Résolution présentée par la délégation de l'Union Européenne

Thème Conflits et Sécurité Internationale

Concerne l'usurpation des données personnelles à des fins malveillantes

L'Assemblée Générale,

Outrée de la manière dont les données privées de milliers d'individus sont utilisées contre leur gré et dans le but de nuire à notre société, tout en violant les articles 3 et 5 de la Déclaration universelle des droits de l'homme,

Dénonçant le gouvernement d'Israel de s'être allié au géant américain Microsoft afin de pouvoir stocker des données privées appartenant à des civils palestiniens sur des serveurs de l'Union Européenne, participant donc à une violation concrète de nos lois du Règlement général sur la protection des données (RGPD),

Notant que les données de ces Palestiniens sont par la suite utilisées pour surveiller, cibler et blesser ces individus, notamment par le biais d'attaques aériennes,

Effarée par la façon dont nos serveurs sont exploités illégalement lors des conflits n'impliquant aucun État de l'Union Européenne et dans une optique de violence et de dégradation de la société,

Ajoutant que des scénarios similaires ont lieu quotidiennement sur le réseau social X, en effet l'intelligence artificielle Grok, fondée par Elon Musk, usurpe les données des utilisateurs dans un but lucratif et non éthique,

Appuyant le fait que n'importe quel pays peut être victime d'une telle violation, encore plus avec l'évolution constante de l'intelligence artificielle et que des mesures rigides doivent être prises le plus rapidement possible,

Décide de fonder une nouvelle Agence Internationale pour la Protection des Données (AIPD),

- pour réglementer le stockage de données au sein d'un état, afin d'empêcher que d'autres nations puissent entreposer leurs informations numériques dans des bases de données ne leur appartenant pas, empêchant par la suite la violation de nombreux règlements,

- pour instaurer un logiciel de pistage de données surveillant le contenu, la provenance et le but final de l'utilisation de celles-ci, tout en conservant une trace de chacune d'entre elles, dans le but de les rendre plus traçables,

- visant à intégrer un mécanisme d'urgence de réprimande basé sur la recherche approfondie des deux paramètres évoqués auparavant, en lançant une alerte rapide laissant le choix entre une procédure de suppression totale des données concernées ou une sanction juridique établie selon la gravité de la transgression du règlement mis en place, éliminant par la suite tous risques d'utilisation malsaines de ces données.

Le texte français fait foi.