Nations Unies A/HRC/46/37

Assemblée générale

Distr. générale
25 janvier 2021
Français
Original : anglais

Conseil des droits de l'homme
Quarante-sixième session
22 février-19 mars 2021
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

Intelligence artificielle et respect de la vie privée, et respect de la vie privée des enfants

Rapport du Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci*, **

Résumé

Le présent rapport a été établi en application des résolutions 28/16 et 37/2 du Conseil des droits de l'homme. Le droit fondamental à la vie privée n'a jamais eu autant d'importance et n'a jamais été autant menacé. Comme cela apparaissait déjà en 2015, le progrès technologique a continué de faire toujours plus obstacle à l'exercice du droit à la vie privée. Le présent rapport, qui est le rapport final du premier Rapporteur spécial sur le droit à la vie privée, traite de deux problèmes distincts, à savoir, d'une part, l'intelligence artificielle et le respect de la vie privée, et, d'autre part, le respect de la vie privée des enfants, en particulier la façon dont le respect de la vie privée favorise l'autonomie et la participation active à la société. Des orientations et des recommandations visant à faire face à ces problèmes, élaborées dans le cadre de consultations et de travaux de recherche, sont présentées. S'ajoutant aux recommandations formulées par le Rapporteur spécial dans ses précédents rapports, le présent rapport complète le programme de travail soumis au Conseil des droits de l'homme en 2016 (A/HRC/31/64). Un aperçu des activités menées depuis 2015 par le Rapporteur spécial dans le cadre de son mandat figure dans les annexes.

* Il a été convenu que le présent rapport serait publié après la date normale de publication en raison de circonstances indépendantes de la volonté du soumetteur.

** Les annexes au présent rapport sont distribuées telles qu'elles ont été reçues, dans la langue de l'original seulement.

I. Recommandations relatives à la protection de la vie privée dans le contexte du développement et l'exploitation de solutions d'intelligence artificielle

Contexte et objet

1. Les présentes recommandations ont pour objet de fournir des principes directeurs relatifs à l'utilisation d'informations personnelles et non personnelles dans le contexte des solutions d'intelligence artificielle (« IA »)[1] développées dans le cadre des technologies de l'information et de la communication (TIC) appliquées, et de mettre en lumière l'importance, pour le traitement des données au moyen de l'IA par les gouvernements et les entreprises, d'une base légitime s'inscrivant dans le cadre général du droit à la vie privée.

2. Les recommandations sont fondées sur la Déclaration universelle des droits de l'homme et en reflètent l'esprit et l'interprétation. Les articles 7 (non-discrimination) et 12 (droit à protection de la vie privée), en particulier, sont essentiels en ce qui concerne le développement ou l'exploitation des solutions d'IA. Les thèmes et les valeurs qui sous-tendent ces dispositions sont énoncés aux articles 2 et 3 (non-discrimination) et à l'article 17 (vie privée) du Pacte international relatif aux droits civils et politiques et constituent des obligations pour les États qui ont ratifié cet instrument.

3. Les droits revêtent une importance cruciale dans la société de l'information. L'Assemblée générale et le Conseil des droits de l'homme ont confirmé que les droits des particuliers devaient être autant protégés en ligne que hors ligne (A/75/62-E/2020/11, par. 9) pour qu'Internet reste un réseau mondial, ouvert et interopérable (résolution 26/13 du Conseil des droits de l'homme) et soit un facteur d'accélération de la réalisation du développement sous ses diverses formes, et notamment celle des objectifs de développement durable (résolution 73/179 de l'Assemblée générale).

4. Les recommandations mettent l'accent sur le caractère confidentiel de toutes les données[2] qui sous-tendent les solutions d'IA. Elles ont vocation à servir de référence commune à l'échelle internationale pour l'établissement de normes de protection des données concernant les solutions d'IA, en particulier de normes qui seront appliquées au niveau national. Si les solutions d'IA présentent de nombreux avantages économiques et sociaux, il importe de protéger le droit à la vie privée dans ce contexte, et les présentes recommandations visent à fournir des points de repère à cet égard.

5. La mise en œuvre des recommandations nécessite une coopération étroite entre les gouvernements, la société civile, le secteur privé et les milieux techniques et universitaires et devrait s'appuyer sur des valeurs humaines communes comme l'inclusion, le respect, une approche centrée sur l'être humain, les droits de l'homme, le droit international, la transparence et la durabilité.

6. Les solutions d'IA comprennent l'application de systèmes destinés à orienter, prévoir ou prendre des décisions qui ont des incidences sur la vie de chacun. Elles présentent des avantages, mais ont aussi d'autres effets qui font actuellement débat au sein de la société. Ce débat − qui porte sur des questions morales, éthiques et sociétales concernant les droits de l'homme, tels que le droit à la vie privée, la non-discrimination et la libre participation − n'est

[1] Il existe plusieurs définitions de l'intelligence artificielle. Le sens retenu dans le présent rapport est le sens le plus courant, à savoir la définition donnée par *Oxford Reference* : « La théorie et le développement de systèmes informatiques capables d'exécuter des tâches qui nécessitent normalement l'intelligence humaine, comme la perception visuelle, la reconnaissance vocale, la prise de décisions et la traduction d'une langue à une autre ». Cette liste des domaines d'application des technologies fondées sur l'IA est loin d'être exhaustive.

[2] Le Rapporteur spécial, qui établit un lien entre la protection des données et le droit au respect de la vie privée consacré par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, envisage le droit relatif à la protection des données comme un sous-ensemble de la réglementation relative à la protection de la vie privée. Soulignant que l'histoire européenne a conduit à l'inclusion, dans la Charte des droits fondamentaux de l'Union européenne, d'un article distinct visant expressément la protection des données, il renvoie le lecteur aux références historiques pertinentes.

toujours pas clos. Pour toutes ces questions, il importe de garantir la licéité du traitement des données du point de vue du respect de la vie privée. Cela est d'autant plus nécessaire que la plupart des données sont détenues par des entreprises privées qui exploitent leur valeur commerciale en combinant divers ensembles de données afin d'en optimiser l'analyse. Il importe de répondre aux préoccupations croissantes du public concernant le caractère intrusif et les conséquences potentielles de la collecte de données, les risques de surveillance et l'utilisation croissante d'algorithmes reposant sur ces données et destinés à automatiser des décisions qui ont des effets sur la vie de chacun (A/75/62-E/2020/11, par. 10).

7. Le déploiement de l'intelligence artificielle doit s'accompagner de la mise en place d'un organisme efficace et indépendant de réglementation de la protection de la vie privée et des données qui soit chargé de contrôler le respect de la législation applicable.

Champ d'application

8. Les présentes recommandations s'appliquent au traitement des données utilisées par les solutions d'IA dans tous les secteurs de la société, et par le secteur privé comme par le secteur public. On entend par traitement des données chaque étape du cycle de vie d'une solution d'IA au cours de laquelle des données sont utilisées, à savoir la conception, le développement, le déploiement et la désactivation d'une solution d'IA, ainsi que toute nouvelle version ou refonte basée sur une solution d'IA précédente.

9. Les recommandations s'adressent à tous les gestionnaires de solutions d'IA. Il peut s'agir du concepteur, du développeur ou de l'exploitant (responsable à titre indépendant ou principal), dans le cadre de leurs fonctions propres. L'objectif est qu'au sein d'une organisation, une personne morale ou physique assume l'entière responsabilité de chaque solution d'IA.

10. Les présentes recommandations ne sauraient avoir pour effet de limiter ou de modifier d'une autre manière l'application des lois accordant davantage de droits, de protection ou de voies de recours aux sujets dont les données sont traitées. Elles ne limitent ni ne modifient d'une autre manière l'application des lois qui imposent aux gestionnaires et aux sous-traitants des obligations plus importantes, plus larges ou plus strictes concernant les aspects relatifs à la protection de la confidentialité des données.

11. Les recommandations ne s'appliquent pas aux solutions d'IA qui pourraient être utilisées par des particuliers dans le cadre d'activités purement privées ou domestiques.

Prise en compte des droits de l'homme et des aspects éthiques

12. Il incombe à la société de développer de façon éthique et responsable des solutions d'IA qui soient respectueuses des droits de l'homme. Les solutions d'IA, qui influencent profondément la vie privée et professionnelle, ont déjà des répercussions dans de nombreux domaines de la vie quotidienne et en auront de plus en plus à l'avenir. Il est probable que les futures solutions d'IA auront des conséquences pour un éventail plus large de principes fondamentaux qui relèvent du droit des droits de l'homme et de l'éthique. La manière dont cette technologie est utilisée revêt une importance cruciale.

13. La non-discrimination est essentielle pour éviter les inégalités, les injustices et les souffrances susceptibles d'avoir une incidence sur l'exercice des droits de l'homme, notamment les droits économiques, sociaux et culturels. L'utilisation de solutions d'IA doit être suivie de près et toutes les discriminations ou autres effets incompatibles avec les droits de l'homme doivent être corrigés pour éviter les conséquences négatives.

14. Les solutions d'IA ne devraient pas être utilisées pour prendre des décisions définitives ; elles devraient uniquement être envisagées comme une aide à la décision, par exemple dans le domaine judiciaire ou médical. Des études d'impact sur les droits de l'homme devraient toujours être réalisées parallèlement aux analyses de la protection des données afin d'offrir une vision globale des conditions d'encadrement nécessaires.

15. Actuellement, dans le monde entier, des comités comme le Comité ad hoc sur l'intelligence artificielle du Conseil de l'Europe œuvrent à l'élaboration de cadres réglementaires et de codes d'éthique applicables aux solutions d'IA. Il convient de s'y

référer, comme à d'autres lignes directrices telles que les Principes directeurs relatifs aux entreprises et aux droits de l'homme.

Intelligence artificielle et confidentialité des données

16. Les systèmes d'IA actuels font intervenir ou représentent une combinaison de systèmes d'analyse fondés sur des connaissances spécialisées formalisées (entrepôt de données, informatique décisionnelle) et sur l'apprentissage automatique, ainsi que sur l'application ciblée de ce qui a été appris. Il existe une différence entre les systèmes préprogrammés et algorithmiques visant à résoudre des problèmes précis, et les systèmes capables d'apprendre. Ces derniers sont équipés d'algorithmes d'apprentissage et doivent être formés.

17. Dans le processus décisionnel algorithmique régulièrement utilisé comme fondement de l'IA, une évaluation faite sur la base d'informations conduit à une décision, une prévision ou une recommandation. Dans le cas de l'« apprentissage supervisé », le système d'IA dispose de critères pour résoudre un problème précis, alors que, dans le cas de l'« apprentissage non supervisé », il choisit ou recommande lui-même les critères pertinents.

18. Par conséquent, tant le traitement des données que la décision prise à la suite de ce traitement exposent le sujet dont les données sont traitées à des risques potentiels.

19. L'informatique classique, divisée en « entrées », « traitement » et « résultats », est élargie par l'aptitude à percevoir, comprendre, agir et apprendre. Ces activités, auparavant propres à l'être humain, sont de plus en plus souvent effectuées par des machines. La notion de « compréhension » est nouvelle en informatique, et sa mise en œuvre doit s'accompagner d'un examen critique de la traçabilité et se faire dans le respect des droits de l'homme et des valeurs éthiques.

20. L'apprentissage automatique désigne, entre autres, une série de méthodes d'optimisation des réseaux de neurones artificiels. Les systèmes d'IA peuvent contenir des structures très complexes entre la couche d'entrée et la couche de sortie. Une cartographie de plusieurs couches de traitement hiérarchique permet à l'apprentissage automatique de gagner considérablement en efficacité (apprentissage profond). Cela entraîne inévitablement une réduction de la traçabilité des décisions prises par une IA. En raison de la complexité des algorithmes et de la multitude d'opérations arithmétiques effectuées par la machine, les critères de décision et leur pondération dans les couches de traitement plus profondes (couches cachées) échappent à toute demande de transparence.

21. La divulgation des algorithmes utilisés est au cœur du débat actuel sur la transparence de l'IA. Même si les algorithmes sont rendus publics, il sera sans doute difficile, dans la pratique, de vérifier concrètement la logique suivie par des systèmes d'IA hautement complexes. Qu'il s'agisse d'IA interprétable ou explicable, ou d'autres modèles, en cas de doute ou d'échec en ce qui concerne le processus ou les résultats, des preuves numériques sont nécessaires pour reconstituer ce qui s'est passé et déterminer pour quelle raison un résultat particulier a été conseillé ou a effectivement été obtenu.

22. Il y a de nombreux avantages, y compris pratiques, à soumettre à une surveillance externe les processus décisionnels des systèmes d'IA, en évaluant les décisions elles-mêmes au regard d'un objectif prédéterminé et des critères d'une gouvernance éthique.

23. Les décisions qui divergent des décisions et résultats escomptés doivent être mises en évidence et une intervention est nécessaire. Des outils spécifiquement conçus pour déceler les résultats non attendus et analyser les décisions prises sont indispensables. En utilisant exclusivement des machines pour surveiller d'autres machines, on augmente la possibilité de risques imprévus ou d'« inconnues inconnues ». Il faut donc poser comme principe que le jugement humain doit toujours prévaloir sur les contrôles effectués par l'IA.

24. La réussite de l'apprentissage automatique dépend, outre de l'efficacité des mécanismes mis en jeu, de la quantité de données disponibles et de leur qualité. L'essor des mégadonnées dans les technologies de l'information et la disponibilité croissante de données de haute qualité accélèrent considérablement le développement des systèmes d'IA.

25. Il est probable que les processus psychologiques et affectifs très complexes de la connaissance humaine et de la prise de décisions continueront d'être dévolus à des humains plutôt qu'à des machines. Par conséquent, lorsqu'il s'agit d'évaluer et de prendre en considération le droit applicable aux systèmes d'IA et aux décisions qu'ils prennent, il faut garder à l'esprit que les décisions prises par des machines sont fondées sur des principes et des mécanismes différents (quoique développés en grande partie par des humains) de ceux appliqués aux décisions humaines.

26. Pour assurer la sécurité nécessaire des systèmes d'IA, il importe de mettre effectivement en œuvre, dans le contexte du contrôle des entités utilisant des solutions d'IA, une gouvernance éthique et juridique complète applicable aux décisions prises par l'IA. Il faut également assurer une meilleure coopération numérique, dans le cadre de laquelle de multiples parties prenantes réfléchiraient à l'élaboration de normes et de principes comme la transparence et l'impartialité et à leur application aux solutions d'IA, dans différents contextes sociaux.

A. Principes relatifs à la confidentialité des données dans le contexte de l'utilisation de solutions d'IA

27. Indépendamment de la juridiction ou du cadre juridique dans lequel opère le gestionnaire responsable, huit grands principes doivent obligatoirement être pris en compte dans le cadre de la planification, du développement et l'implémentation de solutions d'IA. Ces principes et leurs caractéristiques ne visent à pas à remplacer une réglementation différente ou plus stricte en matière de protection des données qui serait applicable aux utilisateurs de solutions d'IA. Il s'agit des principes suivants :

a) Juridiction ;

b) Base éthique et légale ;

c) Éléments fondamentaux des données ;

d) Responsabilité et supervision ;

e) Contrôle ;

f) Transparence et « explicabilité » ;

g) Droits du sujet dont les données sont traitées ;

h) Garanties.

Juridiction

28. Pour garantir la sécurité juridique et la traçabilité, l'idéal serait de disposer d'un cadre transnational qui serait l'expression d'un consensus international et comprendrait des mécanismes chargés de déterminer et réglementer les obligations et les responsabilités dans le domaine des solutions d'IA et de gérer les risques connus.

29. En l'absence d'un tel cadre transnational, des solutions et des garanties peuvent être définies et appliquées à l'échelle locale. Dans ce cas de figure, lorsqu'une solution d'IA utilise un mécanisme de prise de décisions décentralisé, celui-ci devrait également relever d'une juridiction unique.

30. Parmi les autres possibilités, on peut citer la conclusion d'accords bilatéraux ou multilatéraux, ou l'adoption d'une réglementation nationale dont l'application est facilitée par la conclusion d'arrangements transfrontaliers, ou encore, dans les cas où la réglementation applicable reste définie par les forces du marché et les risques, l'application du droit de la consommation ou l'utilisation d'autres voies de droit.

31. Tant qu'un mécanisme de droit international ad hoc chargé de régler les conflits de compétence en matière de TIC n'a pas été mis en place, en particulier en ce qui concerne les solutions d'IA développées dans un État mais utilisées dans un autre, les solutions d'IA prévues pour fonctionner dans plusieurs États devraient être implémentées et exploitées

comme s'il s'agissait d'une association multinationale de solutions d'IA individuelles relevant d'une seule juridiction.

Base éthique et légale

32. Étant donné que le traitement des données personnelles des particuliers empiète toujours sur les droits des personnes concernées, les modalités de traitement des données par une solution d'IA doivent reposer sur un fondement éthique et juridique solide. C'est d'autant plus important si l'objectif de ce traitement est de prendre des décisions qui ont des effets sur la situation ou les droits de la personne ou de conduire à l'adoption de telles décisions. Indépendamment de la juridiction applicable ou du cadre réglementaire dans lequel opère le gestionnaire, la base légale peut être suffisante aux fins du traitement des données dans les cas suivants :

a) Il existe une loi rédigée dans le respect des principes démocratiques et des droits de l'homme qui offre une base légale spécifique en ce qu'elle régit la question du conflit d'intérêts entre les gestionnaires et les sujets dont les données sont traitées et prévoit des garanties suffisantes en matière de protection des droits de ces derniers ;

b) L'utilisation de la solution d'IA est nécessaire aux fins de l'exécution d'un contrat conclu avec le sujet dont les données sont traitées et celui-ci y a expressément consenti, et le contrat ne cause pas de préjudice important à la personne concernée ou ne porte pas atteinte à ses droits humains ou à ceux d'autres personnes ;

c) Le sujet dont les données sont traitées a librement donné son consentement, en toute connaissance de l'objectif visé par l'IA, des conséquences de l'utilisation de l'IA et des procédures applicables au retrait du consentement. Le consentement doit être donné par une action concrète et le gestionnaire responsable doit proposer un système de gestion du consentement qui permette à la personne concernée de retirer son consentement à tout moment et qui comprenne la fourniture des documents nécessaires ;

d) Dans l'intérêt légitime et premier du gestionnaire ou dans l'intérêt supérieur de la société, les sujets dont les données sont traitées reçoivent les informations nécessaires avant le début du traitement des données et se voient offrir la possibilité de s'opposer à ce traitement ou ont, à tout le moins, le droit de faire usage du mécanisme ou des procédures en place dans un délai raisonnable, ou de corriger leur situation ;

e) Chaque solution d'IA est limitée aux finalités pour lesquelles elle a été conçue à l'origine, implémentée et dûment documentée. Cela n'empêche pas d'autres utilisations ou une utilisation complémentaire (comme un traitement ultérieur) ou l'utilisation par un autre gestionnaire, mais toute autre utilisation devrait faire l'objet d'une nouvelle évaluation quant à sa base légale et aux garanties mises en place, notamment en ce qui concerne des objectifs apparemment compatibles ;

f) Des conditions spéciales ont été définies pour protéger les sujets qui appartiennent à des catégories particulières, sensibles ou vulnérables de la population, comme les enfants, les détenus ou d'autres groupes, et pour donner une base légale à l'application des solutions d'IA à ces sujets.

Éléments fondamentaux des données

33. Des données de qualité sont des données exactes (à savoir, entre autres choses, actualisées et non discriminatoires), minimisées et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les exigences en matière de protection des données devraient être prises en compte, de même que toute exigence supplémentaire applicable au traitement de données particulières, telles que les données relatives à la santé ou aux enfants.

Responsabilité et surveillance

34. Il importe que, pour chaque solution d'IA utilisée dans une organisation donnée, une personne physique ou morale assume l'entière responsabilité du traitement des données et de ses résultats. Cela couvre tous les aspects de la gestion du processus et de la technologie, notamment la licéité du traitement, la documentation utilisée, l'adaptation, les résultats, la

vérifiabilité éprouvée de l'ensemble des données de l'algorithme, le traitement des données, la prise en compte des informations et la collaboration à cet égard, ainsi que le respect des droits des sujets dont les données sont traitées. Lorsque la solution d'IA est distribuée à l'extérieur de l'organisation, les responsabilités des autres parties doivent être définies et dûment établies, et faire l'objet d'un accord.

35. Ces responsabilités, y compris celles d'un éventuel sous-traitant de la solution d'IA, doivent être transparentes, et les sujets dont les données sont traitées, les autorités publiques de contrôle et les régulateurs doivent avoir un accès adéquat aux informations les concernant.

36. Une gouvernance appropriée, en particulier dans les grandes entités juridiques, peut impliquer de désigner un responsable de la confidentialité des données, dont les responsabilités et les attributions consistent notamment à dispenser des conseils sur le respect des exigences en matière de protection des données et à suivre l'implémentation de la solution d'IA. Ce responsable doit disposer de ressources et de pouvoirs suffisants pour être à même de s'acquitter de ses fonctions, et suivre une formation complète et adaptée, ou posséder les qualifications nécessaires, du fait de sa formation ou de son expérience, pour exercer ses fonctions avec efficacité et en toute indépendance. Il est vivement recommandé de mettre en place des canaux de communication efficaces entre ce responsable et l'organe de surveillance ou de supervision compétent. Il est nécessaire pour les petits États et les start-ups d'investir dans la gouvernance de l'IA, que celle-ci implique ou non la création d'un tel poste.

37. Les informations relatives à ces dispositions en matière de responsabilité doivent être rendues publiques.

38. Une surveillance doit être exercée par un régulateur indépendant et compétent et un recours judiciaire doit être ouvert en cas de violation de la législation applicable.

Contrôle

39. Les solutions d'IA, y compris celles obtenues auprès d'un tiers, doivent relever entièrement de la compétence du gestionnaire concerné. De la conception initiale jusqu'à la désactivation, il faut établir clairement quelles données sont traitées par la solution d'IA, sur quels paramètres et critères de qualité des données se fonde la prise de décisions et comment ils s'équilibrent et sont pondérés. Les résultats doivent être contrôlés en permanence et corrigés si nécessaire. Aucune décision automatisée ne doit reposer sur des biais conscients ou inconscients. Les biais et effets discriminatoires possibles doivent faire l'objet d'une vérification et être corrigés avant le déploiement du système et à intervalles réguliers tout au long de la durée de vie du système.

40. Dans le cas des systèmes d'aide à la décision, la personne chargée de prendre les décisions doit être soumise à un ensemble similaire de contrôles.

41. Le gestionnaire, au besoin en concertation avec les sous-traitants, doit être en mesure d'arrêter ou de modifier le traitement à tout moment. Les résultats incorrects doivent faire l'objet d'une description, tout comme les mesures correctives prises, le but étant de réduire les risques pour les sujets dont les données sont traitées. Une fois que leur utilisation à des fins de repérage ou de correction ou à des fins judiciaires est terminée, les résultats incorrects doivent être supprimés dans des délais raisonnables.

42. Le fonctionnement de ce contrôle doit faire l'objet d'examens internes et externes permettant de donner suite à toute observation concernant la solution d'IA ou les résultats obtenus.

Transparence et « explicabilité »

43. Les solutions d'IA doivent être rendues transparentes pour le public et les sujets dont les données sont traitées. Les informations doivent être utiles et intelligibles et couvrir tous les éléments pertinents concernant l'évaluation de la solution et les droits éventuels des sujets dont les données sont traitées. Sont notamment visés l'« explicabilité » de l'objectif, les fonctions générales, les processus d'appui, les sources de données utilisées et l'étendue des résultats attendus. Ces éléments peuvent être, entre autres, les suivants :

a) Les sources de données et les données utilisées pour alimenter et former la solution d'IA, en plus des données fournies par la solution d'IA ;

b) La finalité et la base légale du traitement ;

c) Les paramètres qui constituent le fondement des décisions prises par l'IA et leur pondération ;

d) Des éclaircissements sur le point de savoir si la solution d'IA vise à préparer les décisions finales que vont prendre des êtres humains (aide à la décision) ou si elle génère la décision finale elle-même (prise de décisions automatisée) ;

e) La manière dont les responsabilités sont réparties entre le gestionnaire et le sous-traitant, lorsqu'elles ne sont pas identiques, ainsi que les points de contact et les canaux de communication possibles ;

f) La participation de tiers (par exemple, d'autres gestionnaires ou sous-traitants), le transfert vers d'autres pays (le cas échéant) et les raisons de cette participation et de ce transfert. Il est également nécessaire d'indiquer que les tiers sont tenus d'observer les mêmes prescriptions que le gestionnaire, notamment en matière de protection des données, et que leurs fonctions et leurs responsabilités sont similaires, quel que soit le lieu où ils exercent leur activité ;

g) Les informations nécessaires doivent à tout le moins figurer dans la politique de protection de la confidentialité des données relative à la solution d'IA et être accessibles, compréhensibles et utiles aux sujets dont les données sont traitées.

Droits du sujet dont les données sont traitées

44. Les personnes ou groupes de personnes dont les données personnelles sont traitées par la solution d'IA (sujets dont les données sont traitées) ont les droits suivants :

a) Obtenir des informations intelligibles quant à la question de savoir si des données personnelles les concernant sont stockées dans des fichiers automatisés et, dans l'affirmative, à quelles fins, et quels sont les autorités publiques, les particuliers ou les organismes privés qui exercent ou peuvent exercer un contrôle sur les fichiers les concernant ;

b) À tout moment pendant le traitement des données, retirer leur consentement sans subir de préjudice, si ce consentement a été donné et utilisé comme base légale pour ce traitement ;

c) S'opposer au traitement des données à tout moment et pour des raisons valables, si le traitement est fondé sur un intérêt légitime ;

d) Obtenir des informations concernant le respect de toutes les exigences de confidentialité des données énumérées dans la présente section ;

e) Accéder de manière raisonnable à leurs données personnelles en obtenant des informations écrites complètes sur celles-ci, sur la manière dont elles sont utilisées et traitées, ainsi que sur les résultats obtenus et sur les effets que peuvent avoir ces résultats sur leur situation et leurs droits individuels ;

f) Demander qu'une décision soit prise par un être humain, s'ils ont des raisons valables de penser que la décision proposée ou prise par la solution d'IA est erronée ou incorrecte ;

g) Corriger les données, si elles sont inexactes ;

h) Déposer plainte et disposer d'un recours si la plainte est admise ;

i) Effacer et purger les données si l'objectif de la solution d'IA n'existe plus ou si les données ne sont plus nécessaires à d'autres fins légales.

45. Ces droits ne prévalent ou n'empiètent pas sur les droits accordés en vertu du droit applicable dans une juridiction donnée aux sujets dont les données sont traitées.

Garanties

46. Les solutions d'IA devraient fonctionner de manière fiable, s'accompagner de garanties appropriées contre les risques et reposer sur des méthodes propres à favoriser la confiance et la compréhension de toutes les parties concernées, y compris les sujets dont les données sont traitées. Avant d'être déployées, toutes les solutions d'IA, même au stade expérimental, doivent au minimum faire l'objet d'une évaluation initiale des risques en matière de droits de l'homme et de protection des données, afin que les risques particuliers et les points critiques soient mis en lumière. En fonction du résultat de cette évaluation initiale, il peut être nécessaire de procéder à une nouvelle évaluation des droits et des risques.

47. Les garanties techniques et organisationnelles visant à atténuer les risques identifiés doivent être évaluées individuellement dans le cadre d'une approche fondée sur la protection de la vie privée dès la conception (*privacy by design*). Il faudrait envisager des mesures telles que l'anonymisation ou la pseudonymisation, le chiffrement, la séparation des clients, la gestion des accès (limitation), l'élaboration d'une politique de suppression des données et la surveillance des registres et des activités.

48. Les risques et les problèmes nouveaux engendrés par l'évolution technologique, architecturale ou structurelle, comme le développement de l'informatique distribuée, doivent être examinés à l'occasion de l'évaluation des risques.

49. La mitigation des risques peut s'appuyer sur des normes internationales telles que celles publiées conjointement par l'Organisation internationale de normalisation et la Commission électrotechnique internationale dans la série ISO/IEC 27000 (systèmes de gestion de la sécurité de l'information). En particulier, la norme ISO/IEC 27701 contient, en matière de confidentialité des données, des extensions qui prévoient au minimum des mesures de :

a) Protection : contrôles visant à assurer une protection contre les effets des risques évalués ;

b) Détection : contrôles visant à détecter les anomalies le plus rapidement possible ;

c) Réaction : contrôles visant à contenir et à éliminer le risque d'événements anormaux et à faire en sorte que les processus opérationnels de base puissent continuer à fonctionner jusqu'à ce que la solution globale soit trouvée et que la situation revienne à la normale.

B. Évaluation de la criticité des solutions d'IA

50. Les mesures à prendre doivent être centrées sur l'être humain et proportionnées aux risques d'atteintes aux droits de l'homme, en particulier au risque de discrimination, ainsi qu'au risque de violation de données, ainsi qu'à la complexité ou à la criticité de la solution de traitement des données concernée. Les approches appropriées sont notamment les suivantes.

Évaluation des effets sur les droits de l'homme lors de la phase de planification

51. Toutes les solutions d'IA doivent respecter l'état de droit, les droits de l'homme, les valeurs démocratiques et la diversité. Par conséquent, toutes les solutions d'IA envisagées, y compris les algorithmes, devraient faire sans tarder l'objet d'une étude d'impact sur les droits de l'homme, notamment d'évaluations en matière d'éthique et d'égalité. Les solutions d'IA envisagées ne sauraient porter atteinte au droit à l'égalité de traitement. Par exemple, les solutions d'IA utilisant des informations qui reflètent un biais inconscient conduiront à des résultats susceptibles d'être discriminatoires à l'égard de certaines personnes ou certains groupes de population. En outre, une solution d'IA alimentée par de « bonnes » informations peut conduire à de « mauvais » résultats, car l'apprentissage que fait la solution d'IA à partir des informations collectées peut l'amener à formuler des hypothèses erronées.

52. La protection de la vie privée dès la conception ou par défaut implique une évaluation, pendant la phase de planification, des effets que pourrait avoir l'implémentation de la solution d'IA sur les droits de l'homme, y compris le droit à la vie privée.

Phase de test et de correction − suivi

53. À l'issue de la phase de planification et de l'étude initiale d'impact sur les droits de l'homme, les conditions d'encadrement retenues doivent être prises en compte dans la phase de développement qui suit. Au cours de la phase d'implémentation et avant la mise en production, il faudrait soumettre les solutions d'IA à des tests intensifs reposant sur des données de test recueillies dans un environnement circonscrit et contenu, afin de déterminer non seulement si les hypothèses générales sous-jacentes sont prises en compte, mais également si elles se vérifient. Ce n'est que si le gestionnaire peut être sûr que la solution d'IA fonctionne correctement que celle-ci peut être concrètement implémentée.

54. Pendant toute la durée de fonctionnement de la solution d'IA, et jusqu'à l'arrêt définitif, les résultats obtenus doivent être contrôlés au regard des exigences fondamentales définies pendant la phase de planification.

55. Étant donné les difficultés liées au contrôle de tous les aspects des opérations algorithmiques et les changements constants d'algorithmes pendant la durée d'exécution d'une solution d'IA, il est essentiel de vérifier en permanence les résultats au regard de l'objectif initial de la solution en utilisant une autre méthode, afin de disposer d'un point de comparaison. Si l'on soupçonne ou constate un écart, il faut adapter le flux de données utilisées par la solution d'IA en conséquence ou interrompre l'exécution de la solution.

56. Afin de tirer profit des nouvelles approches créatives et d'élargir les perspectives à la fois des développeurs et des gestionnaires, il convient de tenir compte, au moment du développement des solutions d'IA, des tests et du suivi, des contributions et des réactions du secteur privé, de groupes intersectoriels et interprofessionnels, de la société civile et des utilisateurs. Il importe d'établir, pour les solutions d'IA prêtes à être mises en production, des mécanismes de test, comme des tests d'entrée-sortie au cours desquels des tiers entrent des données pour vérifier le type de résultats obtenus. Une autre possibilité serait que les régulateurs installent, dans les entreprises produisant des solutions d'IA, des environnements d'exploitation sécurisés (bacs à sable).

Évaluation de la criticité des données en fonction de leur utilisation

57. Outre la planification, les tests et l'implémentation, la criticité des données et la finalité visée sont également des éléments à prendre en compte pour un traitement adéquat des données.

58. Cela s'applique aux données générales, comme les informations personnelles à caractère général, ou aux données utilisées dans le domaine des télécommunications ou de la santé. Les données relatives à la santé et d'autres informations, par exemple le contenu des télécommunications, doivent faire l'objet d'un traitement plus rigoureux que les informations personnelles moins sensibles. Cela signifie qu'il faut particulièrement renforcer les mesures techniques et organisationnelles pertinentes, comme la limitation stricte des finalités et la minimisation des données, le chiffrement, la pseudonymisation, la restriction de l'accès, la suppression anticipée ou l'anonymisation.

59. L'utilisation envisagée des données joue un rôle clef dans la détermination du niveau de protection requis. Il peut être moindre pour une utilisation à des fins de stockage que pour une utilisation à des fins de profilage. La légitimité de l'objectif et des mesures de protection doit être évaluée avec une extrême attention.

60. Ces mesures doivent être prises et décrites à chaque évaluation des risques.

Évaluation périodique des systèmes d'IA et communication des informations aux organismes d'audit externe et de réglementation

61. L'évaluation du système vise à déterminer :

a) Les résultats escomptés ou non désirés ;

b) Le respect de l'équité, les biais et la discrimination à l'égard des individus et des groupes ;

c) Les compromis et les mesures de mitigation.

C. Autres éléments à prendre en compte

Audits externes et certification

62. Les responsables des audits et de la certification devraient avoir accès à toute la documentation interne utile, telle que les registres d'évaluation, pour pouvoir contrôler la conformité des systèmes d'IA avec les normes techniques et éthiques élaborées selon des approches multipartites et multilatérales.

63. Il conviendrait d'envisager une certification externe par un auditeur agréé en matière de confidentialité des données et dont les compétences en IA sont également reconnues officiellement. Une telle approche peut contribuer à dissiper les inquiétudes du public et des sujets dont les données sont traitées. Elle peut être particulièrement indiquée pour les solutions d'IA susceptibles de donner lieu à des résultats négatifs majeurs et d'entraîner une perte de confiance du public ou des organismes de réglementation.

Modifications de la législation et de la réglementation

64. Partout dans le monde, il est envisagé d'apporter des modifications à la législation et à la réglementation, ce qui aura une incidence sur la majorité des solutions d'IA. L'observation de ces nouvelles règles dépendra en grande partie de :

a) Leur conformité avec les normes nationales et internationales existantes ou nouvelles ;

b) La certification par un organisme de certification approprié opérant dans le cadre d'un accord national ou international.

Participation aux discussions

65. Les responsables des stratégies ou des solutions opérationnelles en matière d'IA et les personnes qui surveillent l'utilisation des solutions d'IA devraient participer aux discussions sur l'IA et sur les nouvelles questions d'ordre éthique et technique.

Éducation et sensibilisation

66. L'IA est un sujet complexe, et il importe que l'alimentation des systèmes d'IA en données et l'utilisation de ces données soient expliquées de façon claire et exhaustive aux utilisateurs et aux fournisseurs de données, ainsi qu'aux dirigeants, aux gestionnaires et aux autres personnes participant aux décisions concernant les solutions d'IA et leur fonctionnement. La seule publication d'algorithmes est insuffisante.

II. Principes et recommandations concernant le droit de l'enfant au respect de sa vie privée

67. Comme toutes les autres personnes, les enfants ont droit au respect des droits de l'homme et des libertés fondamentales. Le droit à la vie privée et le droit de l'enfant au respect de sa vie privée sont consacrés par différents instruments juridiques internationaux et régionaux[3].

[3] On peut citer comme exemples des instruments régionaux comme la Charte africaine des droits et du bien-être de l'enfant (1990) et la Convention européenne sur l'exercice des droits des enfants (1996), et des mécanismes régionaux comme le système interaméricain de protection des droits de l'homme.

68. Les principaux instruments qui consacrent les droits de l'enfant sont la Déclaration universelle des droits de l'homme et la Convention relative aux droits de l'enfant, qui est quasi universelle, puisqu'elle a été ratifiée par 193 parties.

69. L'article 16 de la Convention dispose ce qui suit :

1) Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ;

2) L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

70. Interprété au sens large, cet article s'applique aux différentes expériences des enfants en matière de vie privée[4].

71. Les droits de l'enfant sont universels, indivisibles, interdépendants et indissociables[5]. Le droit de l'enfant au respect de sa vie privée lui permet d'accéder à d'autres droits essentiels au développement de sa personnalité et de son identité[6], tels que, entre autres, les droits à la liberté d'expression[7] et d'association et le droit à la santé. Le droit de l'enfant au respect de sa vie privée est une notion qui recouvre l'intégrité physique et mentale, l'autonomie dans la prise de décisions, l'identité, la protection des informations personnelles et la protection de la vie privée dans ses dimensions physique et spatiale.

72. La vie intellectuelle, affective et sexuelle de l'individu trouve son fondement dans l'enfance et l'adolescence, et la protection de la vie privée joue un rôle à cet égard[8]. La façon de vivre l'enfance et le respect du droit à la vie privée diffèrent d'une région à l'autre[9]. Des facteurs intervenant dans l'intersectionnalité, comme la race, ont une incidence sur la manière dont l'enfant se construit[10].

73. En général, les éléments qui jouent un rôle décisif dans la formation de la personnalité de l'enfant sont la famille, la vie de famille, l'école et les réseaux sociaux. Tout comme les droits de l'enfant, ces éléments sont intimement liés entre eux et sont le reflet de facteurs structurels sous-jacents.

74. Les enfants sans foyer ni famille, tels que les enfants non accompagnés, les enfants en situation de rue, les enfants placés hors du milieu familial, les enfants vivant en zone de conflit ou se trouvant dans d'autres situations de vulnérabilité rencontrent bien plus de difficultés dans l'exercice de leurs droits humains[11].

75. Même si la notion de vie privée a une signification différente selon les personnes, le Rapporteur spécial tient à souligner le caractère positif et le rôle de facilitation du droit à la vie privée, qui touche à la dignité intrinsèque de chacun et favorise l'exercice d'autres droits de l'homme[12].

---

[4] John Tobin et Sarah M. Field, « Article 16: The right to protection of privacy, family, home, correspondence, honour, and reputation », dans *The UN Convention on the Rights of the Child: a commentary*, John Tobin, dir. publ. (Oxford, Oxford University Press, 2019).

[5] Comité des droits de l'enfant, observation générale n° 16 (2013), par. 12.

[6] Communication du Bureau régional du Haut-Commissariat des Nations Unies aux droits de l'homme pour le Moyen-Orient et l'Afrique du Nord (l'autorisation de publier la communication n'a pas été donnée).

[7] Communication de la Fédération internationale des associations et institutions de bibliothèques, p. 2. Les communications que le Rapporteur spécial a reçues en réponse à ses consultations et pour lesquelles l'autorisation de publier a été accordée seront consultables à l'adresse https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx.

[8] Communication du Belgian Disability Forum, p. 2.

[9] Communications de : InternetLab et Alana Institute ; Bureau du Commissaire à l'information de l'État de Victoria (Australie).

[10] Rebecca Epstein, Jamila Blake et Thalia González, « Girlhood interrupted: the erasure of black girls' childhood », Georgetown Law Center on Poverty and Inequality, 2017.

[11] Communication de Maat Foundation for Peace, Development and Human Rights, p. 7.

[12] Voir la résolution 68/167 de l'Assemblée générale et la résolution 20/8 du Conseil des droits de l'homme et le document enregistré sous la cote A/HRC/13/37.

76. L'« autodétermination » se caractérise par la capacité de l'individu à décider si, et dans quelle mesure, il entend divulguer des aspects de sa vie personnelle[13]. L'autonomie s'entend de la capacité à gérer soi-même sa pensée, ses sentiments et ses actes. Le mot « enfant » désigne toute personne âgée de moins de 18 ans.

Repérage des problèmes

Intérêts contradictoires

77. Pour définir en quoi le respect du droit de l'enfant à la protection de sa vie privée et au développement de sa personnalité est un facteur d'autonomie, il faut examiner les tensions et les perspectives divergentes dans lesquelles ce droit s'inscrit.

78. La Convention relative aux droits de l'enfant donne aux États parties et aux parents la capacité et l'obligation − selon le cas − de faire en sorte que les enfants jouissent des droits énoncés à l'article 16, compte tenu du degré de développement de leurs capacités (art. 5), afin de garantir leur intérêt supérieur (art. 3)[14].

79. Le droit de l'enfant au respect de sa vie privée est traditionnellement considéré comme une question gérée par les adultes. Pourtant, les besoins des enfants en matière de vie privée diffèrent de ceux des adultes et peuvent entrer en conflit avec eux[15]. Le « sharenting », par exemple, peut mettre en conflit le droit à la liberté d'expression des parents avec le droit à la vie privée de leur enfant[16].

80. L'interprétation que font les adultes des besoins des enfants en matière de vie privée peut empêcher un développement sain de l'autonomie et de l'indépendance de l'enfant et restreindre sa vie privée au prétexte de la protection[17]. Le recours des adultes à la surveillance pour protéger les enfants en est un exemple éloquent. Bien que cette pratique restreigne leur droit à la vie privée et à l'autonomie[18], les enfants font de plus en plus l'objet d'une surveillance technologique de la part de l'administration, du secteur privé, de leurs parents, de leur famille et de leurs pairs. La surveillance parentale s'accroît au lieu de diminuer à mesure que l'enfant grandit et devient (ou devrait devenir) plus indépendant[19]. Les parents et les personnes qui s'occupent d'enfants ayant des besoins particuliers adoptent volontiers des attitudes encore plus protectrices, en définissant des paramètres de confidentialité élevés par défaut et en se réservant la possibilité de définir les paramètres de la vie privée en ligne de leurs enfants[20].

81. Les parents ont parfois un comportement qui est en contradiction avec les préoccupations qu'ils expriment. Selon les informations disponibles, 57 % des parents d'adolescents âgés de 13 à 17 ans craignent que leur enfant reçoive ou envoie des images explicites[21] et 85 % s'inquiètent du respect de la vie privée de leurs enfants en ligne. Pourtant,

[13] Résumé de l'arrêt de la Cour constitutionnelle fédérale allemande du 15 décembre 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES].

[14] Tobin et Field, « Article 16 ».

[15] Communications de : Parental Rights Foundation ; Action Canada pour la santé et les droits sexuels, p. 4 ; Commission nationale de l'informatique et des libertés (CNIL), p. 11.

[16] Communication du Commissaire à l'enfance et à la jeunesse d'Australie méridionale (où le terme « sharenting » est décrit comme la tendance croissante des parents et futurs parents à utiliser Internet pour publier des informations sur leurs enfants, ce qui façonne l'identité en ligne d'un enfant bien avant que celui-ci n'ait la capacité de donner son consentement ou ne commence à créer sa propre empreinte numérique), p. 3.

[17] Communication de International Child Rights Center et MINBYUN.

[18] Ibid. ; Jane Bailey et Valerie Steeves, *Defamation Law in the Age of the Internet: young people's perspectives* (Commission du droit de l'Ontario, Canada, 2017) ; communication d'Ariel Foundation International.

[19] Communication du Commissaire à l'enfance et à la jeunesse d'Australie méridionale.

[20] Voir www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[21] Monica Anderson, « A majority of teens have experienced some form of cyberbullying », Pew Research Center, 27 septembre 2018.

moins d'un sur trois installe un contrôle parental sur l'appareil de son enfant, et 81 % laissent délibérément leur enfant utiliser le site YouTube général sans supervision[22].

82. La nécessité de disposer d'analyses des risques, de politiques et de réglementations fondées sur des données probantes et centrées sur les enfants a été mise en lumière par des travaux de recherche récents qui montrent que les adultes qui n'ont pas subi de préjudices en ligne (tels que des menaces violentes ou du trolling) sont plus susceptibles que les autres de vouloir restreindre l'accès aux informations et l'anonymat en ligne[23].

83. En grandissant, les enfants désirent et exigent que l'école, les entreprises et l'État, mais aussi leurs parents, respectent leur vie privée[24]. Ce besoin s'accroît au fil du temps. Alors que les enfants âgés de 5 à 7 ans ne considèrent généralement pas la surveillance parentale de leurs activités en ligne comme une violation de leur vie privée, les adolescents âgés de 15 à 17 ans sont souvent préoccupés par la surveillance exercée par leurs parents et par l'école[25]. Ils pensent que le respect de leur vie privée et de leur espace personnel, sans jugement ni surveillance, est propice à l'exploration intellectuelle, à l'expression créative et au développement d'opinions indépendantes[26]. Le contrôle parental doit être proportionnel au degré de développement des capacités et des opinions de l'enfant[27].

Identité personnelle

84. Les enfants d'aujourd'hui sont la première génération à être nés pendant l'ère numérique[28], et leurs parents sont les premiers à élever des « enfants numériques »[29].

85. De plus en plus souvent, l'identité de l'enfant commence à se définir avant la naissance, alors que ses parents et sa famille diffusent sur Internet des images de lui in utero. Bon nombre de ces images contiennent des informations personnelles.

86. L'identité numérique de l'enfant continue de se former tout au long de l'enfance, essentiellement au travers des mesures prises par la famille ; 80 % des enfants vivant dans les pays occidentaux développés ont une empreinte numérique avant l'âge de 2 ans[30]. Il arrive que des images d'enfants soient utilisées sans le consentement des intéressés pour des collectes de fonds à des fins caritatives[31].

87. Les enfants sont désormais présents en ligne de multiples façons, et de plus en plus tôt[32]. Leur utilisation des médias sociaux change radicalement entre 9-10 ans (34 % d'enfants utilisateurs) et 11-12 ans (69 % d'enfants utilisateurs)[33]. Le nombre de contacts en ligne des enfants double entre la septième année d'enseignement et la onzième[34]. De nombreux enfants de moins de 13 ans ont un compte sur des médias sociaux (38 % des enfants âgés de 9 à 12 ans, selon des enquêtes européennes[35]) et la plupart ont entre deux et cinq comptes[36]. La pandémie de maladie à coronavirus (COVID-19) a accentué cette tendance ; ainsi, entre mars

[22] Communication d'ACT/The App Association.
[23] BT/DEMOS, « Online harms: a snapshot of public opinion » (2020). Consultable à l'adresse https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf.
[24] Communications de Future of Privacy Forum et d'Ariel Foundation International.
[25] Communication de Global Privacy Assembly, Digital Education Working Group, p. 25.
[26] Communication du Bureau du Commissaire à l'information de l'État de Victoria (Australie).
[27] Communication de la CNIL, p. 11.
[28] Communication de la Commission canadienne des droits de la personne, p. 2.
[29] Danah Boyd, « Social network sites as networked publics: affordances, dynamics, and implications », dans *A Networked Self: Identity, Community and Culture on Social Network Sites*, Zizi Papacharissi ed. (Routledge, 2011).
[30] Communication de l'Autorité nationale hongroise pour la protection des données et la liberté d'information, p. 42.
[31] Communications de : International Child Rights Center et MINBYUN ; Défenseur des enfants (Croatie), p. 3.
[32] Communications de : Bureau du Commissaire à l'information (Royaume-Uni) ; CNIL ; Commissaire à l'information et à la protection des données (Albanie).
[33] Communication de la Commission économique pour l'Amérique latine et les Caraïbes (CEPALC).
[34] Communication de l'Autorité nationale hongroise pour la protection des données et la liberté d'information, p. 29.
[35] Ibid., p. 53.
[36] Communication du Commissaire à l'information et à la protection des données (Albanie), p. 14.

et septembre 2020, le nombre de comptes Messenger Kids (Facebook) utilisés quotidiennement a augmenté de 350 %[37].

88. L'estime et l'image de soi, nécessaires à la formation de la personnalité et de l'identité, se construisent de plus en plus par le numérique[38]. Les enfants utilisent Internet comme un compte rendu permanent de leur vie ; le cœur et le pouce levés affichés sur les médias sociaux deviennent des extensions de leur pensée[39]. Dans le même temps, les enfants craignent de perdre le contrôle des informations qu'ils postent en ligne[40].

89. La violence, les abus sexuels et la cyberintimidation font partie de la vie numérique, en particulier pour les jeunes lesbiennes, gays, bisexuels, transgenres, queers et intersexes (LGBTQI) (voir A/HRC/43/52). Environ 25 % des adolescents âgés de 13 à 17 ans déclarent avoir reçu des images explicites sans leur consentement[41]. Environ 29 % des filles et 20 % des garçons déclarent avoir été destinataires d'images explicites non sollicitées. La réception et la diffusion d'images non désirées, même quand celles-ci ne sont pas objectivement nuisibles, offensantes ou gênantes, peuvent nuire au développement de l'estime de soi, de l'autonomie, des relations et du développement psychosocial de l'enfant[42].

90. Les abus sexuels sur enfants, qu'ils soient commis hors ligne ou en ligne, constituent une violation de l'intégrité physique et de l'autonomie décisionnelle des personnes concernées. Ils ont des conséquences à long terme sur la personnalité et les capacités des victimes ; le fait que les contenus montrant des violences sexuelles sur enfant restent indéfiniment en ligne aggrave ces conséquences. Les formes que prennent les abus comme leurs effets sont ancrées dans la manière dont la société envisage les enfants et leur corps[43]. Pour lutter contre ces abus, il faut adopter des stratégies fondées sur les droits de l'homme[44]. L'immersion des jeunes dans un environnement numérique toujours plus étendu crée un flux continu de données qui sont collectées et enrichies par l'intelligence artificielle, les applications d'apprentissage automatique et les technologies de reconnaissance faciale et vocale. Les enfants et leurs données alimentent l'économie numérique[45]. Le marché de la publicité en ligne destinée aux enfants pourrait valoir 1,7 milliard de dollars d'ici à 2021, les sociétés de publicité en ligne collectant plus de 72 millions d'unités de données par enfant avant que celui-ci n'atteigne l'âge de 13 ans[46].

91. Les spécialistes du marketing entrent en contact avec les jeunes, les influencent et nouent avec eux des relations suivies. Les jeunes enfants sont particulièrement vulnérables au marketing ciblé car ils ne font pas la différence entre publicité et contenu ni entre fiction et réalité, et ne comprennent pas la fonction persuasive de la publicité[47]. Les technologies qui utilisent des techniques comportementales (design persuasif, pratiques obscures) renforcent l'adhésion, déclenchent des comportements impulsifs, influencent la prise de décisions, suscitent la crainte d'être exclu et font oublier les préoccupations relatives à la vie privée[48].

92. Le profilage des enfants limite le potentiel de développement personnel des intéressés pendant l'enfance et l'adolescence, voire à l'âge adulte, en ce que les prédictions

[37] Communication de Facebook.

[38] Communications de : Anna Bunn, p. 11 ; Bureau du Commissaire à l'information de l'État de Victoria (Australie), p. 2.

[39] Communication de Ariel Foundation International.

[40] Communications de : C. Mahieu ; Bureau du Commissaire à l'information de l'État de Victoria (Australie) ; CNIL.

[41] Monica Anderson, « A majority of teens have experienced some form of cyberbullying ».

[42] Communications de : Bunn ; C. Mahieu.

[43] Communication d'InternetLab et Alana Institute.

[44] Recommandation générale nº 38 (2020) du Comité pour l'élimination de la discrimination à l'égard des femmes ; communication de Maat Foundation for Peace, Development and Human Rights, p. 7.

[45] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019) ; communication d'InternetLab et Alana Institute.

[46] Communication de la CNIL, p. 3.

[47] Communications de : Campaign for Commercial-Free Childhood et Center for Digital Democracy ; InternetLab et Alana Institute ; CNIL.

[48] Communications de : Bureau du Commissaire à l'information (Royaume-Uni) ; Bureau du Commissaire à l'information de l'État de Victoria (Australie) ; C. Mahieu ; Jonathan Crock *et al.*, American University ; CNIL ; CEPALC.

comportementales et les techniques de « nudging » peuvent prédéterminer les options et les choix. Les possibilités offertes par la technologie doivent être évaluées au regard des droits et de l'intérêt supérieur de l'enfant[49], car le traitement des données personnelles concernant des enfants est susceptible de :

a) Porter atteinte à la vie privée et à la protection des données, y compris entraîner une perte d'autonomie et ternir la réputation personnelle ;

b) Nuire à la santé mentale et affective et au bien-être physique des enfants ;

c) Entraîner un préjudice économique ou donner lieu à une exploitation commerciale[50].

93. Les enfants et les jeunes demandent des solutions pour réduire l'accès des entreprises à leurs données et l'utilisation de celles-ci[51], une délimitation des activités commerciales et des mécanismes permettant de faire valoir leur intérêt supérieur, notamment la possibilité d'effacer les contenus publiés[52]. Les enfants estiment qu'ils devraient pouvoir exercer leur droit de demander à n'importe quelle entreprise une copie de leurs données personnelles. Environ 40 % d'entre eux pensent qu'ils devraient pouvoir formuler des demandes d'accès ou d'effacement à tout âge et 21 % estiment que cela devrait être possible dès 13 ans, voire plus jeune. Seuls 13,5 % des enfants interrogés estiment qu'il faut avoir 18 ans ou plus pour faire une demande d'accès ou d'effacement[53].

94. L'ère numérique est bénéfique pour le développement des enfants. Ceux-ci doivent cependant pouvoir jouir de leur droit au libre développement de leur personnalité sans être entravés par des pratiques commerciales.

95. D'après des informations, des technologies biométriques de surveillance et de traçage ont été utilisées en Amérique du Sud pour identifier et surveiller des enfants soupçonnés de comportements illicites, et la vie privée des enfants n'est pas protégée dans les procédures judiciaires[54]. Identifier des enfants suspects ou les enfants de personnes incarcérées ou associées au terrorisme porte atteinte au droit à la vie privée, soumet les enfants concernés à la stigmatisation et à la discrimination et entrave le développement de leur personnalité[55]. Le développement de l'enfant peut aussi être entravé quand les enfants ne sont pas identifiés auprès des services de soutien compétents[56], bien que la communication de données, en particulier aux services de sécurité, puisse poser des problèmes[57].

Sexualité, genre, intégrité corporelle et autonomie physique

96. Les capacités physiques, intellectuelles, sociales et émotionnelles varient énormément d'un enfant à l'autre. Les différences sont particulièrement prononcées à l'adolescence, qui est une période caractérisée par une évolution rapide sur les plans physique, intellectuel et social, y compris par la maturation des organes sexuels et reproducteurs[58].

[49] Communications de : Commission canadienne des droits de la personne, p. 2 ; Bureau du Commissaire à l'information de l'État de Victoria (Australie) ; Campaign for Commercial-Free Childhood et Center for Digital Democracy.

[50] Communication du Bureau du Commissaire à l'information (Royaume-Uni).

[51] Valerie Steeves, « Young Canadians in a wired world, phase III: trends and recommendations », MediaSmarts, 2014.

[52] Communication de The eQuality Project.

[53] Communication de Global Privacy Assembly, p. 24.

[54] Communication d'InternetLab et Alana Institute.

[55] Comité des droits de l'enfant, observation générale n° 24 (2019).

[56] Communications de : Children of Prisoners Europe ; Families Outside ; International Coalition for the Children of Incarcerated Parents ; Quaker United Nations Office.

[57] Office des Nations Unies contre la drogue et le crime (ONUDC), *Manuel sur les enfants recrutés et exploités par des groupes terroristes et extrémistes violents : Le rôle du système judiciaire* (Vienne, 2017), p. 153 et 154 ; Nations Unies, Bureau de lutte contre le terrorisme, *Les enfants touchés par le phénomène des combattants étrangers : Assurer l'adoption d'une approche fondée sur les droits de l'enfant* (2019), p. 74.

[58] Comité des droits de l'enfant, observation générale n° 4 (2003).

97. L'expression de la sexualité, l'intégrité physique et l'autonomie corporelle font intrinsèquement partie de la vie privée des enfants, mais aussi de leur liberté d'expression[59]. Les adolescents doivent pouvoir prendre des décisions concernant leur bien-être et leur corps, et, au fur et à mesure qu'ils grandissent, explorer leur sexualité en toute sécurité et en toute intimité[60], que ce soit en ligne ou hors ligne[61].

98. Pourtant, les actes des États, des entités commerciales, des professionnels de santé et autres, des parents ou des pairs portent parfois atteinte au droit des enfants à l'intégrité physique et à l'autonomie. Parmi les atteintes relevées, on peut signaler[62] :

a) Concernant les filles : mutilations génitales ; mariages forcés ; relations sexuelles forcées ; grossesse et maternité forcées ; tests de grossesse forcés ; stérilisations forcées ; refus d'information ou de prestation de services concernant la santé sexuelle et procréative ; obligation de l'information ou du consentement des parents pour la prescription de contraceptifs ou l'accès à l'avortement ; thérapies de conversion ; sanctions pénales pour des activités sexuelles consenties entre pairs, y compris le sexting ; abus sexuels en ligne et hors ligne ; crimes d'honneur ; « slut-shaming » ;

b) Concernant les garçons : mutilations génitales ; mariages forcés ; relations sexuelles forcées ; stérilisations forcées ; refus d'information ou de prestation de services concernant la santé sexuelle et procréative ; thérapies de conversion ; sanctions pénales pour des activités sexuelles consenties entre pairs, y compris le sexting ; abus sexuels en ligne et hors ligne ; harcèlement ; châtiments corporels ;

c) Concernant les enfants qui ont une identité et une expression de genre non conformes, ont une orientation sexuelle minoritaire ou présentent des variations du développement sexuel : violences ; discrimination et harcèlement ; pathologisation de leur identité de genre ou de leur corps ; traitements médicaux inutiles ; publication d'informations détaillées concernant leurs organes génitaux ; stigmatisation ; viol « éducatif » ; thérapies de conversion ; refus de prestation de services de santé spécifiques, notamment des informations et services en matière de santé sexuelle et procréative adaptés aux transgenres ; refus d'accès aux dossiers médicaux ; sanctions pénales pour des activités sexuelles consenties entre pairs, y compris le sexting ; abus sexuels en ligne et hors ligne ; absence de reconnaissance juridique de l'identité de genre.

99. Les atteintes à l'intimité corporelle ont des répercussions sur d'autres droits, tels que ceux consacrés aux articles 3, 6, 8, 12, 16, 19 et 29 (par. 1) de la Convention relative aux droits de l'enfant. Par exemple[63] :

a) Les tests de grossesse obligatoires portent atteinte au droit des filles à la dignité, à l'égalité et à l'autonomie ;

b) Les enquêtes visant à identifier les élèves qui présentent une variance de genre ou appartiennent à une minorité sexuelle portent atteinte au droit à la non-discrimination et, quand elles sont utilisées pour expulser des élèves, violent le droit à l'éducation ;

c) Les tests de virginité dits « volontaires », souvent imposés par les parents, portent atteinte au droit des filles à la dignité, à l'égalité et à l'autonomie ;

d) L'adoption d'une approche surmédicalisée, dans le cadre de laquelle une intervention chirurgicale conditionne la reconnaissance juridique de l'identité de genre, porte atteinte au droit à la santé[64] ;

[59] Communications de : Matimba ; Conseil de l'Europe ; Commission australienne des droits de l'homme.

[60] Communication de Center for International Human Rights.

[61] Communication de ParentsTogether.

[62] Communications de : Crock *et al.* ; Human Rights Watch ; ILGA-Europe, Transgender Europe et International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation ; NNID (Netherlands organisation for sex diversity) ; CHOICE for Youth and Sexuality ; OutRight Action International ; Commission australienne des droits de l'homme ; Center for International Human Rights ; Conseil de l'Europe.

[63] Communication de Organisation Intersex International Europe.

[64] Communications de : Matimba ; A. McCarthy.

e) Le fait que le consentement ou l'information des parents conditionne l'accès des enfants aux services de santé sexuelle ou procréative met en jeu le droit à la santé, à l'identité, à la vie et à la protection contre tout préjudice, ainsi que l'intérêt supérieur de l'enfant.

100. Les enfants ont besoin et ont le droit de recevoir des conseils sur les relations sexuelles saines, le consentement et les pratiques sûres[65]. Une éducation sexuelle complète peut aider les enfants à protéger et à renforcer leur vie privée, leur indépendance et leur autonomie[66] ; elle peut favoriser leur bien-être, en particulier pour les jeunes LGBTQI[67]. Des réactions hostiles à une éducation sexuelle complète des enfants et adolescents sont signalées dans le monde entier, notamment au Brésil, au Ghana, au Kenya, en Pologne et en République dominicaine[68].

Reconnaissance de l'identité

101. Tous les êtres humains ont des droits justement parce qu'ils sont humains et, partant, égaux entre eux[69]. Les registres et les systèmes d'enregistrement établissent l'identité officielle des individus[70], et pourtant les enfants ont rarement leur mot à dire sur ce qui figure dans leur dossier.

102. L'identité officielle commence avec l'enregistrement de la naissance. Pourtant, de nombreux enfants dans le monde − particulièrement dans les communautés aborigènes et autochtones − ne sont pas enregistrés[71]. Or, l'absence de reconnaissance juridique compromet l'accès à de nombreux droits nécessaires au développement de l'autonomie, comme l'éducation.

103. Les actes de naissances peuvent être problématiques pour la dignité, l'identité, la vie privée ou le développement des enfants transgenres ou intersexes, des enfants nés à l'étranger d'une gestation pour autrui, des enfants disparus, des enfants réfugiés non accompagnés et des enfants pris en charge hors du milieu familial, entre autres[72].

Éducation et enseignement

104. L'éducation vise à favoriser l'épanouissement de la personnalité de l'enfant et le développement de ses dons et de ses aptitudes mentales et physiques, dans toute la mesure de leurs potentialités[73]. C'est à la fois un droit de l'homme et le principal moyen pour les enfants de vivre une vie digne. En les protégeant contre l'exploitation, elle donne aux enfants, individuellement et collectivement, les moyens d'agir. Les États sont tenus de respecter, de protéger et de réaliser le droit à l'éducation en supprimant les obstacles à l'éducation, tels que les interdictions et la violence fondées sur le genre[74].

105. L'école joue un rôle important dans la manière dont les enfants exercent leur droit à la vie privée au quotidien. Le 1er avril 2020, après l'arrivée de la pandémie de COVID-19,

[65] Comité des droits de l'enfant, observation générale nº 15 (2013) ; Comité des droits économiques, sociaux et culturels, observation générale nº 22 (2016). Communications de : Commission australienne des droits de l'homme ; C. Mahieu ; Centre des droits reproductifs, p. 1.

[66] Communications de : Action Canada pour la santé et les droits sexuels ; ILGA-Europe, Transgender Europe et The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation.

[67] Communication de McCarthy.

[68] Communication de Human Rights Watch, par. 18.

[69] Dinah Shelton, « On identity », *The George Washington International Law Review*, vol. 39 (1999).

[70] Communication de Rights in Records by Design, Université Monash et Federation University ; *D. Z. c. Pays-Bas* (CCPR/C/130/D/2918/2016).

[71] Communication de la Commission australienne des droits de l'homme.

[72] Communications de : Commission australienne des droits de l'homme ; Rights in Records by Design, Université Monash et Federation University ; Kathryn Allan et David Lacey, « Identity management in disaster response environments: a child exploitation mitigation perspective », *Australian Journal of Emergency Management*, vol. 33, nº 3 (juillet 2018).

[73] Convention relative aux droits de l'enfant, art. 29 (par. 1 a)).

[74] Résolution 75/166 de l'Assemblée générale.

193 pays avaient fermé les écoles, ce qui représentait environ 90 % des élèves dans le monde[75].

106. Dans le domaine de l'éducation en ligne, le nombre de téléchargements d'applications éducatives a augmenté de 90 % par rapport à la moyenne hebdomadaire de la fin de 2019[76]. Le passage à l'éducation en ligne a accentué le déséquilibre des rapports de force entre les entreprises qui produisent des contenus pédagogiques numériques et les enfants, et entre les administrations et les enfants et leurs parents, plusieurs États ayant dérogé aux lois en vigueur sur la protection des données relatives aux enfants. Au pays de Galles, par exemple, l'administration a supprimé l'obligation de recueillir le consentement des parents et des élèves[77]. Dans d'autres pays, le droit des enfants au respect de leur vie privée n'est pas protégé dans les écoles publiques[78]. Pourtant, il est fréquent que des acteurs non étatiques contrôlent les dossiers pédagogiques numériques des enfants[79].

107. Les données d'apprentissage qui sont numérisées et stockées portent sur le raisonnement, le parcours d'apprentissage, le niveau d'engagement, les temps de réponse, les pages lues et les vidéos visionnées[80]. L'éducation étant obligatoire, la plupart des enfants et des parents n'ont pas la capacité de contester les décisions des entreprises concernées en matière de protection de la vie privée ou de refuser de fournir des données[81].

108. Les écoles choisissent les applications et les outils d'apprentissage en ligne en fonction des programmes d'enseignement et de considérations financières plutôt que de considérations liées à la protection de la vie privée[82]. En septembre 2020, une analyse de 496 applications éducatives utilisées dans 22 pays a révélé que nombre d'applications collectaient des éléments d'identification des appareils, 27 enregistraient les données de localisation et 79 des 123 applications testées manuellement communiquaient des données d'utilisateurs à des tiers, comme des partenaires publicitaires[83]. Il y a donc lieu de se poser des questions sur la sécurité des données. Ainsi, entre le 24 août et le 24 septembre 2020, Microsoft a enregistré, concernant ses logiciels éducatifs, 5,7 millions d'incidents liés à des logiciels malveillants[84].

109. Les écoles elles-mêmes détiennent des quantités importantes d'informations sur les enfants et surveillent de plus en plus les élèves, en contrôlant leurs activités en ligne et en recourant à des caméras de surveillance[85]. Comme pour les applications éducatives, de telles pratiques doivent s'accompagner de la mise en œuvre du principe de responsabilité, du recueil du consentement, de la limitation des finalités, de la minimisation des données et de garanties de transparence et de sécurité[86].

[75] Communication de ParentsTogether.
[76] Communication de Human Rights Watch, par. 44.
[77] Ibid., par. 48.
[78] Communication du Commissaire à l'enfance et à la jeunesse d'Australie méridionale.
[79] Voir https://rm.coe.int/educational-settings/16809f3ba3.
[80] Communication de Global Privacy Assembly, p. 4.
[81] Communications de : DefendDigitalMe ; Conseil de l'Europe.
[82] Communication du Bureau du Commissaire à l'information de l'État de Victoria (Australie).
[83] Alfred Ng, « Education apps are sending your location data and personal info to advertisers », CNET, 1er septembre 2020.
[84] Communication de Human Rights Watch, par. 49.
[85] Communication du Commissaire à l'enfance et à la jeunesse d'Australie méridionale.
[86] Communications de : InternetLab et Alana Institute ; Research Group on Technology, Information and Society, Université de Fortaleza (Brésil) ; Médiateur de la ville autonome de Buenos Aires ; Conseil de l'Europe.

110. Les processus éducatifs ne devraient pas porter atteinte à la jouissance de la vie privée ou d'autres droits, quels que soient le lieu et les modalités de l'enseignement[87], et ne devraient pas aggraver les inégalités existantes[88].

Adaptation à l'âge et degré de développement des capacités

111. L'expression « adapté à l'âge » est généralement entendue comme l'alignement de l'âge chronologique et du comportement, et comme l'alignement des services proposés aux enfants, comme les contenus en ligne, sur l'âge chronologique. Cela se traduit, dans la réglementation, par l'obligation pour les fournisseurs de services en ligne de proposer des services qui conviennent à l'âge des enfants. Le « Age Appropriate Design Code » du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord en est un exemple récent[89]. Aux États-Unis d'Amérique, la loi de 1998 sur la protection de la vie privée des enfants en ligne impose des règles aux opérateurs de sites Web et de services en ligne destinés aux enfants de moins de 13 ans, ainsi qu'aux autres opérateurs de sites Web ou de services en ligne qui recueillent sciemment des informations à caractère personnel concernant des enfants de moins de 13 ans.

112. Pourtant, le mécanisme de l'adaptation à l'âge n'est pas la panacée, puisque :

a) Les contenus peuvent être adaptés à l'âge mais être quand même préjudiciables pour les enfants et leurs droits. Le mécanisme peut protéger un enfant et lui donner des outils utiles s'il est individualisé, mais il peut ne pas répondre aux besoins d'une cohorte d'enfants, compte tenu des variations considérables du développement intellectuel et affectif entre enfants du même âge[90] ;

b) En définissant un seuil général, le mécanisme de l'adaptation à l'âge crée des inégalités dont pâtissent les enfants qui ont des capacités différentes et fournit une évaluation grossière du degré de développement des capacités de ces enfants, ce qui peut entraver le développement de leur personnalité et l'exercice autonome de leurs droits, et est potentiellement discriminatoire ;

c) Quand l'âge est le critère d'accès aux services, des documents d'identité vérifiables sont requis, ce qui soulève des préoccupations en ce qui concerne la sécurité, les approches normatives et l'absence de normes de garantie de l'âge, les outils et les mécanismes de certification du secteur[91]. Certains avancent que les processus de vérification de l'âge peuvent être mis en œuvre d'une manière compatible avec le respect de la vie privée[92].

113. L'âge seul est considéré comme une mesure imparfaite pour évaluer les capacités des enfants[93]. Certains pays reconnaissent une capacité non fondée sur l'âge chronologique[94]. Au début de 2020, les autorités de l'Ontario (Canada) ont adopté une législation qui permet aux jeunes d'accéder à leurs informations personnelles et d'en demander la rectification expressément sur la base de la capacité, et non de l'âge. En cas de litige, les droits de l'enfant peuvent l'emporter sur les décisions des parents ou des tuteurs[95].

[87] Comité des droits de l'enfant, observation générale nº 1 (2001) ; résolution 75/166 de l'Assemblée générale. Communications de : DefendDigitalMe ; Médiateur de la ville autonome de Buenos Aires ; Research Group on Technology, Information and Society, Université de Fortaleza (Brésil) ; Autorité nationale hongroise pour la protection des données et la liberté d'information, numéro de dossier NAIH/2020/7127/.

[88] Résolution 75/166 de l'Assemblée générale. Communications de : Médiateur de la ville autonome de Buenos Aires ; CEPALC ; Conseil de l'Europe.

[89] Voir https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/.

[90] Comité des droits de l'enfant, observation générale nº 7 (2005).

[91] Communications de : CNIL, p. 10 ; Facebook.

[92] Communication de Yoti.

[93] Voir https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf.

[94] Communication de Global Privacy Assembly, p. 20.

[95] Ibid., p. 25.

114. Pour déterminer si un enfant est prêt à prendre des décisions et à assumer ses choix, il faut tenir compte non seulement de l'âge chronologique de l'intéressé mais également du contexte, y compris les risques encourus et le soutien disponible, l'expérience individuelle, les droits mis en cause et la capacité de l'enfant de comprendre les conséquences de ses actes (ou de ses omissions). Pour déterminer le moment où un enfant est capable, par exemple, de consentir au traitement de ses données personnelles, il convient de prendre en considération sa compréhension effective du traitement des données, son intérêt supérieur, ses droits et son opinion[96].

115. Pour résumer, la notion de l'adaptation à l'âge est en porte-à-faux avec le principe de l'évolution des capacités de l'enfant. L'étalonnage des services en fonction du degré de développement des capacités de l'enfant requiert des analyses plus approfondies.

Solutions possibles

116. Il est essentiel, pour protéger l'intérêt supérieur des enfants, de préserver au mieux leur vie privée[97]. Une approche axée sur l'intérêt supérieur de l'enfant suppose que les adultes sollicitent activement l'opinion des enfants et en tiennent dûment compte. Les actes des États, des entreprises, des parents et autres parties prenantes ne reflètent pas toujours une telle approche[98], mais les enfants sont reconnus en droit international comme des êtres humains, et pas seulement comme des humains en devenir, et ont donc le droit de jouir des droits de l'homme[99].

117. Toutes les parties − États, entreprises, communautés, individus et parents − doivent reconnaître que les enfants sont des titulaires de droits. Une lutte efficace et globale contre la maltraitance à l'égard des enfants facilitée par les TIC, par exemple, suppose l'adoption d'une approche multipartite fondée sur les droits de l'homme qui fasse participer activement les enfants, les familles, les communautés, l'administration, la société civile et le secteur privé[100].

118. Si la dépendance des enfants − et donc leur vulnérabilité − peut entraîner des risques, le risque n'est pas synonyme de préjudice et les enfants doivent apprendre à en gérer une certaine dose pour développer leur résilience et leurs capacités d'adaptation[101]. En définissant les enfants uniquement par leur vulnérabilité, sans tenir compte de leurs capacités ou de leur potentiel, on risque d'appliquer des stratégies trop protectionnistes, potentiellement préjudiciables au développement de leur personnalité.

Protection des données des enfants

119. Même si la protection de la vie privée est une notion plus large et plus complexe que la protection des données, la deuxième est étroitement liée à la première. Pour favoriser le libre développement de la personnalité des individus, il faut protéger les personnes concernées contre la collecte, le stockage, l'utilisation et le partage illimités de données personnelles.

120. Beaucoup considèrent le consentement comme un élément fondamental. Cependant, il n'est pas nécessairement l'expression de l'autonomie de l'enfant et il ne protège pas cette autonomie, en particulier lorsque le rapport de force est déséquilibré. En outre, le consentement des parents n'est pas toujours conforme à l'intérêt supérieur de l'enfant et ne reflète pas toujours l'opinion de l'enfant[102].

121. Même si le règlement général sur la protection des données (RGPD) européen pourrait mieux protéger les données personnelles des enfants, il accorde une protection spéciale aux mineurs en exigeant que ceux-ci reçoivent une information adaptée concernant le traitement

[96] Communication du Conseil de l'Europe.
[97] Communication de l'ONUDC.
[98] Communication de Promsex.
[99] John Tobin, « Understanding children's rights: a vision beyond vulnerability », *Nordic Journal of International Law*, vol. 84, n° 2 (juin 2015).
[100] Communications de : ONUDC ; Facebook.
[101] Communication du Commissaire à l'enfance et à la jeunesse d'Australie méridionale.
[102] Communication du Défenseur des enfants (Croatie), p. 4.

de leurs données (art. 12)[103], en prêtant une attention particulière au profilage des enfants (considérant 71) et en prévoyant un droit renforcé à l'oubli (considérant 65) ; en outre, l'article 8 dispose que les enfants âgés de 13 à 16 ans peuvent avoir la capacité de consentir au traitement de leurs données[104]. Les éléments généraux que sont la protection des données dès la conception, le respect de la vie privée par défaut, le droit de ne pas être soumis à une décision individuelle automatisée (art. 22) et les évaluations d'impact sur la protection des données mériteraient d'être appliqués plus largement aux fins de la protection des données personnelles des enfants[105].

122. La Convention 108+[106] protège également les personnes contre les décisions prises uniquement sur le fondement d'un traitement automatisé de données (art. 9 (par. 1 a)), et les lignes directrices récemment adoptées par le Conseil de l'Europe sur la protection des données personnelles des enfants dans un contexte éducatif élargissent la définition du traitement des données à caractère personnel de manière à couvrir les prédictions relatives à des groupes ou à des personnes présentant des traits communs, et la définition du traitement des données biométriques de manière à englober ces types de traitement[107].

Ingénierie de la vie privée et culture numérique

123. La conception technologique peut contribuer à contrer la « conception persuasive » et les « pratiques obscures »[108], et à faire progresser la réalisation des objectifs des lois et des règlements[109].

124. Parallèlement à l'ingénierie de la vie privée dans le contexte des technologies numériques, les enfants et les adolescents ont besoin de compétences opérationnelles et de capacités cognitives et sociales pour utiliser les technologies de manière réfléchie, éthique et sûre. L'éducation à la culture numérique peut prévenir à la source les comportements préjudiciables en ligne[110]. Il y a un large consensus, y compris parmi les enfants eux-mêmes, sur le fait que la culture numérique peut renforcer leur sécurité et leur autonomie en ligne[111], sachant en particulier que les enfants vont sur Internet de plus en plus tôt et que leurs parents ont du mal à leur fournir un soutien efficace[112].

125. Toutefois, les solutions techniques et la culture numérique ne suffisent pas à elles seules ; il faut, de la part des États, une action rigoureuse et soutenue visant à remédier aux inégalités structurelles et à garantir la vie privée, la protection des données et la sécurité des enfants[113]. Les États pourraient investir bien davantage dans de meilleurs partenariats avec la

[103] Simone van der Hof et Eva Lievens, « The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR », *Communications Law*, vol. 23, nº 1 (2018).

[104] En dessous de cet âge, le traitement des données nécessite le consentement du parent ou du tuteur au nom de l'enfant.

[105] Van der Hof et Lievens, « The importance of privacy ».

[106] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, telle que modernisée par le Protocole d'amendement, Série des traités du Conseil de l'Europe nº 223. Consultable à l'adresse https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

[107] Communication du Conseil de l'Europe.

[108] Communications de : Campaign for Commercial-Free Childhood et Center for Digital Democracy ; CNIL.

[109] Communication d'ACT/The App Association.

[110] Jane Bailey et Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices* (University of Ottawa Press, 2015) ; Jane Bailey et Jacquelyn Burkell, « Legal remedies for online attacks: young people's perspectives », *The Annual Review of Interdisciplinary Justice Research*, vol. 9 (2020).

[111] Communications de : Fédération internationale des associations et institutions de bibliothèques ; Bureau du Commissaire à l'information de l'État de Victoria (Australie) ; Future of Privacy Forum ; Conseil de l'Europe ; Commission australienne des droits de l'homme ; Crock *et al.*, p. 5.

[112] Communications de : Commissaire à l'information et à la protection des données (Albanie) ; InternetLab et Alana Institute.

[113] Résolution 75/166 de l'Assemblée générale.

société civile, l'industrie, les universités et les enfants afin de construire ensemble des solutions qui pourront servir de prototypes.

III. Conclusions

126. **Pour promouvoir la vie privée des enfants et favoriser leur autonomie, il faut :**

a) Adopter des politiques, des lois et des règlements qui :

i) Font des enfants des titulaires des droits de l'homme dont les droits à la vie privée, à l'autonomie et à l'égalité sont inaliénables[114] **;**

ii) Protègent la vie privée au sens large, et pas seulement les données, de manière à permettre aux enfants de développer pleinement leur potentiel[115] **;**

iii) Tiennent compte du point de vue des enfants, des stratégies des enfants en matière de respect de la vie privée, des résultats de la recherche axée sur les enfants et des études d'impact relatives à la vie privée des enfants[116] **;**

iv) Établissent des mécanismes indépendants de conciliation, d'arbitrage et de réparation pour les violations individuelles ou systémiques des droits de l'homme commises contre des enfants[117] **et garantissent l'adoption de mesures coercitives en cas d'infraction**[118] ;

b) S'attaquer aux dynamiques structurelles qui font que les enfants sont vulnérables et n'ont pas les moyens d'agir ;

c) Promouvoir les innovations technologiques qui permettent d'améliorer les services de communication de l'information tout en protégeant la vie privée des enfants[119]**.**

IV. Recommandations

127. **Le Rapporteur spécial recommande aux États :**

a) De veiller à ce que les droits et les valeurs de la Convention relative aux droits de l'enfant concernant la vie privée, la personnalité et l'autonomie sous-tendent la législation, les politiques, les décisions, les systèmes d'enregistrement et les services de l'État ;

b) De soutenir l'élaboration d'analyses complètes de la capacité des enfants à prendre des décisions autonomes aux fins de l'accès aux services en ligne et autres, afin de permettre l'adoption de lois, de politiques et de réglementations en matière de protection de la vie privée qui soient spécifiques aux enfants et fondées sur des éléments concrets ;

c) De n'adopter des normes relatives à la prise en considération de l'âge en tant qu'instruments réglementaires qu'avec la plus grande prudence et que lorsqu'il n'existe pas de meilleure solution ;

d) De promouvoir et d'imposer la mise en œuvre des principes directeurs relatifs à la sécurité dès la conception, à la protection de la vie privée dès la conception et à la protection de la vie privée par défaut pour les produits et les services destinés

[114] Bailey et Steeves, *eGirls, eCitizens*.

[115] Communications de : Commissaire à l'enfance et à la jeunesse d'Australie méridionale ; International Child Rights Center et MINBYUN ; Autorité nationale hongroise pour la protection des données et la liberté d'information, p. 58.

[116] Communications de : Commissaire à l'enfance et à la jeunesse d'Australie méridionale ; Bailey et Steeves, *eGirls, eCitizens*.

[117] Communication de la Commission australienne des droits de l'homme.

[118] Communication de 5Rights Foundation.

[119] Communication d'ACT/The App Association.

aux enfants, et de veiller à ce que les enfants disposent de recours efficaces contre les atteintes à la vie privée ;

e) De promouvoir les partenariats avec la société civile et l'industrie pour cocréer des offres technologiques qui répondent à l'intérêt supérieur des enfants et des jeunes ;

f) De suivre les recommandations du Rapporteur spécial concernant la protection contre les atteintes à la vie privée fondées sur le genre (A/HRC/43/52, par. 33 et 34) ;

g) D'élaborer des plans d'action complets pour l'éducation en ligne qui soient fondés sur l'article 29 (par. 1) de la Convention relative aux droits de l'enfant et sur les lignes directrices du Conseil de l'Europe sur la protection des données personnelles des enfants dans un contexte éducatif[120] ;

h) De veiller à l'établissement et au maintien de cadres juridiques appropriés pour l'éducation en ligne ;

i) De créer des infrastructures publiques pour les activités éducatives et sociales non commerciales ;

j) De remédier à toutes les lacunes dans la loi et la procédure pour que tous les enfants en contact avec la justice voient leur vie privée protégée tout au long de la procédure, et d'interdire à vie la divulgation de toute inscription au casier judiciaire faite pendant l'enfance ;

k) De revoir les cadres juridiques pour que les entreprises puissent, de leur propre initiative, détecter de manière légale et proportionnée les contenus en ligne montrant des abus sexuels sur enfant ;

l) De veiller à ce que les données personnelles des enfants associés à des groupes terroristes ou extrémistes violents soient classées et communiquées uniquement lorsque cela est strictement nécessaire à la coordination des mesures de réadaptation et de réinsertion prises à l'intention de ces enfants ;

m) Avant de relier les bases de données de l'état civil et les bases de données judiciaires, de mener des études d'impact sur les droits de l'homme pour évaluer les implications pour les enfants et leur vie privée, et de mener des consultations pour évaluer la nécessité, la proportionnalité et la légalité de la surveillance biométrique ;

n) D'adopter des pratiques et des lois propres à garantir que les informations fournies aux médias ne violent pas le droit des enfants à la vie privée et que la communication d'informations par les médias et d'autres entités ne porte pas atteinte à la vie privée des enfants dont les parents ont maille à partir avec la justice ;

o) De veiller à ce que la vie privée des enfants soit respectée dans le cadre de tous leurs contacts avec leurs parents incarcérés, y compris dans le cadre des communications écrites, électroniques et téléphoniques, et des visites en prison ;

p) De veiller à ce qu'aucune donnée biométrique ne soit collectée auprès d'enfants, sauf à titre exceptionnel et uniquement lorsque cela est légal, nécessaire, proportionné et pleinement conforme aux droits de l'enfant ;

q) De veiller à ce que les données personnelles des enfants soient traitées de manière équitable, correcte et sûre, pour une finalité spécifique, conformément à une base juridique légitime et dans le respect de cadres de protection des données représentant les meilleures pratiques, tels que le règlement général sur la protection des données et la Convention 108+ ;

r) De veiller à ce que les personnes qui traitent les données à caractère personnel, y compris les parents ou tuteurs et les éducateurs, soient sensibilisées au droit des enfants à la vie privée et à la protection des données ;

[120] Voir www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting.

s) De veiller à ce que les enfants aient accès à des informations sur l'exercice de leurs droits, par exemple sur les sites Web des autorités de protection des données, et de veiller à ce qu'ils aient accès à des services d'accompagnement psychologique, à des mécanismes de plainte et à des voies de recours qui leur sont spécifiquement destinés, notamment pour les cas de cyberintimidation ;

t) De veiller à ce que l'anonymat, le pseudonymat ou l'utilisation des technologies de chiffrement par les enfants ne soient pas interdits par la loi ou dans la pratique ;

u) De veiller à ce que les enfants et les jeunes de toutes origines aient la possibilité de participer à la prise de décisions et à la conception des cadres, des politiques et des programmes qui leur sont destinés ;

v) D'interdire le traitement automatisé des données à caractère personnel qui a pour objectif de procéder au profilage des enfants dans le but de prendre des décisions les concernant ou d'analyser ou de prédire leurs préférences, leur comportement et leur disposition d'esprit, en prévoyant des dérogations applicables uniquement dans des circonstances exceptionnelles, dans l'intérêt supérieur de l'enfant ou dans un intérêt public supérieur, et en les assortissant des garanties juridiques appropriées ;

w) De veiller à ce que les droits et les valeurs de la Convention relative aux droits de l'enfant concernant la vie privée, la personnalité et l'autonomie sous-tendent les politiques, les décisions et les services des entreprises ;

x) De mettre en œuvre les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » et les orientations relatives aux questions de genre qui y figurent (A/HRC/41/43, annexe)[121] **;**

y) De mettre en place des mécanismes de recours et de réclamation, tout en veillant à ce qu'ils n'entravent pas l'accès aux mécanismes étatiques ;

z) De fournir des informations compréhensibles sur la façon de signaler les problèmes, y compris sur les mécanismes de plainte, de recours et de réclamation ;

aa) De prendre des mesures raisonnables, proportionnées, opportunes et efficaces pour garantir que les réseaux et les services en ligne ne sont pas utilisés abusivement à des fins criminelles ou à d'autres fins illicites préjudiciables aux enfants ;

bb) De collaborer avec les autorités chargées de l'application de la loi pour faciliter l'identification et la poursuite des auteurs d'infractions visant des enfants.

Travaux futurs

128. **Les priorités immédiates des futurs travaux sur la vie privée et les enfants sont notamment :**

a) Engager un effort international pour mettre en place des cadres visant à donner des orientations en matière de conception, afin de protéger la vie privée des enfants en ligne ;

b) Associer les enfants, lors des visites de pays et dans les rapports thématiques, à la réflexion sur les questions touchant à leur vie privée ;

c) Faire des recherches sur les normes relatives au contrôle parental et leurs effets sur le développement de l'enfant.

[121] Voir également www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf.

Annexe I

Overview of activities

The key achievements of the mandate since 2015 include:

A. Detailed thematic reports and recommendations on:

Big data and open data, A/72/540 (2017) and A/73/438 (2018)

Health-related data, A/74/277 (2019)

Privacy and gender, A/HRC/40/63 (2019)

Artificial intelligence and privacy, and children's privacy, A/HRC/46/37 (2021)

B. Security and surveillance

The establishment of the International Intelligence Oversight Forum, which met in Bucharest (2016), Brussels (2017), Valletta (2018) and London (2019).

The draft legal instrument on government-led surveillance, while not progressed, has increasingly been demonstrated as needed and a useful reference for future work.

Networks have been established through the use of working parties, consultations and involvement of regional human rights bodies/entities, particularly in Europe.

Discussions with and specific recommendations to intelligence agencies, police forces and/or Governments of Member States concerning reinforcement of safeguards and remedies, including legislation regarding surveillance, encryption and independent oversight authorities.

Intensive work on complaints of infringement of privacy by Julian Assange and President Lenin Moreno, including preparation of interim reports.

The Special Rapporteur presented a report to the Human Rights Council on governmental surveillance activities from a national and international perspective, A/HRC/34/60 (2017).

The Special Rapporteur presented a report to the General Assembly on the implications of the COVID-19 pandemic for the right to privacy, A/75/147 (2020).

Communications to Member States

Since 2015, 101 communications have been issued to Member States concerning practices that appeared inconsistent with the right to privacy. Thirty were issued in 2020 (see annex II).

Visits and events

The COVID-19 pandemic prevented any official country visits during 2020.

Country visits were undertaken in: the United States of America in 2017 (A/HRC/46/37/Add.4); France in 2018 (A/HRC/46/37/Add.2); the United Kingdom of Great Britain and Northern Ireland in 2018 (A/HRC/46/37/Add.1); Germany in 2018 (A/HRC/46/37/Add.3); Argentina in 2019 (A/HRC/46/37/Add.5) and the Republic of Korea in 2019 (A/HRC/46/37/Add.6).

During 2020, the Special Rapporteur continued to promote privacy via online events, including the forty-second International Conference of Data Protection and Privacy Commissioners and multiple civil society organization and non-governmental organization events.

Taskforces

Security and surveillance

The annual International Intelligence Oversight Forum 2020 was postponed due to the COVID-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption. More detailed laws are needed to protect encryption and thereby, the privacy of communications.

Taskforce on corporations' use of personal data

The Special Rapporteur held five taskforce meetings attended by civil society organizations and leading corporations. The dialogue was highly productive, addressing issues including identity verification, European Court judgments concerning cross border movement of data, artificial intelligence, and privacy and children.

The taskforce's recommendation on artificial intelligence is provided in the main text of the present report. The draft was provided for international consultation, to which 28 submissions were received.

Taskforce on privacy and personality: children

The Special Rapporteur worked independently yet collaboratively with the Committee on the Rights of the Child on new guidelines to protect children's privacy. He also provided feedback to the Committee on its draft general comment No. 25.

The Special Rapporteur released a call for contributions on how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on research, consultations with children and good practice mechanisms. Nearly 60 submissions were received. The principles and recommendations are included in the main body of the present report.

Annexe II

Communications on the right to privacy

Communications (joint and from the Special Rapporteur on the right to privacy alone) on the right to privacy sent, and replies received, between 1 June 2015 and 1 January 2021

TIME PERIOD: Sent and Responses Received	*TYPE of COMMUNICATION*						
	Joint Urgent Appeals	*Joint Allegation Letters*	*Joint Other Letters*	*SRP Urgent Appeals*	*SRP Allegation Letters*	*SRP Other Letters*	*Total*[a]
2015–2020 Sent	6	60	19	0	5	11	101
2015–2020 Responses	4[b]	51[c]	10[d]	0	7[d]	5	77[a]
2020 Sent	1	22	5	0	0	2	30
2020 Responses	0	16[e]	4[f]	0	0	2	22[a]

Source: OHCHR communication database, https://spcommreports.ohchr.org/TmSearch/Results.

Abbreviation: SRP, Special Rapporteur on privacy.

[a] The number of replies received is not equal to the number of matters raised, as some replies included more than one response.

[b] Two Joint Urgent Appeals received two responses each.

[c] 44 responses to Joint Allegation Letters included six matters which received two responses, and one matter received a total of three responses, making a total of 51 responses from Member States.

[d] Two replies consisted of two responses.

[e] One reply included three responses.

[f] One reply consisted of two responses.