Nations Unies A/79/173

Assemblée générale

Distr. générale
17 juillet 2024
Français
Original : espagnol

Soixante-dix-neuvième session
Point 71 b) de l'ordre du jour provisoire*
Promotion et protection des droits humains : questions relatives aux droits humains, y compris les divers moyens de mieux assurer l'exercice effectif des droits humains et des libertés fondamentales

Droit à la vie privée

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale le rapport établi par la Rapporteuse spéciale sur le droit à la vie privée, Ana Brian Nougrères, en application de la résolution 28/16 du Conseil des droits de l'homme.

* A/79/150.

24-13146 (F) 180824 220824

Proposition de mise à jour de la résolution 45/95 de l'Assemblée générale du 14 décembre 1990, intitulée « Principes directeurs pour la réglementation des fichiers personnels informatisés »

Rapport de la Rapporteuse spéciale sur le droit à la vie privée, Ana Brian Nougrères

Résumé

On trouvera dans le présent rapport une proposition de mise à jour de la résolution 45/95 de l'Assemblée générale du 14 décembre 1990, intitulée « Principes directeurs pour la réglementation des fichiers personnels informatisés », dont l'objectif est d'adapter le contenu de ladite résolution à la réalité sociotechnologique du XXIe siècle.

I. Contexte et justification

1. Dans la Charte des Nations Unies, signée le 26 juin 1945[1], les Gouvernements des Nations Unies ont fixé comme l'un des buts de l'Organisation des Nations Unies celui de « réaliser la coopération internationale [...] en développant et en encourageant le respect des droits de l'homme et des libertés fondamentales pour tous, sans distinctions de race, de sexe, de langue ou de religion »[2]. Les droits des personnes relatifs au traitement des données à caractère personnel font dès lors également partie de la mission de l'Organisation.

2. En effet, l'Assemblée générale[3], par sa résolution 45/95 du 14 décembre 1990, a adopté des principes directeurs pour la réglementation des fichiers personnels informatisés[4]. Cette résolution donne suite à la résolution 1990/42 de la Commission des droits de l'homme, en date du 6 mars 1990, et à la résolution 1990/38 du Conseil économique et social, en date du 25 mai 1990, toutes deux intitulées « Principes directeurs pour l'utilisation des fichiers personnels informatisés ». Bien qu'ils ne soient pas juridiquement contraignants pour les États, ces principes directeurs ont marqué un tournant et ont été pris en compte dans les réglementations nationales et cités par des juges et des universitaires.

3. La résolution 45/95 a été adoptée en 1990 pour apporter des réponses aux réalités sociotechnologiques de l'époque. Depuis, de nouvelles tendances et avancées technologiques sont apparues et ont transformé la société, à telle enseigne qu'elles font désormais partie du quotidien de chacun. Parmi les exemples d'avancées notables, on peut citer :

- L'apparition et la démocratisation d'Internet, qui a révolutionné la manière dont nous accédons à des informations provenant du monde entier et les partageons ;
- Les smartphones, qui sont devenus des appareils incontournables pour communiquer, travailler, apprendre et se divertir ;
- Les réseaux sociaux, qui ont transformé les modes de communication et les rapports sociaux en ligne ;
- L'informatique en nuage, qui a changé la façon dont les entreprises et les particuliers gèrent l'information en leur permettant d'accéder à des données et à des applications en ligne et de stocker des informations, où qu'ils se trouvent dans le monde ;

[1] Le texte de la Charte peut être consulté sur le site Web de l'ONU, à l'adresse suivante : https://www.un.org/fr/about-us/un-charter/full-text.

[2] Voir Article premier, paragraphe 3, de la Charte des Nations Unies. Les buts des Nations Unies énoncés à l'Article premier sont les suivants : « 1. Maintenir la paix et la sécurité internationales [...]. 2. Développer entre les nations des relations amicales fondées sur le respect du principe de l'égalité de droits des peuples et de leur droit à disposer d'eux-mêmes, et prendre toutes autres mesures propres à consolider la paix du monde. 3. Réaliser la coopération internationale en résolvant les problèmes internationaux d'ordre économique, social, intellectuel ou humanitaire, en développant et en encourageant le respect des droits de l'homme et des libertés fondamentales pour tous, sans distinctions de race, de sexe, de langue ou de religion. 4. Être un centre où s'harmonisent les efforts des nations vers ces fins communes. »

[3] Principale instance de délibération et d'élaboration des politiques de l'ONU, l'Assemblée générale est aussi son organe le plus représentatif (https://www.un.org/fr/ga/).

[4] Les principes s'appliquent non seulement aux fichiers informatisés des entités publiques et privées, mais également, par voie d'extension facultative et sous réserve des adaptations adéquates, aux fichiers traités manuellement (Principes directeurs, paragraphe 10).

- Les mégadonnées, grâce auxquelles la prise de décision peut être éclairée par des analyses complexes réalisées en traitant de grandes quantités de données ;
- L'intelligence artificielle (IA), qui suscite de grandes attentes et de profonds bouleversements en permettant de produire des informations au moyen d'algorithmes avancés ;
- L'Internet des objets, qui permet d'interconnecter des appareils physiques grâce à Internet afin de partager des informations et d'automatiser et de contrôler des systèmes divers à distance ;
- La réalité virtuelle et la réalité augmentée, qui ont permis de créer de nouvelles expériences numériques sous la forme de jeux, d'applications d'apprentissage et de simulations ;
- Les véhicules autonomes, qui, grâce aux progrès de l'IA et des capteurs, ont transformé le secteur des transports et les modes de déplacement ;
- Les neurotechnologies, qui permettent une compréhension fine du cerveau et la collecte d'informations neurales sur les personnes (données à caractère extrêmement sensible).

4. Aucune de ces technologies n'avait été découverte au moment de l'adoption de la résolution 45/95 de l'Assemblée générale. Il est donc nécessaire de mettre à jour le contenu de cette dernière afin de l'adapter à la réalité sociotechnologique du XXIe siècle. Qui plus est, les technologies actuelles permettent de collecter, depuis n'importe quel endroit, des données sur des personnes domiciliées ou résidant dans d'autres pays. Ce phénomène, appelé « collecte internationale de données »[5], n'est pas abordé dans la résolution 45/95 et devrait être traité dans les textes internationaux, étant donné qu'il s'agit de la méthode la plus répandue de collecte de données personnelles à l'échelle de la planète.

5. À cela s'ajoute le fait que l'information est essentielle au fonctionnement d'outils technologiques tels que l'IA, dont les résultats ne sont pas produits par les algorithmes en soi, mais par le traitement et l'analyse d'informations par ces derniers.

6. Il convient de faire la distinction entre les informations au sens large et les données à caractère personnel, qui sont si précieuses qu'elles sont parfois appelées « monnaie de l'économie numérique ». À cet égard, par exemple, l'Organisation de coopération et de développement économiques (OCDE) a adopté fin décembre 2022 la Déclaration sur un avenir numérique de confiance, durable et inclusif[6], dont les auteurs saluent, entre autres avancées, « les résultats du projet horizontal de l'OCDE sur la gouvernance des données au service de la croissance et du bien-être [...], qui reconnaissent l'importance des données en tant que **levier de l'économie mondiale** » (caractères gras ajoutés).

7. L'OCDE s'est notamment engagée à œuvrer pour « favoriser une transformation numérique centrée sur l'humain et fondée sur les droits, qui aille de pair avec la promotion du respect des droits humains au sein comme en dehors de l'environnement numérique, de mécanismes solides de protection des données à caractère personnel, de lois et réglementations adaptées à l'ère numérique, et d'une utilisation fiable,

[5] Nelson Remolina Angarita (2015), « Recolección internacional de datos: un reto del mundo post-internet » (Collecte internationale de données : un défi du monde post-Internet), Première édition (Madrid, Espagne, Agencia Estatal, Boletín Oficial del Estado).

[6] OCDE, « Déclaration sur un avenir numérique de confiance, durable et inclusif ». La déclaration a été adoptée à l'occasion de la réunion qui s'est tenue sur l'île de la Grande Canarie (Espagne) les 14 et 15 décembre 2022. La déclaration officielle peut être consultée à l'adresse suivante : https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0488.

sécurisée, responsable et durable des technologies numériques émergentes et de l'intelligence artificielle »[7].

8. Pour leur part, le 23 janvier 2023, le Parlement européen, le Conseil de l'Union européenne et la Commission européenne ont approuvé la Déclaration européenne sur les droits et principes numériques pour la décennie numérique[8]. À la section intitulée « Un environnement numérique loyal » du chapitre III (« Liberté de choix ») de ladite déclaration, les auteurs s'engagent notamment à « garantir un environnement numérique sûr et sécurisé fondé sur une concurrence loyale, où les droits fondamentaux sont protégés, où les droits des utilisateurs et la protection des consommateurs au sein du marché unique numérique sont assurés et où les responsabilités des plateformes, en particulier des grands acteurs et des contrôleurs d'accès, sont bien définies ».

9. Ces travaux ont amené des entités du monde entier à conduire un examen des documents internationaux relatifs au traitement des données, ainsi que des lois locales en la matière, en vue de les mettre à jour. Ainsi, en octobre 2023, l'Assemblée mondiale pour la protection de la vie privée (AMVP) a adopté une résolution sur la mise en place de normes mondiales pour la protection des données, idée qu'elle défend depuis plusieurs dizaines d'années. Elle y énonce des principes à appliquer dans le monde entier pour garantir une forte protection des données et de la vie privée[9], ainsi que des droits et d'autres éléments qu'elle considère comme essentiels pour atteindre cet objectif et qu'elle s'engage à défendre, à promulguer et à promouvoir de sorte qu'ils puissent être effectivement mis en œuvre et appliqués dans tous les contextes, en particulier dans le cadre du traitement des données à l'aide de technologies et d'innovations nouvellement mises au point.

10. Dans sa résolution, l'AMVP souligne également qu'il importe d'assurer la protection transfrontière des données à caractère personnel au moyen de divers mécanismes de transfert, tels que l'adéquation, les clauses types, les certifications et les accords administratifs, l'objectif étant de faire en sorte que les dispositifs de protection des données continuent de s'appliquer aux informations lorsque celles-ci franchissent les frontières. Elle y souligne également les avantages qu'il y a à s'appuyer sur les points communs, les complémentarités et les éléments de convergence pour favoriser à l'avenir l'interopérabilité entre les dispositifs et les mécanismes réglementaires en place et garantir ainsi la sûreté et la fiabilité des flux de données transfrontières[10].

11. Sur le plan international, le XX^{e} siècle a vu l'amorce d'un processus d'harmonisation réglementaire dont les principaux moteurs ont été le Conseil de l'Europe, l'OCDE, l'ONU, le Parlement européen et le Conseil de l'Union européenne, rejoints au XXI^{e} siècle par l'Association de coopération économique Asie-Pacifique (APEC), le Réseau ibéro-américain de protection des données et l'AMVP (anciennement Conférence internationale des commissaires à la protection des données et de la vie privée).

[7] Ibid.

[8] Parlement européen, Conseil et Commission, « Déclaration européenne sur les droits et principes numériques pour la décennie numérique » (2023/C 23/01), 23 janvier 2023. La déclaration officielle peut être consultée à l'adresse suivante : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52022DC0028.

[9] « Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide » (Mise en place de normes mondiales pour la protection des données : principes à appliquer pour garantir une forte protection des données et de la vie privée), Résolution de l'AMVP, octobre 2023. Le texte peut être consulté à l'adresse suivante : https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf.

[10] Ibid.

12. Ainsi, selon le Réseau ibéro-américain de protection des données, l'établissement d'un cadre pour la protection des données harmonisé au niveau mondial est le principal fondement sur la base duquel reposent les différents instruments internationaux adoptés en la matière pour faire en sorte que le développement du commerce mondial soit compatible avec la protection des droits des personnes, en particulier la protection des informations les concernant[11].

13. Enfin, il nous faut évoquer le cyberespace, lieu où se côtoient des millions de personnes à travers le monde.

14. Si le transfert de données à caractère personnel dans le cyberespace est désormais chose courante, ce sujet n'était pas encore à l'ordre du jour lorsque la question de la réglementation du traitement des données est apparue. En d'autres termes, la réalité sociotechnologique a évolué depuis la publication des premiers règlements sur la protection des données à caractère personnel.

15. Or, il se trouve que les informations et les données à caractère personnel sont un élément central et indispensable du cyberespace. Bien que ce terme ait différentes significations, il est utile de rappeler que le cyberespace est composé des éléments suivants :

- Une infrastructure technologique, composée d'une myriade de ressources technologiques (équipements tels que des serveurs, des ordinateurs, des téléphones portables, des tablettes, etc.) situées dans le monde entier ;
- Une plateforme de communication (réseau mondial de communication), d'information et de réseaux interconnectés (Internet), aussi appelée « infrastructure mondiale de l'information » ;
- Des millions de personnes et d'organisations de nationalités diverses, domiciliées dans des pays aux systèmes juridiques différents, qui utilisent les technologies de l'information et de la communication pour interagir avec d'autres personnes, où qu'elles se trouvent, ou pour utiliser des services en ligne ;
- Une quantité phénoménale d'informations (dont des données à caractère personnel) qui circulent en permanence à l'intérieur des pays et par-delà les frontières.

16. Nous assistons progressivement à la migration d'un monde physique délimité par des frontières géographiques vers un cyberespace dématérialisé et sans frontières au sein duquel le nombre de personnes interagissant à un moment donné augmente progressivement.

17. La nature mondiale, internationale et transfrontière de nombreuses activités menées sur Internet (le commerce électronique, par exemple) est l'une des grandes raisons pour lesquelles il nous faut mettre en place une réglementation appropriée pour promouvoir le développement et l'innovation, de même que pour bien protéger les droits des personnes dont les informations sont collectées et utilisées par des

[11] Réseau ibéro-américain de protection des données (2017), « Directrices para la armonización de la protección de datos en la comunidad iberoamericana » (Orientations pour l'harmonisation des règlements relatifs à la protection des données dans la communauté ibéro-américaine), p. 1. On peut également lire dans ce document que l'établissement d'un cadre homogène de réglementation en matière de protection des données, soit par l'adoption d'instruments supranationaux contraignants, soit par l'adoption de lois nationales qui entérinent les principes d'un tel cadre, permettra de développer le commerce dans la zone, en facilitant l'échange d'informations entre les différents opérateurs situés dans les États ibéro-américains, de même qu'avec les pays tiers, en particulier avec les États membres de l'Union européenne, dans des conditions qui ne sont pas restreintes en raison de différences dans le niveau de protection des données à caractère personnel.

entreprises, des particuliers et des administrations un peu partout dans le monde. Il convient de rappeler que si, dans sa Déclaration sur l'utilisation du progrès de la science et de la technique dans l'intérêt de la paix et au profit de l'humanité[12], l'Assemblée générale ne nie pas que « le progrès de la science et de la technique est d'une grande importance pour accélérer le développement économique et social des pays en développement », elle considère également que ce progrès, « tout en augmentant sans cesse les possibilités d'améliorer les conditions de vie des peuples et des nations, peut, dans un certain nombre de cas, engendrer des problèmes sociaux et menacer les droits de l'homme et les libertés fondamentales de la personne humaine ». Elle note par ailleurs qu'il est nécessaire « d'utiliser pleinement le progrès de la science et de la technique pour le bien de l'homme et de neutraliser les conséquences négatives actuelles de certaines réalisations scientifiques et techniques et celles qu'elles pourraient avoir dans l'avenir », estimant dès lors que « tous les États doivent prendre des mesures efficaces, y compris des mesures législatives, afin d'empêcher et d'interdire que les réalisations de la science et de la technique soient utilisées au détriment des droits et des libertés fondamentales de l'homme ainsi que de la dignité de la personne humaine »[13].

II. Rapports des Rapporteurs spéciaux sur le droit à la vie privée consacrés à des questions pertinentes pour la mise à jour de la résolution 45/95

18. Dans un rapport de 2022[14], la Rapporteuse spéciale procède à l'analyse comparative de sept documents internationaux afin de mieux comprendre la portée des principes suivants dans le cadre du traitement des données à caractère personnel : légalité, licéité et légitimité ; consentement ; transparence ; finalité ; loyauté ; proportionnalité ; minimisation ; qualité ; responsabilité et sécurité. Dans cette analyse, elle met également en évidence les points communs qu'ont ces documents internationaux sur ces aspects, dans l'optique de jeter des ponts ou de trouver des chevauchements et de faciliter ainsi l'harmonisation des textes au niveau mondial.

19. Les conclusions de ce rapport sont les suivantes :

- Les principes qui régissent le respect de la vie privée et la protection des données à caractère personnel sont une composante structurelle des systèmes juridiques applicables. Ils fournissent des orientations en matière d'interprétation et contribuent à combler les lacunes de la législation. Ils imposent aux responsables du traitement et aux sous-traitants d'agir de manière appropriée lors du traitement des données à caractère personnel.
- La légalité doit être le fil conducteur de toutes les activités de traitement, tout au long du cycle de vie des données à caractère personnel. Elle repose sur le respect d'une exigence fondamentale : l'existence d'un ou plusieurs des motifs légitimes prévus dans la réglementation applicable.
- Le principe de consentement, qui est étroitement lié au principe de légalité, constitue le motif légitime de traitement des données à caractère personnel le plus courant et est reconnu au niveau international.

[12] Résolution 3384 (XXX) de l'Assemblée générale, en date du 10 novembre 1975.

[13] Ibid., par. 8.

[14] « Principes qui régissent le droit à la vie privée et la protection des données à caractère personnel », Rapport de la Rapporteuse spéciale sur le droit à la vie privée (A/77/196, 20 juillet 2022).

- Le principe de transparence doit être respecté quelle que soit la base juridique qui légitime le traitement.
- Le principe de finalité est établi dans tous les documents d'orientation analysés. La finalité doit être explicite, spécifique, légitime et pertinente. Ces caractéristiques permettent de délimiter les activités de traitement auxquelles les données personnelles seront soumises.
- La loyauté exige que les données personnelles soient traitées dans le respect absolu de toutes les règles et conditions qui ont autorisé leur collecte, et que les moyens de traitement utilisés contribuent à cette exigence.
- En vertu du principe de proportionnalité, l'utilisation des données et les activités de traitement auxquelles elles sont soumises doivent être limitées à la réalisation des finalités pour lesquelles les données ont été collectées.
- La qualité des données personnelles objet du traitement est essentielle à la bonne réalisation des finalités pour lesquelles elles ont été collectées, ainsi qu'à leur traitement ultérieur.
- Le principe de responsabilité vise à renforcer l'obligation de respect des principes et de toute la réglementation sur la protection des données personnelles et de la vie privée, et à faire en sorte que ce principe s'accompagne d'éléments objectifs sur lesquels fonder la réalité de la conformité et l'atteinte de finalités légitimes, dans un climat de confiance et de respect des droits fondamentaux concernés.
- Il ne peut y avoir de protection des données personnelles ni de respect de la vie privée sans sécurité. Garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel est une tâche essentielle et une grande responsabilité. La diversité des technologies et leur constante évolution doivent être prises en compte pour évaluer, de manière responsable et éthique, les risques et les mesures de sécurité appropriées.
- Il existe beaucoup de points communs dans la façon dont les documents d'orientation internationaux définissent les principes de respect de la vie privée et de protection des données à caractère personnel.
- Ces éléments communs mis en évidence peuvent servir de base pour progresser vers un consensus mondial qui nous permettra, conjointement et de manière appropriée, de relever les différents défis liés au traitement des données personnelles. Il s'agit notamment des enjeux inhérents au transfert international de données, à l'utilisation des technologies de l'information et de la communication et de l'intelligence artificielle, dans la mesure où les droits humains méritent le même degré de respect dans les environnements virtuels que dans les situations réelles.
- Il y a lieu de continuer à rechercher un équilibre entre les différents intérêts en jeu dans le traitement des données à caractère personnel à l'ère mondialisée et numérique dans laquelle nous vivons, et ce dans un souci de coopération et d'harmonisation réglementaire.[15]

20. Dans un rapport de 2021 consacré à l'IA et au respect de la vie privée, ainsi qu'au respect de la vie privée des enfants, le Rapporteur spécial fait état des éléments suivants[16] :

[15] Ibid., par. 138 à 150.

[16] « 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 (A/HRC/46/37, 25 janvier 2021).

21. Premièrement, en ce qui concerne la vie privée des enfants, le Rapporteur spécial conclut qu'il faut notamment adopter des politiques, des lois et des règlements qui :

- 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 ;
- Protègent la vie privée au sens large, et pas seulement les données, de manière à permettre aux enfants de développer pleinement leur potentiel ;
- 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 ;
- 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 et garantissent l'adoption de mesures coercitives en cas d'infraction[17].

22. Le Rapporteur spécial recommande par ailleurs :

- 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 ;
- 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+ ;
- 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 ;
- 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 ;
- 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[18].

23. Deuxièmement, en ce qui concerne la protection de la vie privée dans le cadre du développement et du déploiement de solutions d'IA, le Rapporteur spécial formule des recommandations dans le but « de fournir des principes directeurs relatifs à l'utilisation d'informations personnelles et non personnelles dans le contexte des solutions d'IA développées dans le cadre des technologies de l'information et de la communication appliquées, et de mettre en lumière l'importance, pour le traitement

[17] Ibid., par. 126.
[18] Ibid., par. 127.

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 »[19].

24. Sur ce point, le Rapporteur spécial souligne que tant le traitement des données que la décision prise à la suite de ce traitement effectué à l'aide d'outils d'IA exposent le sujet dont les données sont traitées à certains risques. Il juge donc essentiel de définir un certain nombre de principes à prendre en compte dans le cadre de la planification, du développement et du déploiement de solutions d'IA, à savoir : 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 ; g) garanties.

25. Dans un rapport établi ultérieurement, la Rapporteuse spéciale souligne l'importance des principes de transparence et d'explicabilité dans le traitement de données à caractère personnel par l'IA[20].

26. En effet, la transparence et l'explicabilité contribuent non seulement à instaurer la confiance dans l'IA, mais aussi à protéger les droits humains. En vertu de ces principes, d'une part, les personnes disposent en temps utile d'une information complète, simple et claire sur des aspects fondamentaux relatifs à l'utilisation de leurs informations personnelles dans les processus ou projets d'IA et sur les conséquences de ladite utilisation. D'autre part, les personnes affectées par l'IA doivent impérativement être informées des raisons précises à l'origine du préjudice subi. Ainsi, elles seront en mesure d'exercer leurs droits, par exemple le droit à une procédure régulière et le droit à la défense face aux décisions prises par les outils ou les technologies de l'IA.

27. La Rapporteuse spéciale poursuit en soulignant que l'IA comporte différents types de risques. Parmi les éventualités à prendre en compte figurent notamment celles inhérentes au fonctionnement des algorithmes – biais humains, défaillances techniques, vulnérabilités en matière de sécurité, défaillances de mise en œuvre –, ainsi qu'à leur conception et au traitement des données à caractère personnel.

28. En ce qui concerne les données personnelles, la Rapporteuse spéciale fait observer qu'elles constituent un intrant traité par les algorithmes pour produire des résultats. Les intrants peuvent être affectés par des biais (incorporation de données partielles, insuffisantes, obsolètes ou manipulées) ou par un manque de pertinence (données inadaptées, incohérentes ou incomplètes). L'utilisation de données non pertinentes produit donc des résultats erronés. L'algorithme peut quant à lui être affecté par les modèles (biais dans la logique de programmation, inclusion de fonctions imprévues et défaillances inhérentes aux fonctions utilisées pour son codage) et par les erreurs (conditions opérationnelles qui reflètent un fonctionnement différent de celui prévu et qui vont à l'encontre des postulats de la conception envisagée). Tous ces éléments ont une incidence sur les résultats obtenus avec les outils d'IA, qui sont liés à la pertinence et à la précision du résultat de l'exécution de l'algorithme et à la réponse à l'analyse des intrants.

29. Les conclusions de ce rapport sont notamment les suivantes :

a) La transparence et l'explicabilité contribuent à renforcer la confiance dans l'intelligence artificielle et à respecter les droits humains ;

b) Les développeurs d'intelligence artificielle doivent faire preuve de transparence sur la manière dont les données sont traitées (modalités de collecte, de

[19] Ibid., par. 1.

[20] « Principes de transparence et d'explicabilité dans le traitement des données à caractère personnel dans l'intelligence artificielle », Rapport de la Rapporteuse spéciale sur le droit à la vie privée (A/78/310, 30 août 2023).

stockage et d'utilisation), ainsi que sur la manière dont sont prises les décisions fondées sur l'intelligence artificielle, sur la fiabilité de ces décisions et sur la sécurité de l'information ;

c) Les personnes affectées par des décisions prises sur la base de l'intelligence artificielle méritent de recevoir une explication claire, simple, complète, véridique et compréhensible de la motivation de ces décisions. En ce sens, le principe d'explicabilité est d'une importance capitale, non seulement parce qu'il répond au principe de transparence, mais aussi parce qu'il permet aux personnes affectées d'exercer leur droit à la défense et de bénéficier d'une procédure régulière ;

d) L'explicabilité et la transparence exigent la clarté, l'exhaustivité, la véracité, l'impartialité et la divulgation des décisions prises par l'intelligence artificielle, ainsi que de la logique, de la méthode ou du raisonnement permettant de prendre des décisions concernant des êtres humains à partir d'informations et, en particulier, de données à caractère personnel. L'explicabilité et la transparence s'opposent bien entendu à l'opacité, à la dissimulation, à la tromperie, au mensonge et à l'abus de la puissance de calcul, qui sont autant d'indices d'un traitement des données illicite et contraire à l'éthique et d'un manque de respect pour les êtres humains et leur dignité[21].

30. Les recommandations formulées sont les suivantes :

a) Promouvoir la transparence dans le domaine de l'intelligence artificielle afin d'atténuer les risques que l'opacité peut engendrer pour la société et, en particulier, en ce qui concerne la protection des droits humains ;

b) Inscrire le principe d'explicabilité dans leur réglementation, non seulement pour que les personnes comprennent comment les décisions qui les concernent ont été prises, mais aussi pour qu'elles puissent disposer des outils pour défendre leurs droits humains face à l'intelligence artificielle ;

c) Encourager les pratiques éthiques qui garantissent la transparence et l'explicabilité du traitement des données à caractère personnel dans le cadre de projets ou de processus d'intelligence artificielle ;

d) Favoriser, soutenir et faciliter l'éducation et la culture numériques afin d'améliorer la compréhension par les citoyennes et les citoyens des concepts liés à l'intelligence artificielle, à la transparence et à l'explicabilité, de manière à ce que toute personne puisse exiger le respect de ses droits[22].

31. Dans un rapport de 2024[23], la Rapporteuse spéciale effectue une analyse comparative des mécanismes juridiques de protection des données personnelles et de la vie privée à l'ère numérique. Elle y examine également les recours juridiques dont disposent les titulaires de données personnelles pour faire valoir leurs droits, être rétablis dans leurs droits et, s'ils ont subi un préjudice du fait de l'utilisation abusive des données les concernant, demander réparation.

32. Les conclusions de ce rapport sont notamment les suivantes :

a) Dans leur législation, les pays des cinq continents confèrent expressément aux titulaires de données personnelles divers droits qui permettent à ceux-ci d'exercer un contrôle sur l'utilisation de leurs données ;

[21] Ibid., par. 63.

[22] Ibid., par. 64.

[23] « Mécanismes juridiques de protection des données personnelles et de la vie privée à l'ère numérique », Rapport de la Rapporteuse spéciale sur le droit à la vie privée (A/HRC/55/46, 18 janvier 2024).

b) Certaines législations progressent et consacrent de nouveaux droits tels que ceux liés au traitement automatisé et numérisé des données, ainsi que des droits ayant trait aux données communiquées sur Internet, sur les réseaux sociaux ou sur des services équivalents. Ces progrès se traduisent également par une reconnaissance expresse plus détaillée de certains droits ;

c) Dans chacun des systèmes juridiques, des procédures réglementées, qui présentent entre elles des similitudes et des particularités, permettent aux titulaires de données personnelles de faire valoir leurs droits auprès des responsables du traitement ;

d) Parmi les aspects réglementés de la procédure permettant d'exercer ses droits auprès du responsable du traitement figurent, avec des particularités propres à certaines législations, la possibilité pour le titulaire ou son représentant d'introduire une demande d'exercice d'un droit, les formes de réponses possibles, les moyens de réponse, le délai de réponse, la gratuité ou le caractère onéreux de la procédure et l'obligation d'informer le titulaire, en cas de rejet de sa demande, de la possibilité de former un recours auprès d'une autorité administrative ou juridictionnelle ;

e) En ce qui concerne le recours administratif, que le titulaire des données peut former lorsqu'il n'a pas pu exercer son droit ou que le responsable du traitement lui a refusé ce droit, on observe des convergences dans certains aspects de la réglementation. Parmi les particularités propres à certaines législations, on peut citer la gratuité de la réclamation, le délai de procédure et la possibilité de recourir à un mécanisme de règlement des litiges ;

f) En ce qui concerne le recours administratif, les différentes lois prévoient les mesures qui peuvent être ordonnées pour faire droit au recours, dont certaines ont pour objet d'empêcher que la violation ne se poursuive et que la conduite ne se reproduise ;

g) Certaines législations prévoient expressément la possibilité de faire appel des décisions de l'autorité de contrôle auprès d'une autorité administrative supérieure, ainsi que de contester les décisions de l'autorité de contrôle devant certaines juridictions, dans le cadre du droit à une protection juridictionnelle effective ;

h) Afin de garantir un recours effectif en cas de non-respect ou de refus du droit à la protection des données personnelles de la part du responsable du traitement, certaines lois donnent au titulaire des données la possibilité de choisir de saisir l'autorité administrative de contrôle ou d'agir directement en justice auprès de l'organe compétent ;

i) Dans les cinq pays dont la législation a été analysée, les lois réglementent à des degrés divers certains aspects des recours que le titulaire des données personnelles peut utiliser pour obtenir réparation lorsqu'il a subi un dommage du fait d'une violation de la législation sur la protection des données et de la vie privée[24].

33. Dans ce rapport, la Rapporteuse spéciale exhorte les États :

a) À mettre en place, avec le soutien de toutes les parties prenantes, des cadres juridiques multidisciplinaires actualisés et appropriés et, en particulier, à adopter des lois et des règlements adéquats établissant des recours accessibles et utiles afin que les titulaires de données personnelles puissent effectivement faire valoir leurs droits, être rétablis dans leurs droits et obtenir réparation en cas de dommage du fait d'une violation de la réglementation en la matière ;

[24] Ibid., par. 123.

b) Dans le cadre de leur souveraineté, à identifier ou à adopter, dans d'autres lois relatives à la protection des données et de la vie privée, des dispositions qui permettent de mieux garantir le respect effectif de ces droits à l'ère du numérique ;

c) À promouvoir et à encourager en priorité l'information et l'éducation sur les droits de l'homme, en particulier sur la protection des données personnelles et de la vie privée, à tous les niveaux et dans tous les domaines, afin que les titulaires de données connaissent et comprennent leurs droits et soient en mesure de les faire valoir et de recourir, s'il y a lieu, aux mécanismes de protection pour garantir l'exercice de ces droits[25].

34. Enfin, dans un rapport de 2022 consacré à l'application des principes de finalité, de suppression et de responsabilité effective (ou proactive) dans le traitement des données personnelles collectées par des entités publiques pendant la pandémie de maladie à coronavirus (COVID-19)[26], la Rapporteuse spéciale s'emploie à contrôler l'usage qui a été fait, qui est fait et qui sera fait des données à caractère personnel recueillies auprès de millions de personnes de pays du monde entier afin de lutter contre la COVID-19.

35. En se fondant sur l'analyse de la situation dans 20 pays d'Afrique, d'Amérique, d'Asie, d'Europe et d'Océanie, la Rapporteuse spéciale tire un certain nombre de conclusions et formule les recommandations suivantes :

- Vérifier [que les États] respectent effectivement les principes de finalité, de suppression et de responsabilité effective ou proactive eu égard aux données qu'ils ont collectées auprès de millions de personnes dans le but de détecter les cas de COVID-19, de combattre la maladie et de surveiller sa propagation en vue de prévenir sa transmission et de protéger la santé des populations ;
- Renforcer l'application du principe de responsabilité effective ou proactive dans tous les projets ou politiques publiques supposant le traitement de données personnelles ; pour ce faire, il faudra notamment adopter des mesures utiles, appropriées, opportunes et efficaces pour se conformer aux obligations légales énoncées dans la réglementation relative au traitement des données personnelles ; ces mesures doivent être régulièrement évaluées et révisées afin de mesurer leur niveau d'efficacité sur le plan de la conformité et le degré de protection des droits qu'elles offrent aux personnes dont les données personnelles ont été collectées ;
- Mettre en place des procédures et utiliser des outils leur permettant de prouver [que les États] s'acquittent correctement de leurs obligations ; ces procédures et outils doivent être transparents et facilement contrôlables par les autorités publiques compétentes et les citoyens ;
- Mettre en place, grâce à des mesures proactives et préventives, un système de surveillance et de gestion des risques avant de se lancer dans la conception et l'élaboration d'applications et de logiciels qui supposent le traitement de données personnelles à des fins publiques, afin de garantir que les données seront traitées correctement et conformément aux réglementations existantes ;
- Favoriser l'avènement d'une culture publique propice à un traitement des données personnelles transparent, éthique et accompagné de toutes les garanties, afin que ce type de traitement soit une composante essentielle de la conception

[25] Ibid., par. 124.

[26] « Application des principes de finalité, de suppression et de responsabilité effective (ou proactive) dans le traitement des données personnelles collectées par des entités publiques pendant la pandémie de COVID-19 », Rapport de la Rapporteuse spéciale sur le droit à la vie privée (A/HRC/52/37, 27 décembre 2022).

et de l'exécution des projets et politiques publiques qui nécessitent l'utilisation de données personnelles ;

- Renforcer et à consolider la confiance du public dans les projets des entités publiques qui supposent le traitement de données personnelles en mettant en place des mécanismes transparents et accessibles qui permettent à chacun de contrôler, à tout moment et simplement, que les entités publiques se conforment dans la pratique à ce qu'elles annoncent ou promettent dans leurs politiques ou dans les conditions générales de toute activité qui suppose la collecte, l'utilisation, la diffusion ou le traitement de données personnelles[27].

III. Thèmes couverts dans les documents internationaux relatifs au traitement des données personnelles qui ne sont pas abordés dans la résolution 45/95

36. La résolution 45/95 ayant été adoptée en 1990, son contenu n'est plus à jour par rapport aux documents internationaux établis ultérieurement, comme il ressort d'une analyse comparative effectuée avec les documents suivants :

- Cadre sur la vie privée de l'Association de coopération économique Asie-Pacifique (APEC) (2004)
- Normes internationales relatives à la protection des données personnelles et de la vie privée : proposition conjointe pour l'établissement de normes internationales sur la vie privée et la protection des données personnelles (Résolution de Madrid, 2009)
- Recommandation du Conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (2013)
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Estándares de Protección de Datos Personales para los Estados iberoamericanos (normes de protection des données personnelles pour les États ibéro-américains) du Réseau ibéro-américain de protection des données[28], adoptées en 2017
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+) du Conseil de l'Europe (2018)
- Principes actualisés de l'Organisation des États américains relatifs à la vie privée et à la protection des données personnelles (2021)[29]
- Résolution de l'AMVP sur les normes mondiales de protection des données, dans laquelle sont énoncés des principes visant à garantir des niveaux élevés de protection des données et de la vie privée dans le monde entier (2023)[30].

[27] Ibid., par. 27 à 32.

[28] Document adopté lors de la quinzième Réunion ibéro-américaine sur la protection des données du Réseau ibéro-américain de protection des données, tenue à Santiago (Chili) le 22 juin 2017.

[29] Adoptés par le Comité juridique interaméricain et approuvés par l'Assemblée générale de l'Organisation des États américains en 2021.

[30] Voir la note 9.

37. Les principales conclusions de l'analyse comparative sont les suivantes :

Premièrement, en ce qui concerne les principes relatifs au traitement des données personnelles, les principes ci-après ne figurent pas dans la résolution 45/95 : légitimité, transparence, responsabilité effective et confidentialité, comme le montre le tableau ci-dessous :

Tableau 1
Principes relatifs au traitement des données personnelles expressément mentionnés dans les documents internationaux

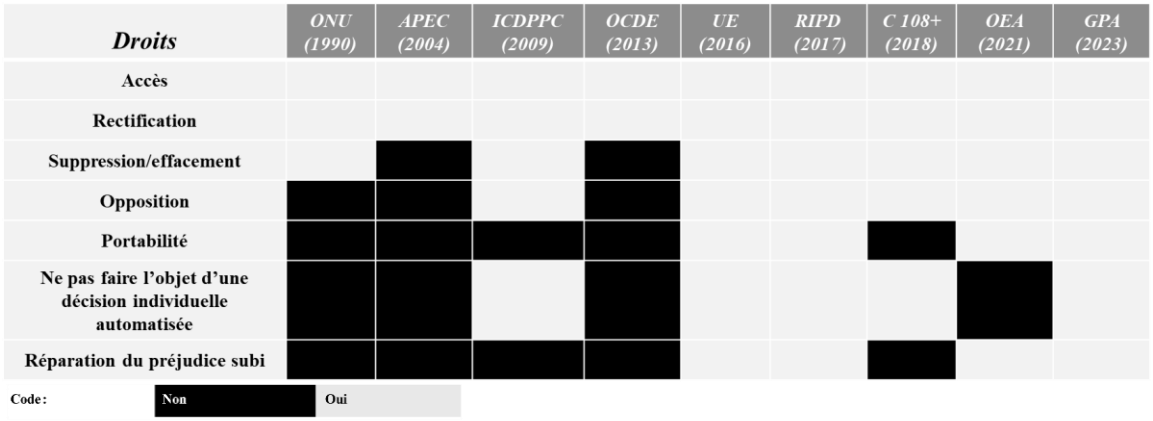
Principe	*ONU (1990)*	*APEC (2004)*	*ICDPPC (2009)*	*OCDE (2013)*	*UE (2016)*	*RIPD (2017)*	*C 108+ (2018)*	*OEA (2021)*	*GPA (2023)*
Légitimité	■								
Licéité									
Loyauté/bonne foi		■							
Transparence	■								
Finalités									
Proportionnalité									
Qualité									
Responsabilité	■								
Ségurité									
Confidentialité	■	■		■					
Caractère temporaire du traitement		■	■	■					
Prévention du préjudice			■	■	■	■	■		
Non-discrimination		■	■	■	■	■	■		

Code : ■ Non Oui

Abréviations : ICDPPC = Conférence internationale des commissaires à la protection des données et à la vie privée ; RIPD = Réseau ibéro-américain de protection des données.

Deuxièmement, en ce qui concerne les droits des titulaires des données personnelles, la résolution 45/95 ne traite pas les droits suivants : droit d'opposition, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée et droit à la réparation du préjudice subi, comme le montre le tableau ci-dessous :

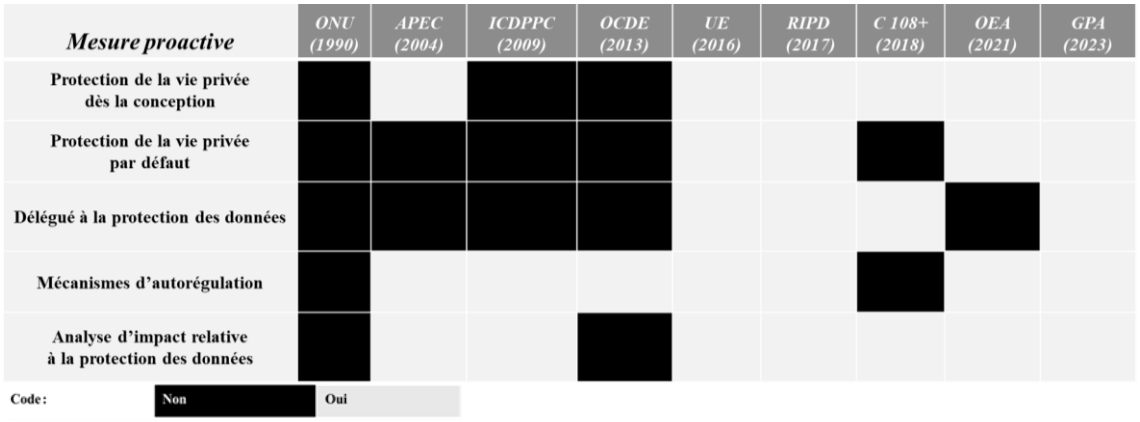
Tableau 2
Droits des titulaires des données expressément mentionnés dans les documents internationaux



Abréviations : ICDPPC = Conférence internationale des commissaires à la protection des données et à la vie privée ; RIPD = Réseau ibéro-américain de protection des données.

Troisièmement, en ce qui concerne les mesures proactives à prendre dans le traitement des données, la résolution susmentionnée ne traite pas de ce qui suit : la protection de la vie privée dès la conception, la protection de la vie privée par défaut, le délégué à la protection des données, les mécanismes d'autorégulation et l'analyse d'impact relative à la protection des données, comme le montre le tableau ci-dessous :

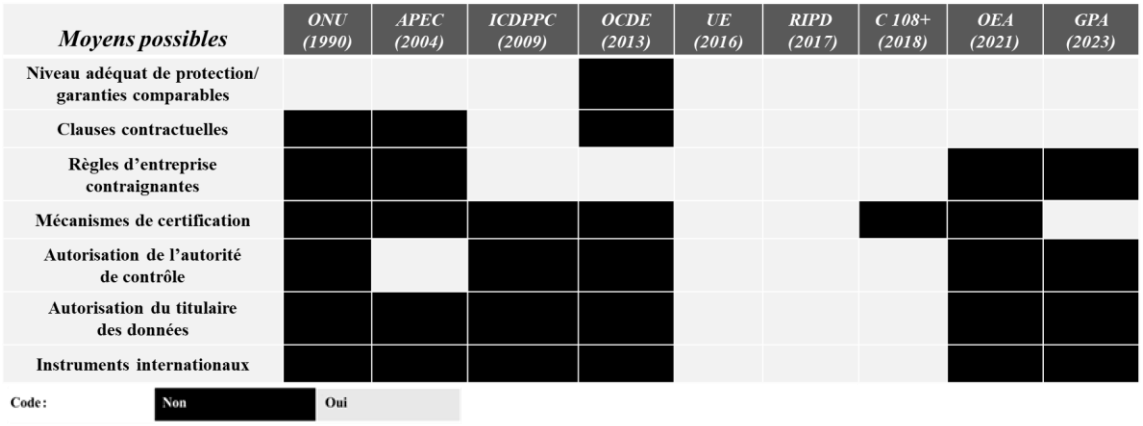
Tableau 3
Mesures proactives à prendre pour le traitement de données personnelles expressément mentionnées dans les documents internationaux



Abréviations : ICDPPC = Conférence internationale des commissaires à la protection des données et à la vie privée ; RIPD = Réseau ibéro-américain de protection des données.

Quatrièmement, pour ce qui est des différents moyens qu'il est possible d'utiliser pour le transfert international de données, la résolution ne comprend pas les éléments suivants : le recours à des clauses contractuelles, le recours à des règles d'entreprise contraignantes, la mise en place de mécanismes de certification, l'autorisation de l'autorité de contrôle, l'autorisation du titulaire des données et les instruments internationaux, comme le montre le tableau ci-dessous :

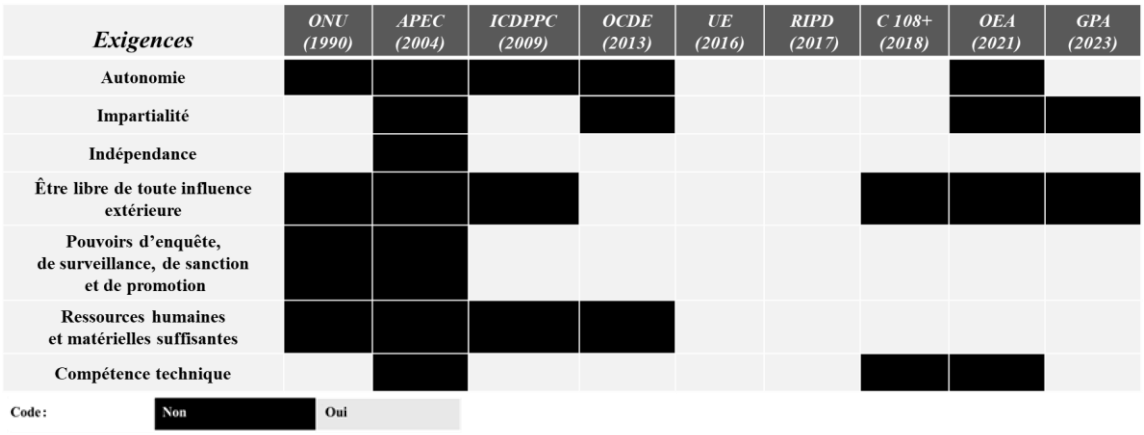
Tableau 4
Moyens qu'il est possible d'utiliser pour le transfert international de données personnelles et qui sont expressément mentionnés dans les documents internationaux



Abréviations : ICDPPC = Conférence internationale des commissaires à la protection des données et à la vie privée ; RIPD = Réseau ibéro-américain de protection des données.

Cinquièmement, en ce qui concerne les exigences auxquelles les autorités de contrôle ou de protection des données personnelles ou les caractéristiques que celles-ci doivent présenter, la résolution n'aborde pas ce qui suit : la nécessité pour les autorités d'être autonomes, d'être libres de toute influence extérieure, d'avoir des pouvoirs d'enquête, de surveillance, de sanction et de promotion, et de disposer de ressources humaines et matérielles suffisantes pour remplir leurs fonctions, comme le montre le tableau ci-dessous :

Tableau 5
Éléments expressément exigés dans les documents internationaux en ce qui concerne les autorités de contrôle ou de protection des données personnelles



Abréviations : ICDPPC = Conférence internationale des commissaires à la protection des données et à la vie privée ; RIPD = Réseau ibéro-américain de protection des données.

Compte tenu des résultats de l'analyse, il est proposé d'ajouter dans la résolution 45/95 les thèmes qui n'y figurent pas actuellement afin que celle-ci soit complète et suffisante pour répondre aux besoins actuels et qu'elle garantisse un traitement adéquat des données à caractère personnel.

Il est donc proposé que l'Assemblée générale adopte la modification ci-après de la résolution 45/95, du 14 décembre 1990 :

Modification qu'il est proposé d'apporter à la résolution 45/95 de l'Assemblée générale en date du 14 décembre 1990

Principes directeurs pour le traitement des données à caractère personnel

Les modalités d'application des règlements concernant le traitement des données à caractère personnel sont laissées à la libre initiative de chaque État sous réserve des orientations suivantes :

A. Principes concernant les garanties minimales qui devraient être prévues dans les législations nationales pour un traitement adéquat des données à caractère personnel

1. Principe de licéité et de loyauté

La collecte, l'utilisation, la circulation, le traitement ou toute autre activité faisant intervenir des données à caractère personnel doivent s'effectuer conformément à la législation de chaque pays et à des fins licites.

Les données concernant les personnes (données à caractère personnel) ne doivent pas être obtenues ou traitées à l'aide de procédés déloyaux, trompeurs, illicites ou frauduleux, ni utilisées à des fins contraires à la dignité humaine ou aux buts et aux principes de la Charte des Nations Unies.

2. Principe d'exactitude ou de qualité des données

Les données à caractère personnel doivent être véridiques, complètes, exactes, tenues à jour, vérifiables, pertinentes au regard de la finalité du traitement et être actualisées chaque fois que nécessaire, soit d'office, par le responsable du traitement ou le sous-traitant, soit à la demande de la personne concernée. Le traitement de données partielles, incomplètes, fragmentées ou de nature à induire en erreur ne doit pas être autorisé.

Les responsables du traitement de données personnelles ou les sous-traitants doivent prendre des mesures pour garantir la qualité, l'actualisation, l'exhaustivité, l'exactitude et la pertinence des informations.

3. Principe de finalité, de nécessité et de proportionnalité, et caractère temporaire du traitement

Le traitement des données doit être limité à des finalités déterminées, explicites et légitimes et les données ne doivent pas être traitées ultérieurement d'une manière incompatible avec celles-ci. Seules doivent être traitées les données nécessaires, pertinentes et utiles à l'accomplissement des buts du traitement. Les données doivent être limitées et ne pas être excessives par rapport aux fins pour laquelle elles ont été collectées.

La finalité du traitement doit être spécifiée, justifiée et, lors de la collecte des données en question, faire l'objet d'une mesure de publicité ou être portée à la connaissance de la personne concernée (titulaire des données), afin qu'il soit ultérieurement possible de vérifier : a) si toutes les données personnelles collectées, enregistrées ou qui font l'objet du traitement restent pertinentes par rapport à la finalité poursuivie ; b) si aucune desdites données personnelles n'est utilisée ou divulguée sans le consentement la personne concernée, ou à des fins incompatibles avec celles qui ont été spécifiées ; c) si la durée de conservation des données personnelles n'excède pas celle permettant d'atteindre la finalité autorisée ou permise pour le traitement des données.

Les données à caractère personnel ne doivent être conservées que pendant le temps nécessaire à l'accomplissement des fins pour lesquelles elles sont collectées ou traitées et doivent être supprimées ou anonymisées lorsqu'elles ne sont plus nécessaires à ces fins.

4. Principe de l'accès par les personnes concernées (titulaires des données)

Toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou l'effacement voulus en cas d'enregistrements illicites, injustifiés ou inexacts, et, lorsqu'elles sont communiquées, d'en connaître les destinataires. Une voie de recours devrait être prévue, le cas échéant, auprès de l'autorité chargée de contrôler le respect des principes. En cas de rectification, le coût devrait être à la charge du responsable du traitement des données personnelles ou du sous-traitant. Il est souhaitable que les dispositions de ce principe s'appliquent à toute personne, quelle que soit sa nationalité ou sa résidence.

5. Principe de non-discrimination et de non-manipulation

Sous réserve des cas de dérogations limitativement prévus sous le principe 6, il convient de ne pas enregistrer les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique d'une personne, les convictions religieuses, philosophiques ou autres de celle-ci, ou son appartenance à une association ou à un syndicat, ou à une organisation sociale ou de défense des droits humains, ou visant à promouvoir les intérêts d'un parti politique ou à garantir les droits de partis politiques d'opposition, ainsi que les données concernant la santé, la vie sexuelle ou les préférences sexuelles et les données génétiques et biométriques permettant d'identifier une personne physique de manière unique ou les données neuronales.

Le traitement des données neuronales, ou neurodonnées, ne peut servir à manipuler ou à altérer la liberté de pensée ou de conscience d'une personne, la rendre dépendante d'un tiers ou influer sur ses idées, sa sécurité et son indépendance, ainsi que sur son identité cérébrale naturelle et son intégrité neurocognitive. Ces données ne peuvent pas non plus être traitées à des fins autres que la promotion de la santé, le diagnostic, la rééducation et les soins palliatifs dans le cadre du droit à la santé, ou les travaux de recherche scientifique dans les domaines de la biologie, de la psychologie et de la médecine visant à atténuer les souffrances ou à améliorer l'état de santé.

6. Faculté de dérogation

Des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées.

Les dérogations au principe 5 relatif à la prohibition de la discrimination, outre qu'elles devraient être soumises aux mêmes garanties que celles prévues pour les dérogations aux principes 1 à 4, ne pourraient être autorisées que dans les limites prévues par la Déclaration universelle des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits et de la lutte contre les discriminations.

7. Principe de sécurité

Des mesures préventives appropriées, raisonnables, suffisantes et utiles doivent être prises en temps opportun pour protéger les fichiers, les bases de données ou les systèmes d'information tant contre les risques naturels, tels que la perte accidentelle ou la destruction par sinistre, que les risques humains, tels que l'accès non autorisé, l'utilisation détournée de données, la contamination par des virus informatiques, l'altération, la perte, la modification, la destruction, l'endommagement ou la divulgation d'informations ou autre forme d'utilisation abusive.

Les mesures de sécurité applicables au traitement des données à caractère personnel doivent régulièrement faire l'objet d'audits, d'examens et de maintenance et être en permanence actualisées.

Il convient également de prendre des mesures pour gérer de manière adéquate et en temps opportun les incidents de sécurité, afin d'éviter tout préjudice aux titulaires de données, aux responsables de traitement, aux sous-traitants et à la société en général.

8. Principe de confidentialité

Toutes les personnes intervenant dans le traitement de données personnelles qui ne sont pas de nature publique sont tenues de garantir la confidentialité des informations, même lorsque leur relation avec l'une ou l'autre des activités de traitement a pris fin, et ne peuvent les fournir ou les communiquer que dans le cadre d'activités autorisées par la loi ou par le titulaire des données.

9. Protection renforcée des données sensibles

Il existe des données sensibles qui touchent la vie privée de leur titulaire ou dont l'utilisation abusive peut susciter la discrimination, telles que les données qui révèlent l'origine raciale ou ethnique, l'orientation politique, les convictions religieuses ou philosophiques, l'appartenance à un syndicat ou à une organisation sociale ou de défense des droits humains, ou qui promeut les intérêts d'un parti politique ou qui protège les droits et les garanties de partis politiques d'opposition, ainsi que les données concernant la santé, la vie sexuelle ou les préférences sexuelles, les neurodonnées (données neuronales) et les données génétiques et biométriques permettant d'identifier une personne physique de manière unique.

Ces données sensibles doivent faire l'objet de mesures spéciales de responsabilité renforcée en matière de sécurité, de confidentialité, d'accès et de limitation de la circulation, afin que nul ne puisse y accéder, ou en faire une utilisation abusive, ni les manipuler ou les détruire.

10. Protection spéciale des données personnelles concernant des enfants et des adolescents

Lors du traitement des données personnelles concernant des enfants et des adolescents, la priorité doit être donnée à la protection de l'intérêt supérieur de ceux-ci, conformément à la Convention relative aux droits de l'enfant et à d'autres instruments internationaux qui visent leur bien-être et leur protection générale.

Les enfants et des adolescents, dans le cadre de leur scolarité, doivent être encouragés à faire une utilisation responsable, appropriée et sûre des technologies, avertis des risques de traitement abusif de leurs données personnelles auxquels ils peuvent être exposés dans les environnements

numériques, et incités à respecter tant leurs libertés et leurs droits que ceux des autres.

Les données personnelles des enfants et des adolescents doivent faire l'objet de mesures spéciales de responsabilité renforcée en matière de sécurité, de confidentialité, d'accès et de limitation de la circulation, afin que nul ne puisse y accéder, ou en faire une utilisation abusive, ni les manipuler ou les détruire.

11. Principe relatif aux décisions individuelles automatisées

Le titulaire des données a le droit de ne pas faire l'objet de décisions qui produisent des effets juridiques le concernant ou l'affectent de manière significative et fondées exclusivement sur un traitement automatisé visant à évaluer, sans intervention humaine, certains aspects personnels le concernant ou à analyser ou prédire des éléments touchant, notamment, son rendement au travail, sa situation économique, son état de santé, ses préférences sexuelles, sa fiabilité ou son comportement.

Ce qui précède ne s'applique pas lorsque le traitement automatisé est nécessaire à la conclusion ou à l'exécution d'un contrat entre le titulaire des données personnelles et le responsable du traitement, lorsque ce traitement est autorisé par le droit interne des États ou lorsqu'il est fondé sur le consentement explicite du titulaire.

Toutefois, lorsque la relation contractuelle le rend nécessaire ou lorsque le titulaire des données a donné son consentement, celui-ci a le droit d'obtenir une intervention humaine, d'obtenir une explication quant à la décision prise, d'exprimer son point de vue et de contester la décision.

12. Principe de transparence

Avant ou au moment de la collecte de données personnelles, il convient d'indiquer l'identité et les coordonnées du responsable des données, les fins précises auxquelles les données seront traitées, le fondement juridique du traitement, les destinataires ou catégories de destinataires auxquels les données seront communiquées, ainsi que les informations qui doivent être transmises et les droits du titulaire à l'égard des données qui doivent être collectées. Lorsque le traitement repose sur le consentement, les données personnelles ne sont collectées qu'avec le consentement préalable, sans équivoque, libre et éclairé de la personne concernée.

Si le titulaire des données fait l'objet d'une décision automatisée, à l'occasion d'un profilage ou d'un processus de décision fondé sur l'intelligence artificielle ou d'autres technologies, il convient de lui communiquer de manière claire et simple ce qui suit :

- Les procédés faisant intervenir l'automatisation, l'intelligence artificielle ou d'autres technologies qui seront utilisés pour le traitement des données ;
- La logique sous-tendant la décision qui le concerne, par des informations claires, véridiques et utiles, afin qu'il ait connaissance des éléments fondamentaux de la prise de décision découlant de ses données personnelles ;
- Les informations qui seront utilisées pour prendre la décision en question ;
- Si la qualité de la décision a été vérifiée dans le cadre d'une supervision humaine qualifiée ;

- Toutes informations supplémentaires lui permettant de savoir en quoi la décision automatisée peut avoir des conséquences, positives, ou négatives, pour lui. Ces informations doivent être formulées dans des termes clairs, simples et faciles à comprendre.

13. Principe d'explicabilité

Le responsable du traitement ou le sous-traitant doit donner au titulaire des données, lorsque celui-ci le demande, des explications claires et compréhensibles sur les informations utilisées et la procédure suivie pour prendre une décision le concernant.

Ces explications doivent non seulement exprimer fidèlement la logique du système appliqué aux fins de la prise de décision, mais aussi être compréhensibles, véridiques, complètes, faciles à comprendre et précises ou concrètes pour l'intéressé. Il convient de donner toutes les informations et explications nécessaires pour que les titulaires de données comprennent comment les décisions qui les concernent ont été prises et qu'ils puissent disposer d'outils pour défendre leurs droits humains ou demander l'examen de la décision.

En outre, il doit y avoir une personne responsable auprès de laquelle les préoccupations ou les objections liées aux décisions automatisées puissent être soulevées et les droits exercés, et qui puisse également déclencher l'évaluation et l'examen du processus de décision automatisée.

14. Principe de responsabilité effective ou proactive (*accountability*)

Les responsables du traitement de données et les sous-traitants doivent adopter et appliquer en temps opportun des mesures techniques, organisationnelles ou autres utiles, appropriées et efficaces pour garantir et démontrer que le traitement est effectué conformément aux principes énoncés dans la présente résolution.

Ces mesures doivent être contrôlées et actualisées périodiquement afin d'établir qu'elles fonctionnent correctement et de mesurer le degré de protection des droits des titulaires des données et de respect des présents principes.

15. Analyses de l'impact du traitement de données

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel en vue de prendre des mesures préventives pour faire face aux risques identifiés et les atténuer.

Une analyse d'impact doit être réalisée, notamment, lorsqu'il s'agit d'évaluer de manière systématique et approfondie des aspects personnels concernant des personnes physiques fondés sur un traitement automatisé, comme le profilage, et sur la base desquels sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire, ou lorsque le traitement massif ou à grande échelle de données sensibles ou de données relatives à des mineurs est envisagé.

16. Protection de la vie privée dès la conception et par défaut

En tenant raisonnablement compte des coûts de mise en œuvre du traitement, de l'état des connaissances et de la nature, du contexte et des finalités du traitement, ainsi que des risques probables et de la gravité de ces risques, le

responsable du traitement (et éventuellement le sous-traitant) doit mettre en œuvre les mesures techniques et organisationnelles propres à rendre effectifs les principes de la présente résolution, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même.

De telles mesures doivent également être mises en œuvre pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique également à la quantité de données à traiter, à l'étendue du traitement, à la durée de conservation des données et à leur accessibilité.

17. Principe de précaution

En cas d'incertitude quant au préjudice que le traitement de données à caractère personnel pourrait causer à leur titulaire ou à la société, et en vue de prévenir des dommages graves et irréversibles, le responsable du traitement ou le sous-traitant doit s'abstenir de procéder à ce traitement ou prendre des mesures de précaution ou préventives pour protéger les droits dudit titulaire, la dignité de celui-ci et d'autres droits humains.

Le principe de précaution s'applique également lorsque le risque encouru ou l'ampleur du dommage causé ou susceptible de survenir ne sont pas connus à l'avance faute de pouvoir déterminer, à moyen ou à long terme, les effets qu'aurait le traitement des données.

18. Principe de l'interprétation la plus favorable ou de prééminence

En cas de doute sur l'interprétation ou l'application des présents principes, l'interprétation la plus favorable au titulaire des données personnelles prévaut.

19. Principe d'autorégulation

Le responsable de traitement peut, de son propre chef, appliquer des dispositifs d'autorégulation contraignants visant, entre autres, à contribuer à la bonne mise en œuvre des présents principes et à permettre le règlement des litiges l'opposant à des titulaires de données, sans préjudice d'autres mécanismes créés par la législation nationale applicable en la matière, compte tenu des caractéristiques du traitement effectué et de la nécessiter de veiller à l'exercice et au respect effectifs des droits du titulaire des données.

Aux fins du paragraphe précédent, des codes de déontologie et des systèmes de certification assortis de labels de confiance, notamment, peuvent être élaborés pour contribuer à la réalisation des objectifs énoncés dans le présent article.

20. Principe de protection effective des droits des titulaires des données à caractère personnel

Des mécanismes utiles, efficaces, simples et rapides sont adoptés pour garantir les droits suivants aux personnes titulaires des données à caractère personnel : droit d'accès, de rectification, de suppression (effacement) et d'opposition, droit à la portabilité, droit de ne pas faire l'objet de décisions automatisées qui produisent des effets juridiques les concernant ou les affectent de manière significative, et droit à la réparation des préjudices causés par le traitement abusif des informations en question.

Outre les procédures juridictionnelles ou administratives prévues par les réglementations nationales, le recours à d'autres moyens de règlement des différends pour résoudre les litiges relatifs au traitement de données à caractère personnel doit être encouragé.

21. Contrôle et sanctions

Chaque État doit désigner l'autorité qui, en conformité avec le système juridique interne, sera chargée de contrôler le respect des principes énoncés dans la présente résolution. Cette autorité doit présenter des garanties d'impartialité, d'indépendance à l'égard des personnes ou organismes responsables des traitements et de leur mise en œuvre, et de compétence technique. En cas de violation des dispositions de la loi interne mettant en œuvre les principes précités, des sanctions pénales ou autres doivent être prévues, ainsi que des recours individuels appropriés.

L'autorité jouit d'une pleine autonomie, est libre de toute influence extérieure, directe ou indirecte, et ne sollicite ni n'accepte aucun ordre ou instruction. Son équipe doit avoir de l'expérience et des compétences spécialisées dans le traitement des données à caractère personnel.

L'autorité est désignée à l'issue d'une procédure publique et transparente, et pour une durée déterminée. Les personnes désignées ne peuvent être démises de leurs fonctions que pour des motifs graves préalablement établis dans la réglementation de chaque pays.

L'autorité doit disposer de pouvoirs d'enquête, de surveillance, de décision, de promotion, de sanction et d'autres pouvoirs nécessaires pour garantir les droits des titulaires de données et le traitement adéquat de ces données. L'autorité doit également disposer de suffisamment de ressources financières, humaines et technologiques pour pouvoir s'acquitter de ses fonctions comme il se doit et en temps opportun.

22. Flux transfrontières de données

Lorsque la législation de deux ou plusieurs pays concernés par un flux transfrontière de données présente des garanties comparables au regard de la protection du traitement des données personnelles, les informations doivent pouvoir circuler aussi librement qu'à l'intérieur de chacun des territoires en question.

En l'absence de garanties suffisantes, des limitations à la circulation des informations ne peuvent être imposées indûment ; la circulation des informations ne peut être limitée que dans la stricte mesure où la protection des droits humains l'exige.

Afin de déterminer l'existence de garanties comparables dans un pays, les éléments suivants, entre autres, peuvent être évalués :

a) Le respect de l'état de droit, le respect des droits humains et des libertés fondamentales, et la législation, tant générale que sectorielle, applicable au traitement des données à caractère personnel.

b) L'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes chargées d'assurer le respect des règles de protection des données et de les faire appliquer, dotées de pouvoirs d'exécution adéquats et de pouvoirs leur permettant d'assister et de conseiller les titulaires de données, ainsi que de coopérer avec les autorités de protection des données.

c) Les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

Le responsable du traitement et le sous-traitant peuvent effectuer des transferts internationaux de données à caractère personnel dans l'un quelconque des cas suivants :

- Lorsqu'il est établi qu'il existe, dans le pays ou la partie de son territoire, le secteur, l'activité ou l'organisation internationale destinataires, des garanties comparables permettant d'assurer le traitement adéquat des données, conformément à la législation nationale du pays d'où celles-ci sont exportées ;
- Lorsque l'exportateur et le destinataire souscrivent des clauses contractuelles ou tout autre instrument juridique offrant des garanties suffisantes et permettant de démontrer la portée du traitement des données, les obligations et responsabilités des parties et les droits des titulaires. L'autorité de contrôle peut valider des clauses contractuelles ou instruments juridiques, selon ce que prévoit la législation nationale ;
- Lorsque l'exportateur et le destinataire adoptent un dispositif d'autorégulation contraignant ou un mécanisme de certification approuvé par l'autorité de protection des données du pays d'où les données sont envoyées ;
- Lorsque le titulaire des données ou l'autorité de contrôle du pays de l'exportateur autorise le transfert, conformément à la législation nationale applicable.

D'autres exceptions peuvent être autorisées, dans des lois nationales ou des instruments internationaux.

23. Collecte internationale de données à caractère personnel

Les États prennent en temps opportun des mesures appropriées et utiles pour assurer le traitement adéquat des données à caractère personnel et la protection effective des droits des personnes concernées par les données que collectent des responsables de traitement ou des sous-traitants se trouvant dans un pays autre que celui du domicile ou de la résidence du titulaire des données et qui n'ont pas de siège physique ou d'établissement dans le pays du domicile ou de la résidence de ce dernier (collecteurs internationaux de données).

En outre, les États coopèrent entre eux, avec les autorités de protection des données et avec les titulaires des données pour atteindre l'objectif énoncé au paragraphe précédent.

Le fait que le collecteur international de données ne se trouve pas ou n'ait pas de résidence physique ou d'établissement dans le pays du titulaire des données ne doit pas entraîner ou favoriser l'impunité ou le défaut de protection des droits des personnes.

24. Champ d'application

Les présents principes doivent s'appliquer, en premier lieu, à tout traitement de données à caractère personnel, public ou privé, quels que soient les moyens ou les technologies utilisés.

B. Application des principes directeurs au traitement des données à caractère personnel par les organisations internationales gouvernementales

Les organisations internationales gouvernementales appliquent les présents principes directeurs au traitement des données à caractère personnel, sous réserve des adaptations nécessaires pour tenir compte des différences qui

peuvent exister entre les fichiers ou systèmes d'information à finalités internes tels que ceux qui concernent la gestion du personnel et les fichiers ou systèmes d'information à finalités externes concernant les tiers en relation avec l'organisation.

Chaque organisation doit désigner l'autorité qui, selon son statut, est compétente pour contrôler la bonne application des présents principes.

Clause humanitaire

Les États prennent des mesures spéciales concernant le traitement des données personnelles pour faciliter et appuyer les actions humanitaires visant à protéger et à aider les personnes vulnérables dans le cadre de conflits armés, de situations de violence, de situations d'urgence ou de catastrophes naturelles.