Nations Unies A/HRC/RES/54/21

Assemblée générale

Distr. générale
16 octobre 2023
Français
Original : anglais

Conseil des droits de l'homme
Cinquante-quatrième session
11 septembre-13 octobre 2023
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Résolution adoptée par le Conseil des droits de l'homme le 12 octobre 2023

54/21. 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 consacrés par 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 et les autres instruments internationaux pertinents relatifs aux droits de l'homme,

Rappelant toutes les résolutions sur le droit à la vie privée à l'ère numérique ainsi que les autres résolutions pertinentes précédemment adoptées par l'Assemblée générale et par lui-même,

Saluant les travaux du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère numérique, et saluant également les travaux de plusieurs titulaires de mandat au titre de ses procédures spéciales sur le droit à la vie privée et leurs contributions à la promotion et à la protection du droit à la vie privée,

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 pacifique et d'association, et qu'il est l'un des fondements d'une société démocratique,

Sachant que le droit à la vie privée est intrinsèquement lié à la protection effective des données personnelles de chaque individu,

Sachant également que le droit à la vie privée peut permettre l'exercice d'autres droits et le libre développement de la personnalité et de l'identité de l'individu, et qu'il peut donner à chacun la possibilité de participer à la vie politique, économique, sociale et culturelle,

Réaffirmant qu'il faut également protéger en ligne les droits dont toute personne jouit hors ligne, notamment le droit à la vie privée, et notant que la synchronisation accélérée des espaces en ligne et hors ligne peut avoir des conséquences pour les individus, notamment pour l'exercice de leur droit à la vie privée,

Notant que les processus décisionnels algorithmiques ou automatisés en ligne peuvent nuire à la jouissance des droits de la personne hors ligne,

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 internes et aux incidences de la surveillance sur l'exercice du 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, et d'examiner les potentiels effets discriminatoires,

Notant que le rythme soutenu des avancées technologiques, qui permet à chacun, partout dans le monde, d'utiliser les technologies de l'information et des communications, 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 constitue donc un motif de préoccupation croissante,

Notant également qu'à l'ère du numérique, les violations du droit à la vie privée et les atteintes à ce droit peuvent toucher tout un chacun et avoir des conséquences particulières pour les femmes, les enfants, les personnes handicapées et les personnes âgées, ainsi que pour les personnes en situation de vulnérabilité et les groupes marginalisés, et que le traitement des données personnelles, en particulier les données des personnes en situation de vulnérabilité, doit faire l'objet de garanties et de restrictions visant à protéger les droits de l'homme,

Notant en outre que les femmes et les filles font l'objet de violations du droit à la vie privée et d'atteintes à ce droit qui sont fondées sur le genre, en ligne comme hors ligne, ainsi que de violations ou d'atteintes qui ont des répercussions particulières selon le genre, et conscient que la manière dont de nombreuses plateformes numériques sont conçues, commercialisées, gérées et régies peut donner lieu à la désinformation, à la mésinformation et à des discours haineux, qui peuvent exacerber les stéréotypes de genre, entraîner des actes de violence sexuelle et fondée sur le genre et nuire à la protection des données et à la réalisation de tous les droits des femmes et des filles, en particulier leur droit à la vie privée,

Notant que les enfants peuvent être particulièrement exposés aux violations du droit à la vie privée et aux atteintes à ce droit, notamment sous des formes telles que le cyberharcèlement, la traque en ligne et la violence et l'exploitation sexuelles, et notant également que les États parties à la Convention relative aux droits de l'enfant doivent en appliquer les dispositions à l'environnement numérique, notamment au regard de l'importance de la vie privée pour la capacité d'action, la dignité et la sécurité des enfants et pour l'exercice de leurs droits,

Sachant qu'il est nécessaire d'exercer une diligence raisonnable en matière de droits de l'homme lors de la conception, de l'élaboration, de l'utilisation, de l'acquisition, du transfert, de la vente, du déploiement et du développement ultérieur des technologies nouvelles et émergentes, telles que celles qui font appel à l'intelligence artificielle, car elles peuvent, en l'absence de garanties appropriées, avoir des répercussions sur l'exercice du droit à la vie privée et d'autres droits de l'homme, et considérant que l'on peut et doit écarter ou réduire au minimum le risque qu'il soit porté atteinte à ces droits, notamment en prenant des mesures pour garantir une infrastructure de données de haute qualité, qui soit sûre, transparente, responsable et sécurisée, en exerçant la diligence voulue et en examinant périodiquement les technologies déjà déployées pour évaluer, prévenir et atténuer les effets négatifs sur les droits de l'homme, en prévoyant des recours utiles, notamment judiciaires, et des mécanismes de réparation, et en instaurant des dispositifs de contrôle humain,

Conscient que, malgré ses effets positifs, l'utilisation des technologies numériques et de systèmes d'intelligence artificielle qui nécessitent le traitement d'importants volumes de données, souvent personnelles, notamment de données sur le comportement, les relations sociales, les préférences personnelles et l'identité d'une personne, y compris de métadonnées, peut faire peser de graves risques sur le droit à la vie privée, notamment lorsque

cette technologie est utilisée à des fins d'identification, de localisation, de profilage, de reconnaissance faciale, de prédiction des comportements ou d'évaluation des personnes,

Notant que l'utilisation de l'extraction des données et des algorithmes pour cibler le contenu en fonction des internautes peut porter atteinte au pouvoir d'action de ceux-ci et à l'accès à l'information en ligne, ainsi qu'au droit à la liberté d'opinion et d'expression, et peut entraîner une intensification des menaces liées à la mésinformation, à la désinformation et aux discours haineux, en particulier sur les plateformes de médias sociaux, qui peuvent conduire à la violence, y compris la violence politique, et rappelant à cet égard le Plan d'action de Rabat sur l'interdiction de l'appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence,

Notant avec préoccupation le caractère intrusif et l'incidence des pratiques de collecte de données, les effets et les torts causés par la surveillance, ainsi que l'utilisation croissante d'algorithmes dans le cadre de l'application des systèmes d'intelligence artificielle,

Notant également avec préoccupation que certains algorithmes prédictifs et l'utilisation croissante de la reconnaissance faciale et des technologies de surveillance peuvent être source de discrimination, en particulier lorsque les données utilisées pour l'apprentissage des algorithmes ne sont pas exactes, pertinentes et représentatives et que l'on n'a pas vérifié qu'elles ne sont pas fondées sur des préjugés,

Notant que, si aucune garantie relative aux droits de l'homme n'est prévue, l'utilisation de l'intelligence artificielle risque de renforcer la discrimination, y compris les inégalités structurelles, en particulier lorsque les données traitées sont des données sensibles, et conscient de la nécessité d'empêcher que la conception, l'élaboration, la mise en application et l'utilisation des technologies numériques nouvelles et émergentes aient des effets discriminatoires, notamment sur le plan racial,

Prenant note avec inquiétude des informations selon lesquelles l'identification fondée sur les données biométriques est moins précise, notamment lorsqu'elle s'appuie sur des technologies de reconnaissance faciale qui sont entachées de préjugés racistes et de préjugés à l'égard des femmes, notamment lorsque des données d'apprentissage non représentatives sont utilisées, relevant que l'utilisation des technologies numériques peut reproduire, renforcer et même exacerber les inégalités raciales et les inégalités de genre, et conscient, dans ce contexte, de l'importance des recours utiles,

Considérant 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, notamment les déplacements, les relations sociales, les activités politiques, les préférences personnelles et l'identité de particuliers, et rappelant à ce titre que les fournisseurs de services devraient prendre des mesures pour minimiser, masquer ou supprimer les métadonnées et pour réduire la traçabilité des métadonnées des utilisateurs afin de renforcer les protections offertes par le chiffrement et de protéger le droit à la vie privée,

Conscient que le manque d'accès à des technologies et services fiables à un coût abordable constitue un obstacle majeur dans de nombreux pays en développement, en particulier pour ce qui est de réduire la fracture numérique, tant entre les pays et à l'intérieur de ces derniers qu'entre femmes et hommes, et d'accélérer les progrès vers le développement sous ses diverses formes, y compris la réalisation des objectifs de développement durable, et soulignant à cet égard que de nombreux États, notamment des pays en développement, partout dans le monde, ont besoin d'aide pour réduire cette fracture numérique et pour atteindre les objectifs de développement durable,

Conscient également qu'il faut veiller à ce que le droit international des droits de l'homme soit respecté, notamment en menant des études d'impact sur les droits de l'homme, lors de la conception, de l'élaboration, du développement, du déploiement, de l'évaluation, de la réglementation et de la normalisation des technologies fondées sur les données, et à ce que ces technologies soient assorties des garanties nécessaires et soumises à un contrôle adéquat,

Constatant avec inquiétude que souvent, les personnes, en particulier les enfants, ne donnent pas ou ne peuvent pas donner expressément leur consentement libre et éclairé à la collecte, au traitement et au stockage ou à la réutilisation, à la vente et à 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, et que la divulgation de données personnelles et sensibles peut causer des dommages, un traumatisme ou des difficultés exceptionnels aux personnes concernées,

Notant en particulier que la surveillance des communications numériques doit être conforme aux obligations internationales relatives aux droits de l'homme et reposer sur un cadre juridique accessible à tous, clair, précis, complet et non discriminatoire, et que toute immixtion dans la vie privée doit être conforme aux principes de légalité, de nécessité et de proportionnalité, en ayant à l'esprit ce qui est raisonnable au regard des objectifs légitimes poursuivis, et rappelant que les États parties au Pacte international relatif aux droits civils et politiques doivent faire le nécessaire pour adopter, selon qu'il convient, des mesures d'ordre législatif ou autre propres à donner effet aux droits reconnus dans le Pacte,

Notant avec une profonde inquiétude que, dans de nombreux pays, il est fréquent que les personnes et les organisations qui œuvrent à la promotion et à la défense des droits de l'homme et des libertés fondamentales, les journalistes et les autres professionnels des médias fassent l'objet de menaces et de harcèlement, se trouvent en situation d'insécurité ou soient l'objet d'immixtions arbitraires ou illégales dans leur vie privée en raison de leurs activités,

Notant également avec une profonde inquiétude que des outils technologiques créés par l'industrie de la surveillance privée sont utilisés par des acteurs privés ou publics pour exercer des activités de surveillance, pirater des dispositifs et des systèmes, notamment au moyen de logiciels malveillants et de logiciels espions, intercepter et perturber des communications et recueillir des données, ce qui constitue une immixtion dans la vie professionnelle et privée de particuliers, notamment de personnes qui œuvrent à la promotion et à la défense des droits de l'homme et des libertés fondamentales, de journalistes et d'autres professionnels des médias, ainsi qu'une violation des droits de l'homme de ces personnes ou une atteinte à leurs droits, en particulier leur droit à la vie privée,

Rappelant que les entreprises, notamment les entreprises technologiques, sont tenues de respecter les droits de l'homme, comme le prévoient les principes intitulés « 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, et saluant les travaux du Haut-Commissariat des Nations Unies aux droits de l'homme sur l'application de ces principes aux technologies numériques,

Soulignant que, à l'ère du numérique, il est important d'avoir recours à des solutions techniques pour protéger la confidentialité des communications numériques, notamment à des techniques de chiffrement, de pseudonymisation et d'anonymisation, pour garantir l'exercice des droits de l'homme, notamment le droit à la vie privée, le droit à la liberté d'opinion et d'expression et le droit à la liberté de réunion pacifique et d'association, et estimant que les États doivent promouvoir de telles mesures et s'abstenir de recourir à des techniques de surveillance illicites ou arbitraires, y compris à des formes de piratage et à des restrictions d'accès aux technologies de chiffrement à l'utilisation de celles-ci,

Soulignant également qu'il convient de veiller à ce que les mesures de sécurité nationale et de santé publique, y compris l'utilisation de la technologie aux fins du suivi et de l'endiguement de la propagation de maladies infectieuses, soient pleinement conformes aux obligations qui incombent aux États, au regard du droit international des droits de l'homme, et respectent les principes de licéité, de légalité et de légitimité du but poursuivi, de nécessité et de proportionnalité, ainsi que l'obligation de protéger les droits de l'homme, notamment le droit à la vie privée, et les données personnelles dans les réponses aux situations d'urgence sanitaire et autres crises, et soulignant en outre qu'il convient de supprimer ou d'anonymiser les données recueillies lorsqu'elles ne sont plus utilisées aux fins pour lesquelles elles ont été collectées,

1. *Réaffirme* le droit à la vie privée, en vertu duquel nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, et le droit à la protection de la loi contre de telles immixtions, consacrés par l'article 12 de la Déclaration universelle des droits de l'homme et par 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 l'exercice du droit à la vie privée respecte les principes de légalité, de nécessité et de proportionnalité ;

3. *Rappelle également* qu'en l'absence de garanties en matière de droits de l'homme, les technologies nouvelles et émergentes, telles que celles qui sont développées dans les domaines de la surveillance, de l'intelligence artificielle, de la prise de décisions automatisée, de l'apprentissage automatique, du profilage, du suivi et de la biométrie, notamment la reconnaissance faciale, ont de plus en plus d'incidences sur le plein exercice du droit à la vie privée et d'autres droits de l'homme, et relève que certaines applications peuvent ne pas être compatibles avec le droit international des droits de l'homme ;

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. *Affirme également* que, pour protéger, respecter et promouvoir le droit à la vie privée, il convient de ne collecter des données personnelles qu'à des fins déterminées, explicites et légitimes, et de les traiter de manière légale, équitable et transparente ;

6. *Souligne* que toute personne devrait être en mesure de déterminer quelles autorités publiques ou quels particuliers ou organismes privés contrôlent ou peuvent contrôler ses données personnelles, et que toute immixtion dans la protection des données doit être légale et conforme au droit international des droits de l'homme, notamment aux principes de légalité, de proportionnalité, de nécessité et de non-discrimination ;

7. *Considère* que l'on peut et que l'on doit réduire au minimum les risques qui pèsent sur le droit à la vie privée et les autres droits de l'homme en adoptant des réglementations adéquates ou en instaurant d'autres mécanismes appropriés, conformément aux obligations édictées à cet égard par le droit international des droits de l'homme pour la conception, l'élaboration, l'utilisation, l'acquisition, le transfert, la vente, le déploiement et le développement de technologies numériques nouvelles et émergentes, telles que l'intelligence artificielle, en garantissant une infrastructure de données de haute qualité, qui soit sûre et sécurisée, en exerçant la diligence voulue pour évaluer, prévenir et atténuer les effets négatifs sur les droits de l'homme, et en instaurant des dispositifs de contrôle humain, ainsi que des mécanismes de réparation ;

8. *Souligne* que les États doivent respecter leurs obligations en matière de droits de l'homme et que les entreprises, y compris les entreprises technologiques, doivent respecter le droit à la vie privée et les autres droits de l'homme lorsqu'elles collectent, traitent, partagent et stockent des données personnelles, notamment en adoptant des politiques de protection des données et des mesures de sauvegarde ;

9. *Souligne également* que les systèmes de télésurveillance biométrique, notamment les systèmes de reconnaissance faciale, soulèvent de sérieuses inquiétudes quant à leur proportionnalité, étant donné leur nature hautement intrusive et leurs vastes répercussions pour un grand nombre de personnes ;

10. *Demande* à tous les États :

a) De respecter et protéger le droit à la vie privée, y compris dans le contexte des communications numériques et des technologies numériques nouvelles et émergentes ;

b) De prendre des mesures pour mettre fin aux violations du droit à la vie privée et aux atteintes à ce droit et 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, en particulier en ce qui concerne les personnes en situation de vulnérabilité ou les groupes marginalisés ;

c) De revoir régulièrement leurs procédures, leurs pratiques et leur législation relatives à la surveillance des communications, y compris la surveillance à grande échelle et l'interception et la collecte de données personnelles, ainsi qu'au recours au profilage, à la prise de décisions automatisée, à l'apprentissage automatique et aux 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 s'acquitter de leurs obligations internationales en matière de droits de l'homme, notamment celles relatives au droit à la vie privée, lorsqu'ils interceptent des communications numériques de particuliers ou collectent des données personnelles, lorsqu'ils échangent des données ou donnent accès à des données collectées dans le cadre d'accords d'échange d'informations et de renseignements et lorsqu'ils imposent à des tiers, notamment à des entreprises, de communiquer des données personnelles ;

e) 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 au regard du droit international ;

f) De veiller à ce que les technologies d'identification et de reconnaissance biométriques, y compris les technologies de reconnaissance faciale, utilisées par des acteurs publics et privés, ne permettent pas une surveillance arbitraire ou illégale, notamment des personnes exerçant leur droit à la liberté de réunion pacifique ;

g) De faire en sorte que la conception, l'exécution et l'exploitation des programmes d'identification numérique ou biométrique soient conditionnées par la mise en place préalable de garanties techniques, réglementaires, légales et éthiques appropriés et se déroulent dans le plein respect des obligations qui incombent aux États au regard du droit international des droits de l'homme ;

h) D'élaborer ou de conserver, et d'appliquer, une législation adaptée, qui prévoie des sanctions et des voies de recours effectives, en vue de protéger les personnes contre les violations du droit à la vie privée et les atteintes à ce droit, notamment celles résultant de la collecte, du traitement, de la conservation ou de l'utilisation de données personnelles, par des particuliers, des administrations publiques, des entreprises ou des organismes privés, par des moyens licites mais sans le consentement libre, exprès et éclairé des intéressés, conformément au droit international des droits de l'homme ;

i) D'envisager d'adopter ou de conserver des lois, des règlements et des politiques de protection des données, y compris celles relatives aux communications numériques, qui soient conformes à leurs obligations internationales en matière de droits de l'homme, notamment des dispositions relatives à la protection des données personnelles sensibles et à la mise en place des autorités nationales indépendantes dotées de l'autorité et des moyens nécessaires pour assurer le suivi des pratiques en ce qui concerne la confidentialité des données, enquêter sur les violations et les atteintes et recevoir des communications émanant de particuliers ou d'organismes, et d'offrir des voies de recours efficaces adéquates ;

j) D'envisager d'adopter ou de réviser des lois, des règlements ou des politiques pour faire en sorte que toutes les entreprises, notamment les entreprises de réseaux sociaux et autres plateformes en ligne, tiennent pleinement compte du droit à la vie privée et des autres droits de l'homme lorsqu'ils conçoivent, mettent au point, déploient et évaluent des technologies, y compris l'intelligence artificielle, de prendre les mesures appropriées pour améliorer et favoriser le respect, par les entreprises, du principe de responsabilité et de permettre aux personnes qui ont pu être victimes de violations de leurs droits ou d'atteintes à ces droits d'accéder à des voies de recours efficaces, notamment d'obtenir une réparation et des garanties de non-répétition ;

k) De renforcer ou conserver, à cet égard, les mesures préventives et les voies de recours contre les violations du droit à la vie privée et les atteintes à ce droit qui, à l'ère du numérique, pourraient toucher chaque personne, y compris lorsqu'elles ont des conséquences particulières pour les femmes, les enfants, les personnes en situation de vulnérabilité ou les groupes marginalisés ;

l) D'élaborer, d'examiner, d'appliquer et de renforcer des politiques et des programmes tenant compte des questions de genre qui contribuent à l'autonomisation de toutes les femmes et de toutes les filles et qui promeuvent et protègent le droit de tous à la vie privée à l'ère du numérique ;

m) De donner aux entreprises des orientations efficaces et actualisées en ce qui concerne le respect des droits de l'homme, y compris des conseils sur les méthodes à employer, notamment sur la diligence voulue en matière de droits de l'homme, et la manière de tenir effectivement compte des questions liées au genre, à la vulnérabilité ou à la marginalisation, et 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 ;

n) De s'abstenir d'utiliser les technologies de surveillance d'une manière qui ne soit pas conforme aux obligations internationales relatives aux droits de l'homme, notamment à l'égard de défenseurs des droits de l'homme, de journalistes et d'autres professionnels des médias, et de prendre des mesures concrètes aux fins de la protection contre les violations du droit à la vie privée, notamment de réglementer la vente, le transfert, l'utilisation et l'exportation des technologies de surveillance ;

o) De promouvoir une éducation de qualité accessible et inclusive et des possibilités d'apprentissage tout au long de la vie pour tous afin de favoriser, entre autres, l'acquisition d'une culture du numérique et des données et de compétences techniques, notamment en offrant une formation, des conseils et des activités de sensibilisation à la sécurité en ligne, qui sont nécessaires pour protéger efficacement la vie privée, et de garantir l'accès des parties prenantes à une formation appropriée dans ce domaine ;

p) De s'abstenir d'imposer 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 ;

q) De redoubler d'efforts pour lutter contre la discrimination résultant de l'utilisation de systèmes d'intelligence artificielle, notamment en exerçant la diligence voulue pour évaluer, prévenir et atténuer les effets négatifs du déploiement de ces systèmes sur les droits de l'homme ;

11. *Engage* toutes les entreprises, en particulier les entreprises qui collectent, stockent, utilisent, échangent et traitent des données :

a) À revoir leurs modèles d'entreprise et à s'assurer que leurs processus de conception et de développement, leurs opérations commerciales, leurs pratiques de collecte et de traitement des données sont conformes aux principes intitulés « 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 à souligner l'importance d'exercer une diligence raisonnable en matière de droits de l'homme en ce qui concerne leurs produits, en particulier s'agissant du rôle des algorithmes et des systèmes de classement ;

b) À informer les utilisateurs, d'une manière claire et adaptée à leur âge, et qui soit aisément accessible, notamment aux personnes handicapés, 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, à ne pas collecter, utiliser, partager ni conserver ces données sans le consentement des intéressés ou en l'absence d'un fondement juridique, à garantir la transparence et à appliquer des politiques qui prévoient le consentement libre, éclairé et véritable des utilisateurs ;

c) À prendre en considération le droit à la vie privée et les autres droits de l'homme pertinents dans le cadre de l'élaboration des politiques internes, de l'ingénierie des entreprises, du développement des activités, de la formation du personnel et des autres processus internes pertinents ;

d) 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 que le traitement soit nécessaire aux fins des objectifs visés, et pour garantir le bien-fondé de ces objectifs ainsi que l'exactitude, l'intégrité et la confidentialité du traitement des données, et à prévenir la divulgation ou l'utilisation des données sans autorisation ;

e) À veiller à ce que les personnes aient accès à leurs données et aient la possibilité de les modifier, de les corriger, de les mettre à jour, de les effacer et de retirer leur consentement à leur utilisation, en particulier si ces données sont fausses ou inexactes ou si elles ont été obtenues par des moyens illicites ou utilisées à des fins discriminatoires ;

f) 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'exploitation, l'évaluation et la réglementation des technologies de prise de décisions automatisée et d'apprentissage automatique, et à prévoir des mesures de réparation effectives, notamment une indemnisation, pour les atteintes aux droits de l'homme qui leur sont imputables ou auxquelles elles ont contribué ou ont été liées ;

g) 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 ;

h) À redoubler d'efforts pour lutter contre la discrimination résultant de l'utilisation de systèmes d'intelligence artificielle, et notamment à exercer la diligence voulue en matière de droits de l'homme et à surveiller et évaluer les systèmes d'intelligence artificielle tout au long de leur cycle de vie, ainsi que l'incidence du déploiement de ces systèmes sur les droits de l'homme ;

i) À promouvoir la transparence et l'explicabilité du processus décisionnel algorithmique, des systèmes automatisés et des systèmes fondés sur l'approche de l'humain dans la boucle (« human-in-the-loop »), et à veiller à ce que les données utilisées pour l'apprentissage des algorithmes soient représentatives et recueillies de manière légale ;

j) À mettre en place des mesures de sauvegarde appropriées pour garantir que la distribution et le transfert de données au sein des organisations et entre elles et la restructuration des données, y compris au moyen de l'informatique en nuage, des ensembles de données non structurées, de la technologie de la chaîne de blocs, de la réalité augmentée et de l'Internet des objets, sont compatibles avec la protection des données et le droit au respect de la vie privée ;

k) À prendre des mesures appropriées tout au long du cycle de vie des systèmes d'intelligence artificielle et des technologies numériques, y compris avant de commencer la conception et le développement d'applications et de logiciels qui impliquent le traitement de données personnelles, en vue de mettre en place un système de surveillance et de gestion des risques pour garantir que les données sont traitées en toute impartialité et dans le respect de la légalité ;

12. *Engage* les entreprises, notamment les fournisseurs de services de communication, à favoriser la mise en place de solutions techniques permettant de garantir et de préserver la confidentialité des communications et des transactions numériques, notamment des techniques de chiffrement, de pseudonymisation et d'anonymisation, et à veiller à ce que des garanties conformes aux droits de l'homme soient mises en place, et demande aux États de promouvoir l'utilisation de mesures et de solutions techniques de chiffrement, de pseudonymisation et d'anonymisation poussés, de ne pas entraver 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, ainsi que d'adopter des politiques qui protègent la confidentialité des communications numériques des particuliers ;

13. *Engage* les États et, le cas échéant, les entreprises à exercer systématiquement la diligence voulue en matière de droits de l'homme tout au long du cycle de vie des systèmes d'intelligence artificielle qu'ils conceptualisent, conçoivent, mettent au point, mettent en service ou vendent ou obtiennent et exploitent, notamment en effectuant de manière périodique et exhaustive des études d'impact sur les droits de l'homme et en faisant participer toutes les parties concernées ;

14. *Engage* toutes les parties concernées à prendre en compte systématiquement les questions de genre dans la conceptualisation, la mise au point et le déploiement des technologies numériques et des politiques y relatives, et à promouvoir la participation des femmes afin de lutter contre la violence et la discrimination à l'égard de toutes les femmes et toutes les filles qui découlent de l'utilisation de la technologie ou sont amplifiées par la technologie, notamment en encourageant les entreprises du numérique, y compris les fournisseurs d'accès à Internet, à respecter les normes établies et à mettre en place des dispositifs de signalement transparents et accessibles ;

15. *Prie* le Haut-Commissariat des Nations Unies aux droits de l'homme d'établir un rapport sur les difficultés et les risques, sur le plan de la discrimination et des inégalités dans l'exercice du droit à la vie privée, associés à la collecte et au traitement de données, notamment ceux dont il est question dans la présente résolution, afin de mettre en évidence et d'expliciter les principes, les garanties et les meilleures pratiques en matière de droits de l'homme qui s'y rapportent, et de lui soumettre ce rapport à sa cinquante-septième session, avant la tenue d'un dialogue sur la question ;

16. *Prie également* le Haut-Commissariat de solliciter, lorsqu'il établira le rapport susmentionné la contribution d'acteurs concernés de diverses régions géographiques, notamment des États, des organisations internationales et régionales, des titulaires de mandat au titre des procédures spéciales, des organes conventionnels et des autres bureaux, organismes, fonds et programmes des Nations Unies compétents, dans le cadre de leurs mandats respectifs, des institutions nationales des droits de l'homme, de la société civile, du secteur privé, des milieux techniques et des établissements universitaires, et de tenir compte des travaux déjà menés sur la question.

48e séance
12 octobre 2023

[Adoptée sans vote]