



Assemblée générale

Distr. générale
7 octobre 2019
Français
Original : anglais

Conseil des droits de l'homme

Quarante-deuxième session

9-27 septembre 2019

Point 3 de l'ordre du jour

Résolution adoptée par le Conseil des droits de l'homme le 26 septembre 2019

42/15. Le droit à la vie privée à l'ère du numérique

Le Conseil des droits de l'homme,

Guidé par les buts et principes énoncés dans la Charte des Nations Unies,

Réaffirmant les droits de l'homme et les libertés fondamentales inscrits dans la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques, le Pacte international relatif aux droits économiques, sociaux et culturels, la Convention relative aux droits de l'enfant et la Convention relative aux droits des personnes handicapées, et d'autres instruments internationaux relatifs aux droits de l'homme,

Réaffirmant également la Déclaration et le Programme d'action de Vienne,

Affirmant le caractère universel, indivisible, interdépendant et indissociable de tous les droits de l'homme et de toutes les libertés fondamentales,

Rappelant toutes les résolutions antérieures de l'Assemblée générale et du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique, ainsi que les autres résolutions pertinentes,

Rappelant également que les entreprises sont tenues de respecter les droits de l'homme, comme le prévoient les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « Protéger, respecter et réparer » des Nations Unies, et que c'est à l'État qu'il incombe au premier chef de promouvoir et de protéger les droits de l'homme et les libertés fondamentales,

Saluant les travaux du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique¹, prenant note avec intérêt des rapports qu'il a établis sur le sujet, et rappelant l'atelier d'experts sur le droit à la vie privée à l'ère du numérique qu'il a organisé les 19 et 20 février 2018,

Saluant également le travail accompli par le Rapporteur spécial sur le droit à la vie privée et prenant note de ses rapports ainsi que des contributions à la promotion et à la protection du droit à la vie privée d'autres titulaires de mandat au titre des procédures spéciales du Conseil des droits de l'homme,

¹ A/HRC/39/29.



Prenant note de la stratégie du Secrétaire général en matière de nouvelles technologies, y compris des travaux du Groupe de haut niveau sur la coopération numérique et du rapport intitulé *The Age of Digital Interdependence* (L'ère de l'interdépendance numérique) que celui-ci a présenté au Secrétaire général le 10 juin 2019,

Notant l'adoption des Principes en matière de protection des données personnelles et de la vie privée par le Comité de haut niveau sur la gestion, le 11 octobre 2018,

Prenant note avec satisfaction de l'observation générale n° 16 (1988) du Comité des droits de l'homme sur le droit de chacun à la protection de sa vie privée et de la recommandation que le Comité a faite aux États de prendre des mesures effectives pour empêcher la conservation, le traitement et l'exploitation illicites de données personnelles stockées par les autorités publiques ou les entreprises, et prenant note également des progrès technologiques considérables qui ont été accomplis depuis l'adoption de l'observation générale et de la nécessité d'examiner le droit à la vie privée au regard des enjeux de l'ère du numérique,

Réaffirmant le droit à la vie privée, en vertu duquel nul ne peut être l'objet d'immixtions arbitraires ou illégales en lien avec son domicile ou sa correspondance ou dans sa vie privée et sa vie familiale, et le droit à la protection de la loi contre de telles immixtions, et conscient que l'exercice du droit à la vie privée est important aux fins de la réalisation d'autres droits de l'homme, dont le droit à la liberté d'expression, le droit de ne pas être inquiété pour ses opinions et le droit à la liberté de réunion et d'association pacifiques, et qu'il est l'un des fondements d'une société démocratique,

Sachant que le droit à la vie privée peut permettre l'exercice d'autres droits, contribuer au libre développement de la personnalité et de l'identité de chacun et faciliter la participation individuelle à la vie politique, économique, sociale et culturelle, et notant avec préoccupation que les violations du droit à la vie privée et les atteintes à ce droit peuvent avoir des incidences sur la réalisation d'autres droits de l'homme, dont le droit à la liberté d'expression et de ne pas être inquiété pour ses opinions et le droit à la liberté de réunion et d'association pacifiques,

Rappelant que l'Assemblée générale, dans sa résolution 73/179 en date du 17 décembre 2018, a encouragé le Conseil des droits de l'homme à poursuivre activement l'examen de la question et a invité tous les acteurs concernés à examiner plus avant les conséquences que le profilage, la prise de décisions automatisée et l'apprentissage automatique, parfois désigné sous le nom d'intelligence artificielle, ont sur l'exercice du droit à la vie privée si aucune garantie n'est prévue, afin d'apporter des éclaircissements sur les principes et les normes existants et de déterminer les meilleures pratiques à adopter en matière de promotion et de protection du droit à la vie privée ;

Sachant que le débat sur le droit à la vie privée devrait être mené à la lumière des obligations juridiques imposées par le droit interne et le droit international, y compris le droit international des droits de l'homme, ainsi que des engagements pris en la matière, et ne devrait pas ouvrir la voie à un empiètement injustifié sur les droits de la personne,

Conscient de la nécessité de continuer d'examiner et d'analyser, à la lumière du droit international des droits de l'homme, les questions liées à la promotion et à la protection du droit à la vie privée à l'ère du numérique, aux garanties procédurales, aux voies de contrôle et de recours interne et aux incidences de la surveillance sur le droit à la vie privée et d'autres droits de l'homme, ainsi que de la nécessité de tenir compte des principes d'absence d'arbitraire, de licéité, de légalité, de nécessité et de proportionnalité en ce qui concerne les pratiques de surveillance,

Notant que le rythme soutenu des avancées technologiques qui permet à chacun, partout dans le monde, d'utiliser les technologies de l'information et de la communication, accroît dans le même temps les moyens dont disposent les pouvoirs publics, les entreprises et les particuliers pour mener des activités de surveillance et intercepter, pirater et collecter des données, ce qui peut aboutir à des violations des droits de l'homme ou à des atteintes à ces droits, notamment le droit à la vie privée, et est donc un motif de préoccupation croissante,

Notant également que les violations du droit à la vie privée à l'ère du numérique et les atteintes à ce droit peuvent toucher tout un chacun et avoir des conséquences particulières pour les femmes, ainsi que pour les enfants, les personnes handicapées et les personnes vulnérables et marginalisées,

Estimant que les gouvernements, le secteur privé, les organisations internationales, la société civile, les milieux techniques et universitaires et tous les acteurs concernés doivent avoir conscience des conséquences de l'évolution technologique rapide pour la promotion et la protection des droits de l'homme, des perspectives qu'elle offre et des difficultés qu'elle représente, ainsi que du potentiel qu'elle a de contribuer aux efforts, d'accélérer le progrès humain et de promouvoir et protéger les droits de l'homme et les libertés fondamentales,

Constatant que l'utilisation de l'intelligence artificielle peut contribuer à la promotion et à la protection des droits de l'homme et qu'elle peut aussi avoir des répercussions mondiales de portée considérable, y compris en ce qui concerne le droit à la vie privée, qui sont en train de transformer les gouvernements et les sociétés, les secteurs économiques et le monde du travail,

Conscient du fait que, malgré ses effets positifs, l'utilisation de l'intelligence artificielle, qui nécessite le traitement d'importants volumes de données, souvent personnelles, y compris des données sur le comportement, les relations sociales, les préférences personnelles et l'identité d'une personne, peut faire peser de graves risques sur le droit à la vie privée, en particulier lorsqu'elle est utilisée à des fins d'identification, de localisation, de profilage, de reconnaissance faciale, de prédiction des comportements ou d'évaluation des individus,

Notant que, s'il n'existe pas de garanties adéquates, l'utilisation de l'intelligence artificielle risque de renforcer la discrimination, y compris les inégalités structurelles,

Reconnaissant que si les métadonnées peuvent apporter des avantages, certains types de métadonnées peuvent aussi, par agrégation, révéler des informations personnelles tout aussi sensibles que le contenu même des communications et donner des indications sur le comportement, les relations sociales, les préférences personnelles et l'identité de particuliers,

Notant avec préoccupation que le traitement automatisé de données personnelles à des fins de profilage, de prise de décisions automatisée et d'apprentissage automatique peut, s'il n'existe pas de garanties adéquates, conduire à une discrimination ou à des décisions susceptibles d'affecter la jouissance des droits de l'homme, y compris des droits économiques, sociaux et culturels, et reconnaissant la nécessité d'appliquer le droit international des droits de l'homme à la conception, au développement, au déploiement, à l'évaluation et à la régulation de ces technologies et d'en assurer une protection et un contrôle adéquats,

Constatant avec inquiétude que souvent, les personnes ne donnent pas ou ne peuvent pas donner leur consentement libre, exprès et éclairé à la collecte, au traitement et au stockage ou à la réutilisation, la vente et la revente de leurs données personnelles, eu égard au fait que la collecte, le traitement, l'utilisation, le stockage et l'échange des informations personnelles, y compris d'informations sensibles, se sont beaucoup développés à l'ère du numérique,

Soulignant que la surveillance et l'interception illicites ou arbitraires des communications et la collecte illicite ou arbitraire de données personnelles ou le piratage illicite ou arbitraire et l'utilisation illicite ou arbitraire des technologies biométriques sont des activités éminemment intrusives qui constituent une violation du droit à la vie privée ou une atteinte à ce droit, sont susceptibles de porter atteinte à d'autres droits, notamment le droit à la liberté d'expression et le droit de ne pas être inquiété pour ses opinions, ainsi que le droit à la liberté de réunion et d'association pacifiques, et peuvent être contraires aux principes d'une société démocratique, notamment lorsqu'elles sont pratiquées en dehors du territoire national ou à grande échelle,

Soulignant également que les États doivent s'acquitter de leurs obligations internationales en matière de droits de l'homme relatives au droit à la vie privée lorsqu'ils interceptent des communications numériques de particuliers ou collectent des données personnelles et lorsqu'ils font jouer, entre autres, des accords d'échange de renseignements pour échanger des données ou autoriser l'accès aux données qu'ils ont collectées et lorsqu'ils demandent à des tiers, y compris à des entreprises, de communiquer des données personnelles,

Constatant l'intensification de la collecte de données biométriques sensibles auprès de particuliers et soulignant que les États doivent respecter leurs obligations en matière de droits de l'homme et que les entreprises devraient respecter le droit à la vie privée et les autres droits de l'homme lorsqu'elles collectent, traitent, échangent et stockent les données biométriques, notamment en adoptant des mesures de protection et des garde-fous,

Constatant également que, si la prévention et la répression du terrorisme et de l'extrémisme violent pouvant conduire au terrorisme constituent un intérêt public d'une grande importance et si des préoccupations relatives à la sécurité publique peuvent justifier la collecte et la protection de certaines données confidentielles, les États doivent s'acquitter pleinement des obligations que leur impose le droit international des droits de l'homme,

Soulignant que, à l'ère du numérique, il peut être important d'avoir recours à des solutions techniques pour protéger la confidentialité des communications numériques, dont les techniques de chiffrement, de pseudonymisation et d'anonymisation, pour garantir l'exercice des droits de l'homme, en particulier le droit à la vie privée, le droit à la liberté d'expression et le droit de réunion pacifique et de libre association, et estimant que les États doivent s'abstenir de recourir à des techniques de surveillance illicites ou arbitraires,

1. *Réaffirme* le droit à la vie privée, en vertu duquel nul ne peut être l'objet d'immixtions arbitraires ou illégales en lien avec son domicile ou sa correspondance ou dans sa vie privée et sa vie familiale, et le droit à la protection de la loi contre de telles immixtions, tels qu'ils sont définis à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques ;

2. *Rappelle* que les États devraient veiller à ce que toute immixtion dans la vie privée soit conforme aux principes de légalité, de nécessité et de proportionnalité ;

3. *Considère* que le caractère mondial et ouvert d'Internet et la rapidité des progrès accomplis dans le domaine des technologies de l'information et de la communication jouent un rôle prépondérant dans l'accélération de la réalisation du développement sous toutes ses formes, notamment la réalisation des objectifs de développement durable ;

4. *Affirme* que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, y compris le droit à la vie privée ;

5. *Constate* que l'utilisation, le déploiement et le développement des technologies naissantes et de technologies nouvelles telles que l'intelligence artificielle, peuvent avoir des incidences sur l'exercice du droit à la vie privée et d'autres droits de l'homme, et que les risques qui pèsent sur le droit à la vie privée peuvent et doivent être réduits au minimum en adoptant une réglementation adéquate ou d'autres mécanismes appropriés, y compris en tenant compte du droit international des droits de l'homme dans la conception, le développement et le déploiement des technologies naissantes et des technologies nouvelles telles que l'intelligence artificielle, en garantissant des infrastructures des données de qualité, sûres et sécurisées, et en créant des mécanismes de contrôle axés sur l'humain ainsi que des mécanismes de réparation ;

6. *Demande* à tous les États :

a) De respecter et de protéger le droit à la vie privée, y compris dans le cadre des communications numériques ;

b) De prendre des mesures pour mettre fin aux violations du droit à la vie privée et aux atteintes à ce droit et de créer les conditions permettant de prévenir ce type de violations et d'atteintes, y compris en veillant à ce que la législation nationale pertinente soit conforme aux obligations que leur impose le droit international des droits de l'homme ;

c) De revoir régulièrement leurs procédures, leurs pratiques et leur législation en ce qui concerne la surveillance des communications, y compris la surveillance à grande échelle et l'interception et la collecte de données personnelles, ainsi que l'utilisation du profilage, de la prise de décisions automatisée, de l'apprentissage automatique et des technologies biométriques, dans le souci de défendre le droit à la vie privée en respectant pleinement et effectivement toutes leurs obligations au regard du droit international des droits de l'homme ;

d) De faire en sorte que toute mesure prise dans le cadre de la lutte contre le terrorisme et l'extrémisme violent pouvant conduire au terrorisme qui porte atteinte au droit à la vie privée soit conforme aux principes de légalité, de nécessité et de proportionnalité et aux obligations qui leur incombent en vertu du droit international ;

e) De mettre ou de maintenir en place des mécanismes nationaux de contrôle judiciaire, administratif ou parlementaire indépendants, effectifs, impartiaux, dotés de moyens suffisants et pouvant garantir la transparence, selon qu'il convient, et la responsabilité des États au regard de la surveillance et de l'interception des communications et de la collecte de données personnelles ;

f) D'élaborer ou de maintenir, et d'appliquer, une législation adaptée prévoyant des sanctions et des voies de recours effectives, en vue de protéger les personnes contre les violations du droit à la vie privée et des atteintes à ce droit, notamment celles résultant de la collecte, du traitement, de la conservation et de l'utilisation illicites et arbitraires de données à caractère personnel par des particuliers, des administrations publiques, des entreprises ou des organismes privés ;

g) D'envisager l'adoption ou la révision de la législation, des règlements ou des politiques pour faire en sorte que les entreprises tiennent pleinement compte du droit au respect de la vie privée et d'autres droits de l'homme dans la conception, la mise au point, le déploiement et l'évaluation des technologies, y compris de l'intelligence artificielle, et de permettre aux personnes dont les droits peuvent avoir été violés ou auxquels il peut avoir été porté atteinte d'accéder à des voies de recours effectives, y compris des réparations et des garanties de non-répétition ;

h) De renforcer ou de maintenir les mesures préventives et les voies de recours existant contre les violations du droit à la vie privée à l'ère du numérique et les atteintes à ce droit pouvant toucher toutes les personnes, notamment lorsqu'elles ont des conséquences particulières pour les femmes, ainsi que pour les enfants et les personnes vulnérables et marginalisées ;

i) De promouvoir une éducation de qualité et des possibilités de formation permanente pour tous afin de favoriser, notamment, l'acquisition des connaissances informatiques et des compétences techniques nécessaires à la protection effective de la vie privée ;

j) De s'abstenir de demander aux entreprises de prendre des mesures qui portent atteinte au droit à la vie privée de façon arbitraire et illicite, et de protéger les personnes contre le tort qui pourrait leur être fait, y compris par les entreprises, du fait de la collecte, du traitement, du stockage et de l'échange de données et de l'utilisation du profilage, de processus automatisés et de l'apprentissage automatique ;

k) D'envisager de prendre des dispositions permettant aux entreprises d'adopter volontairement des mesures de transparence appropriées s'agissant des demandes d'accès aux données et informations des utilisateurs privés émanant des autorités publiques ;

l) D'élaborer ou maintenir des lois, des mesures préventives et des voies de recours contre le tort causé par le traitement, l'utilisation, la vente ou la revente ou tout autre partage entre les entreprises de données personnelles, sans le consentement libre, exprès et éclairé des intéressés ;

m) De prendre les mesures appropriées pour garantir que la conception, la mise en œuvre et l'exploitation des programmes d'identification numérique ou biométrique s'accompagnent des garanties juridiques et techniques appropriées et se déroulent dans le plein respect du droit international des droits de l'homme ;

7. *Encourage* tous les États à faire en sorte que les technologies de l'information et de la communication s'inscrivent dans un environnement ouvert, sûr, stable, accessible et pacifique, fondé sur le respect du droit international, y compris les obligations inscrites dans la Charte des Nations Unies et les instruments internationaux relatifs aux droits de l'homme ;

8. *Encourage* toutes les entreprises, en particulier les entreprises qui collectent, stockent, utilisent, partagent et traitent des données :

a) À s'acquitter de l'obligation qui leur incombe de respecter les droits de l'homme, comme le prévoient les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « Protéger, respecter et réparer » des Nations Unies, y compris le droit à la vie privée à l'ère du numérique ;

b) À informer les utilisateurs des pratiques de collecte, d'utilisation, de partage et de conservation des données de nature à porter atteinte à leur droit à la vie privée, et de mettre en place des politiques de transparence qui prévoient le consentement éclairé des utilisateurs, selon qu'il convient ;

c) À mettre en place des garanties administratives et des mesures de protection technique et physique pour veiller à ce que les données soient traitées de manière licite et à ce que le traitement soit nécessaire aux fins des objectifs visés, et pour garantir la légalité de ces objectifs, et l'exactitude, l'intégrité et la confidentialité du traitement des données ;

d) À veiller à ce que les personnes aient accès à leurs données et qu'elles aient la possibilité de les modifier, les corriger, les mettre à jour et les effacer, en particulier si les données sont fausses ou inexactes ou si elles ont été obtenues par des moyens illicites ;

e) À veiller à ce que le respect du droit à la vie privée et d'autres droits de l'homme pertinents soit pris en compte dans la conception, l'utilisation, l'évaluation et la réglementation des programmes informatiques d'aide à la décision et de l'apprentissage automatique, et de prévoir d'accorder des réparations pour les atteintes aux droits de l'homme qui leur sont imputables ou auxquelles elles ont contribué ;

f) À mettre en place des garanties adéquates en vue de prévenir ou d'atténuer les incidences négatives sur les droits de l'homme qui sont directement liées à leurs activités, produits ou services, y compris, le cas échéant, au moyen de clauses contractuelles, et à informer rapidement les organes de surveillance nationaux, régionaux ou internationaux compétents des atteintes ou des violations dans le cas où une utilisation abusive de leurs produits et services est constatée ;

9. *Encourage* les entreprises à mettre en œuvre des solutions techniques permettant de garantir et de préserver la confidentialité des communications numériques, notamment des techniques de chiffrement et d'anonymisation, et demande aux États de ne pas s'ingérer dans l'utilisation de telles solutions et de n'imposer d'autres restrictions que celles qui sont conformes aux obligations mises à leur charge par le droit international des droits de l'homme ;

10. *Prie* la Haute-Commissaire des Nations Unies aux droits de l'homme d'organiser, avant la quarante-quatrième session du Conseil des droits de l'homme, un séminaire d'experts d'une journée pour examiner les incidences que l'intelligence artificielle, y compris le profilage, la prise de décisions automatisée et l'apprentissage automatique, si elle n'est pas accompagnée des garanties appropriées, peut avoir sur l'exercice du droit à la vie privée, d'établir un rapport thématique sur cette question et de le soumettre au Conseil à sa quarante-cinquième session ;

11. *Encourage* les États, les organismes, fonds et programmes des Nations Unies concernés, les organisations intergouvernementales, les organes conventionnels, les titulaires de mandat au titre des procédures spéciales, les mécanismes régionaux de défense des droits de l'homme, les organisations de la société civile, les milieux universitaires, les institutions nationales des droits de l'homme, les entreprises, la communauté technique et d'autres acteurs intéressés à participer activement au séminaire d'experts ;

12. *Décide* de poursuivre l'examen de cette question au titre du même point de l'ordre du jour.

39^e séance
26 septembre 2019

[Adoptée sans vote]
