Big Data representan un nuevo paradigma en la manera en que se recolecta, combina y analiza la información. Los Big Data o grandes volúmenes de datos, que se benefician de la interrelación con otros entornos tecnológicos como son el Internet de las cosas y la computación en la nube, pueden ser fuente de valor e innovación significativos para la sociedad, mejorando la productividad, el desempeño del sector público y la participación de la sociedad.

Los valiosos descubrimientos revelados a través de los Big Data cambian la manera en que es posible comprender y organizar a la sociedad. No todos los datos procesados en un contexto de Big Data tienen relación con los datos personales y la interacción de los seres humanos, pero sí una gran cantidad y con un impacto directo sobre los individuos y sus derechos con respecto al tratamiento de datos de carácter personal.

Asimismo, dado que los Big Data permiten recolectar y analizar grandes cantidades de datos para identificar patrones de actitud y predecir el comportamiento de grupos y comunidades, también es necesario considerar la dimensión colectiva de los riesgos relacionados con el uso de datos.

Esto llevó al Comité del Convenio para la Protección de las Personas en Relación con el Tratamiento Automatizado de Datos de Carácter Personal (CETS 108, en adelante el "Convenio 108") a redactar estas Directrices, con las cuales se busca ofrecer un marco general para que las Partes apliquen las políticas y medidas adecuadas y hacer efectivos los principios y las disposiciones del Convenio 108 en el contexto de los Big Data.

Estas Directrices han sido redactadas de conformidad con los principios del Convenio 108, a la luz del proceso de modernización en marcha, y están principalmente dirigidas a legisladores, quienes ejercen el control y realizan el tratamiento, tal como se define en la Sección III.

Considerando que es necesario asegurar la protección de la autonomía personal basada en el derecho de las personas a controlar sus datos de carácter personal y el tratamiento de los mismos, la naturaleza de este derecho a controlar deberá tratarse con sumo cuidado en el contexto de los Big Data.

El control requiere tener consciencia del uso de los datos personales y una libertad de elección verdadera. Estas condiciones, esenciales para la protección de los derechos fundamentales, y en particular para proteger el derecho fundamental a la protección de los datos de carácter personal, pueden lograrse mediante diversas soluciones legales. Dichas soluciones deberán ajustarse de conformidad con cada contexto social y tecnológico, tomando en consideración la falta de conocimientos de las personas.

La complejidad y poca claridad de las aplicaciones de los Big Data deberán, por lo tanto, provocar en los legisladores la consideración de la noción del control como algo no circunscripto al mero control individual. Deberán adoptar una idea más amplia del control sobre el uso de los datos, según el cual el control individual evoluciona hacia un proceso de mayor complejidad de evaluación de riesgos con múltiples efectos relativos al uso de datos.

II. Alcance

Estas Directrices recomiendan medidas que deben ser tomadas por las Partes, por quienes ejercen el control y por quienes realizan el tratamiento de los Big Data para evitar el potencial impacto negativo del uso de estos sobre la dignidad y los derechos de los seres humanos, y sobre las libertades fundamentales individuales y colectivas, en especial

con respecto a la protección de datos de naturaleza personal.

En virtud de la naturaleza de los Big Data y sus problemas, la aplicación de algunos de los principios tradicionales de tratamiento de datos (por ej. el principio de minimización de datos, limitación de la finalidad, lealtad y transparencia, y consentimiento libre, específico e informado) puede ser un desafío en este escenario tecnológico. Estas Directrices, por lo tanto, sugieren una aplicación específica de los principios del Convenio 108, de manera tal de que sean más efectivos en la práctica en el contexto de los Big Data.

El propósito de estas Directrices es contribuir con la protección de los titulares de los datos en cuanto al tratamiento de sus datos personales en el contexto de los Big Data mediante la explicación detallada de los principios de protección de datos aplicables y de las prácticas correspondientes, tendientes a limitar los riesgos que pudieran correr los derechos de dichos titulares. Estos riesgos básicamente refieren al potencial sesgo del análisis de los datos, a una subestimación de las implicancias legales, sociales y éticas ante el uso de Big Data en los procesos de toma de decisiones, y a la marginalización de una participación efectiva e informada de quienes son parte de estos procesos.

En vista del alcance de los Big Data en expansión en varias aplicaciones específicas a algunos sectores, estas Directrices la protección de las personas dentro de campos específicos de aplicación de los Big Data (por ej. en el sector sanitario, o en el financiero, o en el sector público, como en el ámbito del cumplimiento de la ley).

Asimismo, a la luz de la evolución de las tecnologías y sus usos, el texto actual de estas Directrices podrá ser revisado en el futuro cuando el Comité del Convenio 108 lo considere necesario.

Nada de lo expresado en estas Directrices podrá interpretarse como impedimento hacia la aplicación de las disposiciones del Convenio 108 o como limitante, así como tampoco a las del Convenio Europeo de los Derechos Humanos.

III. Terminología utilizada a los efectos de estas Directrices

a) **Big Data:** Hay varias definiciones de Big Data que difieren entre sí dependiendo de la disciplina específica. La mayoría de ellas se centra en la capacidad tecnológica creciente para recolectar, procesar y extraer conocimientos nuevos y predictivos a partir de grandes volúmenes de datos sumamente variados y con gran velocidad.[3] En términos de protección de datos, los problemas principales no tienen relación solamente con el volumen, la velocidad y la variedad de datos procesados, sino con el análisis de datos que utilizan programas para extraer conocimientos nuevos y predictivos con el fin de utilizarlos en la toma de decisiones relativas a personas y grupos de personas. A los efectos de estas Directrices, la definición de Big Data, por tanto, incluye a los Big Data y a los Big Data analytics.[4]

b) **Controlador:** Es la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otra entidad que sola o en conjunto con otros, tiene la potestad para tomar decisiones al respecto del tratamiento de datos.

c) **Procesador:** Es una persona física o jurídica, autoridad pública, servicio, agencia o cualquier otra entidad que realiza el tratamiento de los datos de naturaleza personal en representación del controlador.

d) **Tratamiento / Procesamiento:** Es cualquier operación o conjunto de operaciones

realizados sobre datos personales, tales como recolección, almacenamiento, conservación, alteración, recuperación, divulgación, disponibilización, borrado o destrucción de dichos datos, o la realización de operaciones lógicas o aritméticas sobre dichos datos.

e) **Seudonimización:** Se refiere al tratamiento de datos de naturaleza personal a través del cual los datos personales ya no pueden ser atribuidos a una titular de datos específico sin utilizar información adicional, siempre y cuando dicha información adicional se mantenga separada y esté sometida a medidas técnicas y organizativas que aseguren que los datos personales no puedan atribuirse a una persona física identificada o identificable.

f) **Datos abiertos:** Refiere a cualquier información públicamente disponible que puede ser utilizada libremente, modificada, compartida y reutilizada por cualquier persona y con cualquier finalidad, de conformidad con las condiciones de las licencias abiertas.

g) **Partes:** Son las partes legalmente obligadas por el Convenio 108.

h) **Datos de naturaleza personal:** Refiere a cualquier información relacionada con una persona identificada o identificable (el titular de los datos)[5].

i) **Datos sensibles:** Refiere a categorías particulares de datos cubiertos en el Artículo 6 del Convenio 108 que requieren de garantías adicionales adecuadas cuando son sometidos a tratamiento.[6]

j) **Autoridad de control:** Refiere a la autoridad establecida por una Parte y responsable de garantizar el cumplimiento de las disposiciones del Convenio 108.

[3] El término “Big Data” generalmente identifica conjuntos de datos extremadamente grandes que pueden ser analizados con recursos informáticos para realizar inferencias sobre patrones de datos, tendencias y correlaciones. Según la Unión Internacional de Telecomunicaciones, Big Data refiere a “un paradigma para hacer posible la recopilación, el almacenamiento, la gestión, el análisis y la visualización, potencialmente en condiciones de tiempo real, de grandes conjuntos de datos con características heterogéneas” (ITU. 2015. Recomendación Y.3600. Big Data – Requisitos y capacidades de los Big Data basados en la nube).

[4] Este término se utiliza para identificar tecnologías informáticas que analizan grandes cantidades de datos para descubrir patrones ocultos, tendencias y correlaciones. Según la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, el término Big Data analytics “refiere a todo el ciclo de la gestión de datos al recolectar, organizar y analizar datos para descubrir patrones, inferir situaciones o para predecir y entender comportamientos” (ENISA. 2015. Privacidad desde la concepción en los Big Data. Descripción general de las tecnologías que fomentan la privacidad en tiempos de Big Data analytics).

[5] Según esta definición, también cualquier dato utilizado para identificar personas a partir de conjuntos de datos para tomar decisiones que las afectarán en base a información del perfil del grupo es considerado dato personal.

[6] En el contexto de los Big Data, es especialmente relevante en cuanto a información sobre el origen racial o étnico, opiniones políticas, participación gremial, convicciones religiosas o de otra índole, así como los datos personales relativos a la salud o a la vida sexual revelada a través de datos de naturaleza personal mediante procesamientos complementarios o en combinación con otros datos.

IV. Principios y Directrices

1. Utilización de datos con ética y conciencia social

1.1 En virtud de la necesidad de equilibrar los intereses implicados en el tratamiento de datos de naturaleza personal, y en particular en los casos en que los mismos se utilizan con fines predictivos en los procesos de toma de decisiones, tanto controladores como procesadores deberán considerar adecuadamente el posible impacto del pretendido procesamiento de los Big Data y sus amplias implicancias éticas y sociales para salvaguardar el derecho de las personas y las libertades personales, y asegurar el respeto por el cumplimiento de las obligaciones en cuanto a la protección de datos, tal como se estipula en el Convenio 108.

1.2 El tratamiento de datos personales no deberá entrar en conflicto con los valores éticos generalmente aceptados en la comunidad o comunidades correspondientes y no deberá perjudicar los intereses de la sociedad, así como tampoco sus valores ni normas, incluida la protección de los derechos humanos. Si bien definir recomendaciones éticas prescriptivas puede suponer complicaciones debido a la influencia de factores contextuales, es posible encontrar los valores éticos conductores comunes en las cartas internacionales de derechos humanos y libertades fundamentales como el Convenio Europeo de Derechos Humanos.

1.3 En el caso de que la evaluación del posible impacto del pretendido procesamiento de datos descrito en la Sección IV.2 muestre un alto impacto del uso de los Big Data sobre los valores éticos, los controladores podrán establecer un comité de ética *ad hoc* o utilizar otros ya existentes, para identificar los valores éticos específicos a salvaguardar al utilizar los datos. El comité de ética será un organismo independiente compuesto por miembros seleccionados por su competencia, experiencia y características profesionales y por desempeñar sus tareas con imparcialidad y objetividad.

2. Políticas preventivas y evaluación de riesgos

2.1 En virtud de la creciente complejidad del tratamiento de datos y de los usos transformativos de los Big Data, las Partes deberán ser cautelosos al regular la protección de datos en este campo.

2.2 Los controladores deberán adoptar políticas preventivas en cuanto a los riesgos de utilizar Big Data y su impacto sobre los individuos y la sociedad, de manera de asegurar la protección de las personas en relación con el tratamiento de datos de naturaleza personal.

2.3 Dado que el uso de Big Data podría afectar no solo la privacidad y la protección de datos individuales sino también la dimensión colectiva de estos derechos, las políticas preventivas y la evaluación de riesgos deberá considerar el impacto legal, social y ético de su utilización, incluyendo la consideración del derecho de igualdad de trato y de no discriminación.

2.4 De conformidad con los principios de legitimidad del procesamiento de datos y de calidad de los datos del Convenio 108, y de acuerdo con la obligación de evitar o minimizar el impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de los datos, es necesaria una evaluación de riesgos del potencial impacto del procesamiento de datos sobre los derechos y libertades fundamentales para equilibrar la protección de aquellos derechos y libertades con los diferentes intereses afectados por el uso de Big Data.

2.5 Los controladores deberán examinar el posible efecto del pretendido procesamiento de datos sobre los derechos y libertades fundamentales de los interesados para:

1) Identificar y evaluar el riesgo de cada una de las actividades de procesamiento que impliquen el uso de Big Data y los posibles resultados negativos sobre los derechos de las personas y sus libertades fundamentales, en especial el derecho a la protección de datos personales y el derecho a la no discriminación teniendo en cuenta los impactos sociales y éticos.

2) Desarrollar y ofrecer medidas adecuadas, tales como soluciones "desde la concepción" y "por defecto"[7] para mitigar dichos riesgos.

3) Supervisar la adopción de las soluciones ofrecidas y su efectividad.

2.6 Este proceso evaluativo debería ser realizado por personas con las cualificaciones y los conocimientos para evaluar los diversos impactos, incluyendo los ámbitos legal, social, ético y técnico.

2.7 Con respecto al uso de Big Data que podría afectar los derechos fundamentales, las Partes deberán alentar la participación de las diversas partes interesadas (por ej. personas o grupos de personas potencialmente afectados por el uso de Big Data) durante este proceso de evaluación y en el diseño del procesamiento de los datos.

2.8 En los casos en que el uso de Big Data pueda tener un efecto significativo sobre los derechos y las libertades fundamentales de los interesados, los controladores deberán consultar a las autoridades de control en un intento por mitigar los riesgos mencionados en el párrafo 2.5 y beneficiarse de la orientación disponible que ofrecen dichas autoridades.

2.9 Los controladores deberán revisar los resultados del proceso de evaluación regularmente.

2.10 Los controladores deberán documentar la evaluación y las soluciones a las que refiere el párrafo 2.5.

2.11 Las medidas adoptadas por los controladores con el fin de mitigar los riesgos referidos en el párrafo 2.5 deber ser consideradas durante la evaluación de posibles sanciones administrativas.

3. Limitación de la finalidad y transparencia

3.1 Los datos personales podrán procesarse con finalidades determinadas y legítimas y no se utilizarán de una forma incompatible con dichas finalidades. No se deberá procesar nuevamente los datos personales de una manera que el titular de los datos pudiera considerar no esperable, inadecuada, u objetable de cualquier otra manera. La exposición de los titulares de los datos ante diversos riesgos o riesgos mayores a aquellos contemplados en relación con las finalidades iniciales podría ser considerada como un caso de procesamiento adicional de datos de una manera no esperable.

[7] En el contexto de protección de datos, los términos "desde la concepción" y "por defecto" refieren a mediadas técnicas y organizativas tomadas teniendo en consideración la totalidad del proceso de gestión de datos desde la etapa de diseño inicial, para implementar los principios legales de una manera efectiva y crear las garantías de protección de datos en los productos y servicios. Según el enfoque "por defecto" en el ámbito de la protección de datos, las medidas que salvaguardan los derechos a la protección de datos son las incluidas en la configuración por defecto, y especialmente aseguran que solamente se procesa la información personal necesaria para un tratamiento específico.

3.2 En virtud de la naturaleza transformadora del uso de los Big Data, para cumplir con el requisito de un consentimiento libre, específico, informado e inambiguo, y en pos de que los principios de limitación de la finalidad, lealtad y transparencia se cumplan, los controladores deberán identificar los posibles impactos sobre los individuos de los diversos usos de datos e informar a los titulares de los datos sobre dicho impacto.

3.3 De conformidad con el principio de transparencia del tratamiento de datos, los resultados de la evaluación descritos en la Sección IV.2 deben estar públicamente disponibles, sin perjuicio de la información confidencial salvaguardada por ley. Cuando exista dicha confidencialidad, los controladores suministrarán cualquier tipo de información confidencial en un anexo aparte del informe de la evaluación. Dicho anexo no será público, podrá ser accedido por las autoridades de control.

4. Enfoque desde la concepción

4.1 Basados en el proceso de evaluación descrito en la Sección IV.2, los controladores, y cuando corresponda, los procesadores, deberán adoptar soluciones desde la concepción adecuadas en las diversas etapas del tratamiento de los Big Data.

4.2 Los controladores, y cuando corresponda, los procesadores, deberán considerar cuidadosamente el diseño de su procesamiento de datos de manera de minimizar la presencia de datos redundantes o marginales, evitar potenciales datos sesgados ocultos y el riesgo discriminación o de un impacto negativo sobre los derechos y las libertades fundamentales de los titulares de los datos, tanto en la etapa de recolección como en la de análisis.

4.3 Siempre que sea técnicamente posible, los controladores y cuando corresponda los procesadores, deberán comprobar la adecuación de las soluciones adoptadas con el enfoque desde la concepción sobre una cantidad limitada de datos utilizando simulaciones, antes de utilizarlas a gran escala. Esto permitirá evaluar el potencial sesgo al utilizar diversos parámetros al analizar datos y suministrar pruebas para minimizar el uso de información y mitigar los potenciales resultados negativos identificados durante el proceso de evaluación de riesgos descrito en la Sección IV.2.

4.4 En cuanto al uso de datos sensibles, las soluciones desde la concepción serán adoptadas para evitar, tanto como sea posible, el uso de datos no sensibles para inferir información sensible y, si así se hiciera, extender las mismas garantías de las que gozan los datos sensibles, a estos datos.

4.5 Medidas como la seudonimización, que no exime de la aplicación de los principios de protección de datos correspondientes, pueden reducir los riesgos sobre los titulares de los derechos.

5. Consentimiento

5.1 El consentimiento libre, específico, informado e inambiguo deberá estar fundado en la información proporcionada al titular de los datos de conformidad con el principio de transparencia de tratamiento de Big Data, esta información incluirá exhaustivamente el resultado del proceso de evaluación descrito en la Sección IV.2 y podrá además ser proporcionada a través de una interfaz que simula los efectos del uso de datos y su impacto potencial sobre el titular de los datos, utilizando un enfoque de aprendizaje a través de la experiencia.

5.2 Cuando los datos han sido recolectados según el consentimiento del titular de los datos, los controladores y cuando corresponda, los procesadores, ofrecerán recursos técnicos simples y fáciles de utilizar para que los titulares de los datos puedan reaccionar ante tratamientos de datos incompatibles con las finalidades iniciales y retirar el consentimiento.

5.3 El consentimiento no se ha otorgado libremente si existe un desequilibrio claro de poder entre el titular de los datos y el controlador, quien tiene injerencia frente a las decisiones del primero en relación con el tratamiento. El controlador deberá demostrar la inexistencia de dicho desequilibrio o que no afecta el consentimiento dado por el titular de los datos.

6. Anonimización

6.1 En la medida que los datos permitan identificar o reidentificar a las personas, serán de aplicación los principios de protección de datos.

6.2 El controlador deberá evaluar el riesgo de reidentificación tomando en consideración el tiempo, esfuerzo y recursos necesarios en virtud de la naturaleza de los datos, el contexto en que se utiliza, las tecnologías de reidentificación disponibles y los costos asociados. Los controladores deberán demostrar cuán adecuadas son las medidas adoptadas para anonimizar datos y así como para asegurar la efectividad de la desidentificación.

6.3 Será posible combinar medidas técnicas con obligaciones legales o contractuales para evitar la posible reidentificación de las personas en cuestión.

6.4 Los controladores deberán revisar regularmente la evaluación del riesgo de reidentificación a la luz del desarrollo tecnológico con respecto a las técnicas de anonimización.

7. El papel de la intervención del ser humano en las decisiones fundamentadas en Big Data

7.1 El uso de los Big Data deberá salvaguardar la autonomía de la intervención del ser humano en el proceso de toma de decisiones.

7.2 Las decisiones basadas en los resultados proporcionados por Big Data analytics deberán considerar todas las circunstancias relativas a los datos y no deberán estar basadas solamente en información descontextualizada o resultados del tratamiento de datos.

7.3 Cuando las decisiones basadas en Big Data podrían afectar los derechos individuales significativamente o producir efectos legales, a solicitud del titular de los datos, una persona con capacidad para tomar decisiones explicará el razonamiento subyacente al proceso, incluidas las consecuencias de dicho razonamiento sobre el titular de los datos.

7.4 Fundado en argumentos razonables, la persona con capacidad para tomar decisiones tendrá la libertad para no basarse en el resultado de las recomendaciones suministradas utilizando Big Data.

7.5 En los casos en que haya indicaciones a partir de las cuales pueda presumirse la existencia de discriminación directa o indirecta en base al análisis de los Big Data, los controladores y los procesadores deberán demostrar la ausencia de tal discriminación.

7.6 Los individuos afectados por una decisión fundamentada en Big Data tienen el derecho a impugnarla ante la autoridad competente.

8. Datos abiertos

8.1 En vista de la disponibilidad de Big Data analytics, las entidades públicas y privadas deben considerar muy cuidadosamente sus políticas de datos abiertos en lo que concierne a los datos personales, ya que los datos abiertos pueden utilizarse para inferir información sobre personas y grupos.

8.2 Cuando los Controladores de Datos adoptan políticas de datos abiertos, el proceso de evaluación descrito en la Sección IV.2 debe considerar los efectos de la fusión y la minería de datos diferentes pertenecientes a conjuntos de datos diversos, también a la luz de las disposiciones referidas en el párrafo 6.

9. Educación

Co la intención de ayudar a las personas en la comprensión de las implicancias del uso de la información y datos de naturaleza personal en el contexto de los Big Data, las Partes deben considerar la información y la alfabetización digital como una habilidad educativa esencial.