



DIE 42. GESCHLOSSENE SITZUNG DES GLOBAL PRIVACY ASSEMBLY

OKTOBER 2020

Angenommene EntschlieÙung zur Gesichtserkennungstechnologie

SPONSOREN:

- Information Commissioner's Office, Vereinigtes K nigreich
- Office of the Australian Information Commissioner, Australien

CO-SPONSOREN:

- Agencia de Acceso a la Informaci n P blica (AAIP), Argentinien
- The Information and Data Protection Commissioner, (Komisioner p r t  Drejt n e Informimit dhe Mbrojtjen e t  Dh nave Personale), Albanien
- National Privacy Commission, Die Philippinen
- Office of the Privacy Commissioner of Canada
- Personal Information Protection Commission, Japan
- Pr pos  f d ral   la protection des donn es et   la transparence (PF PDT), Schweiz
- San Marino Autorit  Garante per la protezione dei dati personali
- National Institute for Transparency, Access to Information and Personal Data Protection, Mexico
- Office of the Privacy Commissioner, Neuseeland
- Commission nationale de l'informatique et des libert s, Frankreich
- National Commission for Informatics and Liberties, Burkina Faso

Die 42. jährliche geschlossene Sitzung des Global Privacy Assemblys

Anerkennend, dass die Fähigkeiten der Gesichtserkennungstechnologie bedeutsam sind und ihre potenziellen Anwendungen Vorteile für die Sicherheit und die öffentliche Sicherheit bringen könnten;

Betonend, dass die Gesichtserkennungstechnologie in der Lage ist, eine weitverbreitete Überwachung zu ermöglichen, dass sie stark in die Privatsphäre eindringt, verzerrte Ergebnisse liefert und den Datenschutz, die Privatsphäre und die Menschenrechte untergräbt, was wiederum das Vertrauen in ihre Nutzung verringert;

Betonend, dass die Gesichtserkennungstechnologie auf sensible biometrische Informationen beruht, die einzigartig und dauerhaft sind, und dass Entscheidungen über Personen aufgrund der Nutzung dieser Identifikatoren, möglicherweise ohne ihr Wissen oder ihr Einverständnis, zu nachteiligen Folgen führen können, ohne angemessene Abhilfemöglichkeiten;

Feststellend, dass die Gesichtserkennungstechnologie eine Person falsch identifizieren oder authentifizieren kann oder eine Person nicht identifizieren oder authentifizieren kann;

Feststellend, dass öffentliche Einrichtungen, private Organisationen und die Zivilgesellschaft ihr Besorgnis darüber zum Ausdruck gebracht haben, dass die Technologie Herausforderungen hinsichtlich der Privatsphäre, des Rechts und der Ethik darstellt, die angegangen werden müssen;

In der Erkenntnis, dass es gemeinsame, weit verbreitete Bedenken über bestimmter Anwendungen der Gesichtserkennungstechnologie und ihres verstärkten Einsatzes in vielen Anwendungen und unterschiedlichen Zusammenhängen gibt, einschließlich, aber nicht beschränkt auf:

- Die Live-Identifizierung von Personen in öffentlichen Räumen zu Zwecken der öffentlichen Sicherheit oder der Verhütung und Aufdeckung von Straftaten, durch Strafverfolgungsbehörden und anderen Organisationen;
- Die Nutzung von Live-Gesichtserkennung bei der Bekämpfung von COVID-19, bei der Identifizierung von Personen mit Symptomen oder bei der Verletzung von Quarantäneregeln;
- Identifizierung von Personen durch Abgleich von Fotografien mit Bildern in Datenbanken, die aus Quellen wie sozialen Medien zusammengestellt wurden;
- Die Möglichkeit, dass die Nutzung der Gesichtserkennungstechnologie sich dahingehend weiterentwickelt, dass sie auf unvorhergesehene Weise oder in Verbindung mit anderen technologischen Fähigkeiten eingesetzt werden kann, so dass die Gefahr der Schädigung der Einzelpersonen und des Vertrauens der Öffentlichkeit besteht.

In der Erkenntnis, dass unterschiedliche Anwendungen der Gesichtserkennung unterschiedliche Risikoarten und -niveaus darstellen und daher sorgfältig geprüft werden müssen, um geeignete Schutzmaßnahmen in jedem Zusammenhang und für jeden Einsatz zu ermitteln;

Besorgt darüber, dass die Einhaltung der Rechte des Schutzes der Privatsphäre und der Daten durch die rasche Entwicklung der Gesichtserkennungstechnologie immer schwieriger wird. Bei dieser Technologie werden große Datensätze oft aus einer Vielzahl öffentlich zugänglicher und privater Quellen zusammengetragen, oft ohne das Wissen oder die Einwilligung einer Person, und kommerziell für die Verwendung in neuen oder unvorhergesehenen Zusammenhängen zur Verfügung gestellt;

Besorgt darüber, dass die weitverbreitete Nutzung der Gesichtserkennung diskriminierende Auswirkungen haben kann und sich auf die Ausübung bestimmter anderer Grundrechte wie der Meinungs- und Versammlungsfreiheit auswirken kann;

In der Erkenntnis, dass die potenziell erheblichen Risiken für den Datenschutz und die Privatsphäre für Einzelpersonen, Gruppen von Einzelpersonen und für die Gesellschaft insgesamt ermittelt und abgemildert werden müssen, um das Vertrauen und das Vertrauen der Bürger zu stärken und zu erhalten. Dies ist möglich durch die Einhaltung der einschlägigen rechtlichen Rahmenbedingungen, die Festlegung technischer und organisatorischer Garantien und die Berücksichtigung ethischer Fragen und der Menschenrechte vor dem Einsatz der Gesichtserkennungstechnologie.

Betonend, wie wichtig es ist, dass die Entwicklung und Umsetzung dieser Rechtsrahmen Grundsätze des Schutzes der Daten und der Privatsphäre umfasst, einschließlich klar definierter Zwecke, klarer rechtlicher Grundlagen, Notwendigkeit und Verhältnismäßigkeit, Fairness und Transparenz, individueller Rechte und klarer, rechenschaftspflichtiger Governance-Strukturen, und zwar vor dem Einsatz der Gesichtserkennungstechnologie;

Daran erinnernd, dass das Global Privacy Assembly zuvor die Notwendigkeit festgestellt hat, auf globale Politiken, Standards und Modelle hinzuarbeiten und ein größeres Maß an regulatorischer Zusammenarbeit zu gewährleisten, um die wirksame Prävention, Aufdeckung, Abschreckung und Abhilfe im Zusammenhang mit datenschutzrechtlichen Angelegenheiten zu verbessern, und um die Einheitlichkeit und Berechenbarkeit des Aufsichtssystems in der Datenwirtschaft zu gewährleisten;

Bekräftigend, dass die Datenschutzbehörden ihre Anstrengungen koordinieren müssen, um Einfluss auf die Entwicklung und Umsetzung dieser Ansätze für den Datenschutz weltweit auszuüben, und um gegebenenfalls Maßnahmen zu ergreifen; und

In Bekräftigung der von der 32. Konferenz 2010 in Jerusalem angenommenen Entschließung über [Privacy by Design](#), der von der 35. Konferenz 2013 in Warschau angenommenen [Entschließung über Profiling](#), der von der 36. Konferenz 2014 in Fort Balaclava angenommenen Entschließung über [Big Data](#) und [der Erklärung zu Ethik und Datenschutz im Bereich der künstlichen Intelligenz](#), die von der 40. Konferenz in Brüssel angenommen wurde.

Daher betont das 42. Global Privacy Assembly die Bedeutung der:

1. Grundsätze des Datenschutzes und von Privacy by Design bei der Entwicklung und Nutzung von Gesichtserkennungstechnologien;
2. Grundsätze der Notwendigkeit und Verhältnismäßigkeit zur Gewährleistung, dass die Gesichtserkennungstechnologie nicht eingesetzt werden kann, wenn sich der Zweck auf

einer angemessenen Art und Weise mit weniger in die Privatsphäre eingreifenden Mittel erreichen lässt;

3. Transparenz und Rechenschaftspflicht hinsichtlich der Verwendung und Verwaltung personenbezogener Daten bei Anwendungen für die Gesichtserkennung, und anwendbare Rechte für Einzelpersonen, einschließlich bei der Bereitstellung der Technologie für Strafverfolgungsbehörden und der Nutzung durch besagte Behörden;
4. Anforderungen an die Fairness bei der Verarbeitung personenbezogener Daten;
5. Ethischen Vorgehensweise bei der Nutzung biometrischer Daten; und
6. Rechtlichen Rahmenbedingungen, die für die Regulierung der sich entwickelnden Technologien wie der Gesichtserkennungstechnologie geeignet sind.

Das 42. Global Privacy Assembly beschließt, in den Jahren 2020-21 zusammenzuarbeiten, um:

1. Sich auf die oben beschriebenen Bereiche zu konzentrieren, um zu überlegen, unter welchen Umständen die Gesichtserkennungstechnologie das größte Risiko für das Recht auf Datenschutz und den Schutz der Privatsphäre darstellt, und um eine Reihe vereinbarter Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie zu entwickeln, einschließlich der Empfehlung, wie die Risiken gemildert werden können. Diese Grundsätze sollen auf der 43. geschlossenen Sitzung des Global Privacy Assemblys angenommen werden;
2. Die oben vereinbarten Grundsätze zu fördern, indem eine Reihe wichtiger externer Interessengruppen, wie etwa Entwickler und Nutzer von Systemen zur Gesichtserkennung, ermittelt werden, um sicherzustellen, dass innovative Anwendungen der Gesichtserkennungstechnologie die Verpflichtungen hinsichtlich des Datenschutzes und der datenschutzfreundlichen Voreinstellungen respektieren;
3. Die Arbeitsgruppe „Internationale Rechtsdurchsetzung“ und die Arbeitsgruppe „Ethik und Datenschutz in der künstlichen Intelligenz“ zu ersuchen, diese Arbeiten gegebenenfalls unter Berücksichtigung der Tätigkeiten anderer Arbeitsgruppen der Konferenz und gegebenenfalls in Abstimmung mit dem Referenzgremium der Interessengruppen durchzuführen.