



42° ASAMBLEA GLOBAL DE PRIVACIDAD

OCTUBRE 2020

RESOLUCIÓN ADOPTADA SOBRE LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL

PATROCINADORES:

- Oficina de la Comisionada de Información, Reino Unido (Presidenta de la GPA)
- Oficina de la Comisionada de Información de Australia, Australia

CO-PATROCINADORES:

- Agencia de Acceso a la Información Pública (AAIP), Argentina
- Comisionado de Información y Protección de Datos, (Komisioner për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale), Albania
- Comisión Nacional de Privacidad, Filipinas
- Oficina del Comisionado de Privacidad de Canadá
- Comisión para la Protección de Información Personal, Japón
- Comisionado Federal de Protección de Datos e Información, Suiza
- Autoridad Garante para la Protección de Datos Personales, República de San Marino
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México
- Oficina del Comisionado de Privacidad, Nueva Zelandia
- Comisión Nacional de Informática y Libertades, Francia
- Comisión Nacional de Informática y Libertades, Burkina Faso

La 42ª sesión cerrada anual de la Asamblea Global de Privacidad

RECONOCIENDO que las capacidades de la tecnología de reconocimiento facial son significativas, y que sus posibles aplicaciones podrían aportar beneficios a la seguridad y a la protección pública;

DESTACANDO que la tecnología de reconocimiento facial tiene la capacidad de permitir una vigilancia generalizada, ser altamente intrusiva, proporcionar resultados sesgados y erosionar la protección de los datos, la privacidad y los derechos humanos, lo que a su vez reduce la confianza en su uso;

DESTACANDO que la tecnología de reconocimiento facial se basa en información biométrica sensible que es única y duradera, y que las decisiones que se tomen sobre las personas utilizando esos

identificadores, potencialmente sin su conocimiento o consentimiento, pueden tener consecuencias adversas sin que existan medidas de reparación adecuadas;

OBSERVANDO que la tecnología de reconocimiento facial puede identificar o autenticar incorrectamente a un individuo o puede fallar al identificar o autenticar a un individuo;

OBSERVANDO que los organismos públicos, las organizaciones privadas y la sociedad civil han expresado su preocupación por el hecho de que la tecnología plantea desafíos a la privacidad, legales y éticos, que deben ser abordados;

RECONOCIENDO que hay preocupaciones compartidas y generalizadas acerca de ciertos usos de la tecnología de reconocimiento facial y su creciente despliegue en una serie de aplicaciones y contextos variados, entre ellos:

- La identificación en vivo de personas en espacios públicos con fines de seguridad pública o de prevención y detección de delitos, por parte de los órganos de aplicación de la ley y otras organizaciones;
- El uso de reconocimiento facial en vivo en la lucha contra el COVID-19, para la identificación de individuos que muestran síntomas, o que incumplan las normas de cuarentena;
- La identificación de individuos mediante la comparación de fotografías con imágenes contenidas en bases de datos compiladas de diversas fuentes como los medios de comunicación social;
- La capacidad del uso de la tecnología de reconocimiento facial para evolucionar y ser utilizada de forma imprevista o vinculada con otras capacidades tecnológicas, de forma que se cree un riesgo que dañe a las personas y la confianza pública.

RECONOCIENDO que los diferentes usos del reconocimiento facial plantean diferentes tipos y niveles de riesgos para la privacidad de las personas y que, por lo tanto, requieren un examen cuidadoso a fin de determinar las salvaguardias adecuadas en cada contexto y uso;

PREOCUPADA por el hecho de que el respeto a los derechos de protección de datos y privacidad se vean cada vez más cuestionados por el rápido desarrollo de la tecnología de reconocimiento facial, en la que a menudo se recopilan conjuntos de datos a gran escala procedentes de diversas fuentes públicas y privadas, a menudo sin el conocimiento o el consentimiento de la persona, y que se comercializan para su uso en contextos nuevos o imprevistos;

PREOCUPADA por el hecho de que el uso generalizado del reconocimiento facial pueda tener efectos discriminatorios y repercutir en la capacidad de ejercer otros derechos fundamentales, como la libertad de expresión y de asociación;

RECONOCIENDO que para crear y mantener la confianza de los ciudadanos, es necesario identificar y mitigar los riesgos más importantes para la protección de los datos y la privacidad de las personas, los grupos de personas y la sociedad en general mediante la adhesión a los marcos jurídicos pertinentes, el establecimiento de salvaguardias técnicas y organizativas y la consideración de las preocupaciones éticas y los derechos humanos antes de que se despliegue la tecnología de reconocimiento facial.

DESTACANDO la importancia de que el desarrollo y la aplicación de esos marcos incorporen los principios de protección de datos y privacidad, lo que incluye exigir unos fines claramente definidos, una base legal clara, la necesidad y la proporcionalidad, la legalidad y la transparencia, los derechos individuales y unas estructuras de gobierno claras y responsables, antes de que se despliegue la tecnología de reconocimiento facial;

RECORDANDO que la Asamblea Global de Privacidad ha identificado previamente la necesidad de trabajar en la elaboración de políticas públicas, estándares y modelos globales y de asegurar mayores niveles de cooperación reglamentaria para mejorar la prevención, detección, disuasión y reparación eficientes de los problemas de protección de datos y privacidad y para asegurar la coherencia y previsibilidad del sistema de supervisión en la economía de los datos;

AFIRMANDO la necesidad de que las autoridades encargadas de hacer cumplir la ley de protección de datos y privacidad coordinen sus esfuerzos para influir en la elaboración y aplicación de esos enfoques de protección de datos y privacidad en todo el mundo y adopten medidas cuando proceda; y

REAFIRMANDO la resolución sobre privacidad por diseño adoptada en la 32ª Conferencia en 2010 en Jerusalén, la resolución sobre la elaboración de perfiles adoptada en la 35ª Conferencia en 2013 en Varsovia, así como la resolución sobre *big data* adoptada en la 36ª Conferencia en 2014 en Fort Balaclava y la resolución sobre Ética y Protección de Datos en la Inteligencia Artificial adoptada en la 40ª Conferencia en Bruselas.

Por lo tanto, la 42ª Asamblea Global de Privacidad reitera la importancia de:

- 1. Los principios de protección de datos y privacidad por diseño en el desarrollo y uso de la tecnología de reconocimiento facial;**
- 2. Los principios de necesidad y proporcionalidad, que garantizan que la tecnología de reconocimiento facial sólo se utilice cuando el propósito no pueda lograrse por medios menos intrusivos;**
- 3. La transparencia y la rendición de cuentas responsable [y demostrable] sobre el uso y la gestión de datos personales en las aplicaciones de reconocimiento facial, y los derechos aplicables a las personas, incluyendo el suministro de la tecnología a los organismos encargados de hacer cumplir la ley y su utilización por dichos organismos;**
- 4. Requerimiento de lealtad en el tratamiento de los datos personales;**
- 5. Un enfoque ético para la utilización de los datos biométricos; y**
- 6. Marcos jurídicos adecuados para regular las tecnologías que se encuentran evolucionando, como la tecnología de reconocimiento facial.**

La 42ª Asamblea Global de Privacidad resuelve trabajar juntos en 2020-21 para:

- 1. Enfocarse en los ámbitos antes mencionados y elaborar un conjunto de principios acordados y expectativas para el uso de la información personal en la tecnología de reconocimiento facial, señalando en dónde la tecnología plantea el mayor riesgo para los derechos de protección de datos y privacidad; y recomendar cómo se pueden mitigar**

esos riesgos, para que se adopten en la 43ª sesión cerrada de la Asamblea Global de Privacidad;

2. Tratar de promover los principios acordados mencionados arriba con una serie de grupos clave de terceros interesados que se identificarán, como los desarrolladores y usuarios de sistemas de tecnología de reconocimiento facial, para garantizar que los usos innovadores de la tecnología de reconocimiento facial respeten las obligaciones de protección de datos y de privacidad por diseño;
3. Pedir al Grupo de Trabajo sobre la aplicación internacional de la ley y al Grupo de Trabajo sobre Ética y Protección de Datos en la Inteligencia Artificial que realicen esta labor, teniendo en cuenta las actividades realizadas por otros grupos de trabajo de la Conferencia y consultando con el panel de referencia, según proceda.