Nations Unies A/77/196

Assemblée générale

Distr. générale
20 août 2022
Français
Original : anglais

Soixante-dix-septième session
Point 69 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.

22-11362X (F)

Résumé

Les principes qui régissent la vie privée et la protection des données à caractère personnel sont une composante structurelle des systèmes juridiques applicables en la matière, car ils remplissent une double fonction d'interprétation et d'intégration du cadre réglementaire. Ils constituent le moyen le plus précieux et le plus utile pour les responsables du traitement des données et les sous-traitants qui cherchent à assurer un traitement adéquat des données personnelles, en particulier lorsqu'ils doivent faire face aux risques d'utilisation abusive des technologies de l'information et de la communication.

Dans le présent rapport, nous analyserons en particulier les principes suivants, qui fondent l'ensemble du système juridique relatif au droit à la vie privée et à protection des données à caractère personnel : légalité, licéité et légitimité ; consentement ; transparence ; finalité ; loyauté ; proportionnalité ; minimisation ; qualité ; responsabilité et sécurité. Nous réaliserons ensuite une étude comparative à partir de la description de ces principes, telle qu'elle figure dans sept documents d'orientation internationaux. Nous mettrons en évidence leurs éléments communs afin de progresser vers une harmonisation à l'échelle mondiale, de manière à relever les défis de la protection de la vie privée et des données personnelles, un droit humain fondamental qui – de par sa transversalité – favorise le plein exercice d'autres droits fondamentaux comme le droit à la liberté, à l'égalité, à l'honneur et à la dignité humaine à l'ère numérique.

Principes qui régissent le droit à la vie privée et la protection des données à caractère personnel

I. Introduction

1. Dans le domaine du droit à la vie privée et de la protection des données à caractère personnel, il existe des principes directeurs qui fournissent des orientations pour leur interprétation et pour contribuer à combler les lacunes de la législation. Ces principes revêtent une importance fondamentale en ce qui concerne la manière de gérer les problèmes qui se posent lors du traitement des données personnelles au moyen des technologies de l'information et de la communication.

2. Les réglementations nationales et internationales dans ce domaine se caractérisent par leur portée générale. Par conséquent, elles doivent être appliquées lors des différentes activités de traitement des données à caractère personnel, par les responsables de ces activités et les sous-traitants des différents secteurs dans lesquels ils opèrent, qu'ils soient publics ou privés, nationaux ou internationaux, et quelle que soit la technologie utilisée[1]. À cet égard, l'application effective de la réglementation est un objectif essentiel, car dans un système de gouvernement démocratique, la simple reconnaissance et la définition législative des droits fondamentaux ne suffisent pas. Ces droits consacrés doivent s'accompagner de garanties concrètes pour leur mise en œuvre, quel que soit le contexte.

3. Dans ces conditions, les principes directeurs que nous allons analyser sont les moyens les plus précieux et les plus utiles de garantir un traitement adéquat des données personnelles.

4. Les principes qui régissent la vie privée et la protection des données à caractère personnel ne doivent pas être considérés comme de simples recommandations : leur rang est supérieur à celui d'une recommandation, ce qui en fait des composantes structurelles des systèmes juridiques dans ce domaine. Ces principes imposent aux responsables du traitement et aux sous-traitants d'agir de manière appropriée lors du traitement des données à caractère personnel et de gérer les risques d'utilisation abusive des technologies de l'information et de la communication, de l'intelligence artificielle et d'autres évolutions technologiques, ce qui, en retour, permettra aux personnes concernées de conserver leur pouvoir de contrôle sur leurs données personnelles.

5. Ces principes sont étroitement liés entre eux. C'est pourquoi ils doivent être appliqués non seulement individuellement, mais en tant que partie d'un tout auquel ils appartiennent, de manière à mettre en œuvre une gestion correcte des données personnelles, respectueuse des droits et libertés fondamentaux associés.

6. Par ailleurs, il convient de prendre en compte les catégories particulières de données à caractère personnel, notamment les données sensibles. Il existe aujourd'hui un consensus sur les restrictions au traitement de ces données, qui nécessitent une protection accrue dans la mesure où elles touchent à la sphère la plus intime de la personne. Leur traitement peut donc entraîner un risque plus important en matière de droits et libertés fondamentaux.

---

[1] « Cette neutralité technologique est particulièrement importante étant donné la rapidité de l'innovation technique et aide à garantir que la législation puisse s'accommoder des progrès futurs sans devenir obsolète trop rapidement. », Commission des Nations Unies pour le droit commercial international, *Promouvoir la confiance dans le commerce électronique : questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques* (Vienne, 2009).

7. Conformément aux documents d'orientation internationaux, la plupart des pays n'autorisent généralement pas le traitement des données sensibles, sauf dans les cas explicitement prévus par la réglementation. Cette règle trouve sa raison d'être dans la nécessité d'éliminer les risques de discrimination à l'égard des personnes concernées.

8. Il a été jugé opportun que le droit interne définisse les catégories de données personnelles sensibles, en précisant la portée de la protection et les exceptions applicables, car il est légitime que chaque État tienne compte de son contexte (culturel, social ou politique) et des réalités locales lorsqu'il détermine quelles données relèvent de cette catégorie.

9. Le traitement des données personnelles sensibles devrait être autorisé si les lois prévoient des garanties adéquates en matière de protection. Ces garanties devraient expressément inclure la nécessité d'appliquer les principes directeurs sur le respect de la vie privée et la protection des données.

10. Pour contribuer à la réalisation de l'objectif visant à élaborer des principes de protection de la vie privée et des données à caractère personnel applicables à l'échelle mondiale, on s'est attaché, dans le présent rapport, à analyser les principes directeurs figurant dans sept documents d'orientation internationaux sur la question.

11. Les aspects communs fondamentaux de ces documents ont été mis en évidence, de même que certaines dispositions particulières, en vue de rechercher un consensus qui permette d'harmoniser les efforts destinés à faire en sorte que le traitement des données à caractère personnel réponde aux exigences en matière de défense de ce droit ainsi que de respect de la vie privée et de la dignité de la personne à l'ère numérique.

II. Analyse normative

12. Dans ce qui suit, nous analyserons les principes de légalité, de licéité et de légitimité, de consentement, de transparence, de finalité, de loyauté, de proportionnalité, de minimisation, de qualité, de responsabilité et de sécurité. À cette fin, les documents suivants sont les pièces maîtresses de notre analyse :

- Règlement général sur la protection des données de l'Union européenne (Règlement général)[2] ;
- Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108 modernisée)[3] :
- Résolution 45/95 de l'Assemblée générale des Nations Unies, intitulée « Principes directeurs pour la réglementation des fichiers personnels informatisés » (Principes directeurs des Nations Unies) ;
- Normes de protection des données personnelles pour les États ibéro-américains, approuvées par le Réseau ibéro-américain de protection des données (Normes ibéro-américaines)[4] ;
- Recommandations du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

[3] Disponible sur : https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

[4] Réseau ibéro-américain de protection des données, *Normes de protection des données personnelles pour les États ibéro-américains*. Disponible sur : https://www.redipd.org/sites/default/files/inline-files/Estandares_Fr.pdf.

personnel de l'Organisation de Coopération et de Développement Économiques (OCDE) (Lignes directrices de l'OCDE)[5] ;

- Cadre sur la vie privée de l'Association de coopération économique Asie-Pacifique (APEC) (Cadre sur la vie privée de l'APEC)[6] ;
- Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations, adoptés par l'Assemblée générale de l'Organisation des États américains (OEA) (Principes de l'OEA)[7].

Principe de légalité, licéité et légitimité

13. Ce principe signifie que le traitement des données à caractère personnel, tout au long de leur cycle de vie, doit être effectué par le responsable du traitement ou le sous-traitant d'une manière qui respecte les lois applicables, dans la mesure où celles-ci sont conformes aux droits humains internationalement reconnus. Cela implique que, grâce à un traitement approprié et donc licite des données personnelles, le respect de la vie privée ainsi que des autres droits et de la dignité humaine de la personne concernée sera également garanti.

14. Le droit à la protection des données à caractère personnel, reconnu comme contribuant au respect des autres droits[8], permet d'assurer que le traitement correct des données concernant un individu garantit, à son tour, le respect effectif des autres droits fondamentaux auxquels il peut prétendre.

15. S'il est vrai que la légalité doit être le fil conducteur de toutes les activités de traitement des données à caractère personnel tout au long de leur cycle de vie, c'est-à-dire de leur collecte à leur suppression, l'accent est en général mis sur la première d'entre elles, à savoir la collecte des données. En effet, si elles sont obtenues de manière illégale, cela affectera la licéité des activités de traitement ultérieures[9].

16. En ce qui concerne la légitimité du traitement, la Convention 108 modernisée précise que celui-ci doit poursuivre une finalité légitime à chacune de ses étapes, et ce dans le respect de la loi (art. 5.1).

17. Les Principes directeurs des Nations Unies, en vertu du principe de licéité et de loyauté, prévoient que les données personnelles ne devraient pas être obtenues ou traitées à l'aide de procédés illicites ou déloyaux.

18. Les différents documents d'orientation internationaux ont introduit ou intégré d'autres principes de protection des données, qui sont connexes et complémentaires au principe de légalité.

19. Dans cet ordre d'idée, et aux termes de son article 6 et des considérants 39 et 40, le Règlement général considère que le principe de licéité est respecté lorsque le traitement est effectué conformément à l'une des bases juridiques établies par le droit.

20. Dans le cas des Normes ibéro-américaines, le principe de légitimité autorise le traitement des données personnelles sous réserve qu'il soit réalisé en vertu de l'une des bases juridiques prévues par la loi (art. 11).

---

[5] Disponible sur : https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188

[6] Disponible sur : https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

[7] Rapport du Comité juridique interaméricain, *Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones*. 9 avril 2021.

[8] Article 1 de la Convention 108 modernisée.

[9] Paragraphe 7 des Lignes directrices de l'OCDE ; principe 1 des Principes de l'OEA ; article 1 des Principes directeurs des Nations Unies.

21. Les Lignes directrices de l'OCDE indiquent que la collecte des données personnelles devrait être obtenue par des moyens licites et loyaux, et après information de la personne concernée ou avec son consentement (par. 7).

22. La légalité du traitement des données à caractère personnel a pour exigence fondamentale le respect de certains des motifs légitimes établis dans la réglementation applicable. À partir de l'analyse des dispositions des documents d'orientation internationaux, le tableau 1 ci-après liste les motifs légitimes internationalement reconnus.

Tableau 1
Motifs légitimes du traitement des données personnelles

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article*	*Paragraphe*	*Principe*	*Principe*
Consentement de la personne concernée	5.2		11.1.a)	6.1.a)	10.a)	III.24	1
Accord de la personne concernée pour une finalité incompatible avec celle pour laquelle la collecte a été autorisée		3 b)					
Dispositions légales	5.3		14.1		10.b)	IV.25 c)	1
Obligation légale du responsable du traitement			11.1.f)	6.1.c)			1
Contrat ou mesures précontractuelles			11.1.e)	6.1.b)		IV.25 b)	1
Intérêt public			11.1.h)	6.1.e)			1
Intérêt légitime du responsable du traitement			11.1.i)	6.1.f)			1
Intérêts vitaux de la personne concernée ou d'un tiers			11.1.g)	6.1.d)			1
Reconnaissance ou défense des droits de la personne concernée devant une autorité publique			11.1.d)				1
Ordre judiciaire, résolution ou mandat fondé par une autorité publique			11.1.b)				1

23. Dans ce qui suit, les motifs autorisant le traitement des données à caractère personnel sont présentés dans l'ordre de la fréquence de leur apparition, telle qu'elle ressort de l'analyse des documents d'orientation internationaux.

24. Six documents mentionnent le consentement de la personne concernée parmi les fondements légitimes du traitement des données à caractère personnel. Il s'agit là du motif le plus fréquemment évoqué dans les documents analysés.

25. Dans les Principes directeurs des Nations Unies, le consentement n'est pas établi comme un motif autorisant le traitement de manière générale, mais il est prescrit pour les activités de traitement ayant d'autres fins que celles qui ont permis la collecte. Compte tenu de ce qui précède, ainsi que de l'article 1 des Principes directeurs, qui traite du consentement, le traitement des données personnelles peut être autorisé à condition d'utiliser des procédés loyaux, licites et conformes aux buts de la Charte des Nations Unies, ce qui implique que la finalité fasse l'objet d'une mesure de publicité ou que la personne concernée en soit informée.

26. Après le consentement de la personne concernée, les règles de droit ou les dispositions légales existant dans le droit interne de chaque État Membre sont le motif le plus souvent cité, celui-ci figurant dans cinq des documents analysés.

27. Quatre documents font référence aux contrats et mesures précontractuelles comme motif autorisant le traitement. Dans le cadre des relations civiles et commerciales, comme dans celui du commerce électronique, la reconnaissance de ce motif revêt une importance particulière dans le contexte économique de l'ère numérique.

28. Trois documents légitiment le traitement des données pour les motifs suivants : l'obligation légale du responsable du traitement, l'intérêt public, l'intérêt légitime du responsable et les intérêts vitaux de la personne concernée ou d'un tiers. Enfin, deux documents mentionnent la reconnaissance ou la défense des droits de la personne concernée devant une autorité publique, ainsi qu'un ordre judiciaire, une résolution ou un mandat fondé par une autorité publique.

29. En ce qui concerne le droit à la protection des données à caractère personnel, au respect de la vie privée et à la dignité de la personne humaine, et quel que soit le contexte réglementaire, un responsable du traitement et, le cas échéant, un sous-traitant ne peuvent traiter des données personnelles que s'ils agissent en vertu de l'un de ces motifs légitimes.

Principe de consentement

30. Le consentement est une manifestation de volonté, expresse ou tacite, par laquelle un sujet est juridiquement lié. Lorsque la personne concernée donne son consentement, le pouvoir de contrôle sur ses données personnelles, qui lui est dévolu en tant que personne concernée, est directement mis en évidence.

31. Le principe de consentement est étroitement lié au principe de légalité, dans la mesure où il s'agit du motif légitime le plus courant et reconnu au niveau international pour le traitement des données à caractère personnel.

32. Le principe du consentement implique la nécessité pour la personne concernée d'exprimer sa volonté afin que les données puissent être collectées, enregistrées, transformées, communiquées, transférées et, en général, pour que toute activité de traitement puisse être effectuée jusqu'à la suppression des données. Ce motif légitime

et délimite l'ensemble du cycle de vie des données entre les mains du responsable du traitement[10].

33. Dans les documents d'orientation analysés, le consentement est l'un des motifs légitimes les plus importants pour le traitement des données à caractère personnel puisqu'il est spécifiquement prévu comme tel dans six d'entre eux[11], associé à différentes caractéristiques.

34. Ces caractéristiques permettent de définir les conditions dans lesquelles le consentement peut être donné, de manière à refléter le plus fidèlement possible l'expression de la volonté de la personne concernée.

35. Le tableau 2 ci-dessous compare les caractéristiques mentionnées dans les sept documents d'orientation internationaux analysés.

[10] Considérant 32 du Règlement général.

[11] Comme indiqué au point précédent concernant le principe de légalité, licéité et légitimité, dans les Principes directeurs des Nations Unies, le consentement n'est établi comme motif légitime que lorsque les activités de traitement sont réalisées à des fins autres que celles pour lesquelles la collecte des données a été autorisée.

Tableau 2
Caractéristiques du consentement

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article(s)*	*Paragraphe*	*Principe*	*Principe*
Libre	5.2			4.11			2
Spécifique	5.2		12	4.11			2
Éclairé	5.2			7.3 et 4.11	Point 52 de l'exposé des motifs		2
Univoque	5.2		12	4.11			2
Révocable			12.2	7.3			2

36. Comme on peut le constater, la Convention 108 modernisée (art. 5.2), le Règlement général[12] et les Principes actualisés de l'OEA (principe 2) sont les textes qui associent le plus de caractéristiques au type de consentement requis pour la protection des données personnelles, en tant que manifestation fidèle de la volonté de la personne concernée.

37. Ce type de consentement, selon le recensement des caractéristiques indiquées dans les documents, doit être libre, spécifique, éclairé, univoque et révocable. On constate que la révocabilité est une caractéristique a priori absente de la Convention 108 modernisée, de même que des Principes directeurs des Nations Unies (art. 4), des Lignes directrices de l'OCDE et du Cadre sur la vie privée de l'APEC (art. 21 à 23 et 26). Néanmoins, dans les différents documents, une telle possibilité peut être prévue en vertu des droits des personnes concernées[13]. La révocation y est présentée comme un corollaire de la faculté de consentir, mais dans un sens opposé et à un moment postérieur au consentement initial.

38. Dans le cas des Lignes directrices de l'OCDE, la caractéristique de consentement éclairé ne découle pas à proprement parler du libellé de l'article, qui prévoit que la collecte des données doit être effectuée (le cas échéant) après en avoir informé la personne concernée ou avec son consentement. Cependant, l'exposé des motifs des principes note que, si l'obtention du consentement de la personne concernée peut être ou non imposée, l'information doit être l'exigence minimale[14]. Par conséquent, lorsque le consentement est requis pour la collecte de données à caractère personnel, il doit être éclairé, car l'information de la personne concernée est l'exigence minimale à respecter.

39. La caractérisation de l'expression de la volonté autorisant le traitement des données n'apparaît pas toujours dans les articles qui réglementent le principe du consentement, mais il convient de noter que certains documents – comme l'article 4 du Règlement général – prévoient quelques-unes de ces caractéristiques dans les définitions et dans les considérants.

40. Les Principes directeurs des Nations Unies et le Cadre sur la vie privée de l'APEC ne définissent pas les caractéristiques du consentement.

41. Il convient de préciser que, si le consentement est le motif qui légitime le traitement des données à caractère personnel, il doit être donné avant le début des activités auxquelles il se rapporte.

42. Le principe du consentement est directement lié au principe de transparence, dans la mesure où un consentement valablement exprimé par la personne concernée implique qu'elle soit informée de manière adéquate des activités dont ses données personnelles feront l'objet.

43. Il est important de souligner la manière dont les différents documents analysés abordent le consentement au traitement des données personnelles des mineurs. En ce qui concerne la protection des données à caractère personnel, les enfants et les adolescents sont considérés comme un groupe vulnérable particulièrement exposé aux conséquences du traitement des informations les concernant, et leur protection spécifique ainsi que le respect de leur bien-être sont donc de rigueur.

44. Que ce soit dans les Normes ibéro-américaines (art. 13), le Règlement général (art. 8) ou les Principes de l'OEA (principe 2, annotation), le consentement des mineurs est subordonné à l'autorisation des titulaires de la responsabilité parentale ou de ceux qui exercent leur représentation légale, qui seront responsables des

[12] Articles 4.11 ; 6.3 a) et b) ; 6.1 a), b), c), d) et e) ; 7 et 8.

[13] Article 9 de la Convention 108 modernisée ; article 4 des Principes directeurs des Nations Unies.

[14] Exposé des motifs (point 52), p. 19.

conséquences du traitement. Sur ce point, les documents précités disposent également que le droit interne de chaque État peut fixer un âge minimum pour que les mineurs puissent donner eux-mêmes leur consentement, avec les garanties appropriées.

Principe de transparence

45. L'un des principes relatifs au traitement des données à caractère personnel prévoit que celles-ci doivent être traitées par le responsable de manière transparente par rapport à la personne concernée. Ce principe suppose que le responsable du traitement informe la personne concernée des modalités de traitement auxquelles ses informations personnelles seront soumises, dès leur collecte, de manière à ce que la personne concernée soit en mesure d'exercer le pouvoir de contrôle qui lui est dévolu sur ces données.

46. Le tableau 3 ci-dessous recense les informations que les responsables du traitement doivent fournir aux personnes concernées, aux termes des documents d'orientation internationaux analysés.

Tableau 3
Informations devant être fournies aux personnes concernées

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*		*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
				Quand les données sont obtenues auprès de la personne concernée	*Quand les données ne sont pas obtenues auprès de la personne concernée*			
	Article	*Article*	*Article*	*Article(s)*		*Paragraphe*	*Principe*	*Principe*
Identité et coordonnées du responsable du traitement et/ou de son représentant	8.1.a)		16.2a)	13.1.a)	14.1.a)	12	21.d)	2
Existence et caractéristiques principales du traitement			16.1			12	21.a)	
Base juridique du traitement	8.1.b)			13.1.c)	14.1.c) et 14.2b)			2
Finalités du traitement	8.1.b)		16.2b)	13.1.c)	14.1.c)	12	21.b)	2
Catégories de données concernées	8.1.c)				14.1.d)			
Origine des données si elles n'ont pas été obtenues directement de la personne concernée			16.2.e)		14.2.f)			
Destinataires ou catégories de destinataires	8.1.d)		16.2.c)	13.1.e)	14.1.e)		21.c)	2
Information sur les droits et les modalités de leur exercice	8.1.e)		16.2.d	13.2.b) et c)	14.2.c) et d)		21.e)	2
Droit d'introduire une réclamation auprès d'une autorité de contrôle				13.2.d)	14.2.e)			

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*		*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
				Quand les données sont obtenues auprès de la personne concernée	*Quand les données ne sont pas obtenues auprès de la personne concernée*			
	Article	*Article*	*Article*	*Article(s)*		*Paragraphe*	*Principe*	*Principe*
Informations sur l'exigence de fourniture de données si elle a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir ses données personnelles, et sur les conséquences de leur non-fourniture				13.2.e)				
Existence d'une prise de décision automatisée, y compris un profilage, et informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement				13.2.f)	14.2.g)			
Informations s'il est prévu un traitement ultérieur pour une finalité autre que celle pour laquelle les données ont été obtenues				13.3	14.4			
Coordonnées du délégué à la protection des données				13.1.b)	14.1.b)			

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*		*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
				Quand les données sont obtenues auprès de la personne concernée	*Quand les données ne sont pas obtenues auprès de la personne concernée*			
	Article	*Article*	*Article*	*Article(s)*		*Paragraphe*	*Principe*	*Principe*
Durée de conservation ou critères de détermination de cette durée				13.2.a)	14.2.a)			
Prévision de communication ou de transferts des données, et réglementation qui l'autorise				13.1.f)	14.1.f)			
Informations devant être transférées								2
Objectifs qui motivent le transfert des données			16.2.c)					

47. Comme on peut le constater, parmi les sept documents d'orientation internationaux analysés, les Principes directeurs des Nations Unies n'ont pas réglementé le principe de transparence. Par conséquent, nous examinerons la récurrence des dispositions relatives aux informations qui, selon les six autres documents, doivent être fournies aux personnes concernées, conformément au principe de transparence.

48. Six documents précisent que l'identité et les coordonnées du responsable du traitement des données ou de son représentant, ainsi que les finalités ou les objectifs du traitement doivent être communiqués. Ces informations constituent les principaux fondements de la transparence.

49. Cinq documents indiquent que la personne concernée doit être informée de ses droits et de la manière de les exercer, ainsi que des destinataires ou de la catégorie de destinataires des données. En ce qui concerne l'information de la personne concernée sur les droits dont elle dispose en tant que telle, il est important qu'elle soit dans des conditions lui permettant d'exercer son pouvoir de contrôle sur ses données à caractère personnel.

50. Trois documents précisent que des informations doivent être fournies sur la ou les bases légales du traitement, ainsi que sur l'existence ou les caractéristiques principales du traitement.

51. Le principe de transparence doit être respecté quelle que soit la base juridique qui légitime le traitement. Il peut y avoir des exceptions, liées au moment de la fourniture de l'information à la personne concernée [15], ou lorsque la personne concernée n'est pas la source à partir de laquelle ses données personnelles sont collectées [16]. Néanmoins, ces exceptions devraient s'appliquer de manière à rechercher la plus grande transparence possible et à respecter la loyauté.

52. Deux documents prescrivent la divulgation de la catégorie de données traitées et de l'origine des données lorsqu'elles n'ont pas été obtenues directement auprès de la personne concernée.

53. La communication d'autres informations peut aussi être prévue dans un seul document d'orientation international, où il est établi que ces informations doivent être fournies à la personne concernée dans la mesure où elles visent à lui assurer de meilleures conditions d'exercice de son pouvoir de contrôle.

54. C'est notamment le cas des Normes ibéro-américaines à propos des finalités qui motivent les transferts de données, et du Règlement général en ce qui concerne les éléments suivants : coordonnées du délégué à la protection des données ; durée de conservation des données ou critères utilisés pour déterminer cette durée ; prévision de communication ou de transferts des données et réglementation qui l'autorise ; droit d'introduire une réclamation auprès d'une autorité de contrôle ; informations sur l'exigence de fourniture de données si elle a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir ses données personnelles, et sur les conséquences de leur non-fourniture ; existence d'une prise de décision automatisée, y compris un profilage, et informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement ; informations s'il est prévu un traitement ultérieur pour une finalité autre que celle pour laquelle les données ont été obtenues.

55. Parmi les informations uniquement prévues par le Règlement général, nous n'en citerons qu'une, qui vise à permettre à la personne concernée de comprendre les

[15] Article 22 du Cadre sur la vie privée de l'APEC.

[16] Article 8.3 de la Convention 108 modernisée.

modalités du traitement auquel seront soumises ses données, par exemple s'il s'agit d'intelligence artificielle. La disposition en question prévoit qu'il faut lui fournir : « des informations utiles concernant la logique sous-jacente » et « l'importance et les conséquences prévues »[17].

56. Pour respecter le principe de transparence, l'information dont doit disposer la personne concernée doit être communiquée dans un langage clair, simple et facile à comprendre[18], en particulier s'il s'agit d'enfants et d'adolescents[19].

57. Il convient d'ajouter le souci particulier d'une action vigilante du responsable lors du traitement des données à caractère personnel, qui devrait pouvoir se référer à des politiques transparentes pour le traitement des données personnelles[20].

Principe de finalité

58. Le principe de finalité guide et délimite toutes les activités de traitement des données personnelles, de la collecte à la suppression. En règle générale, la finalité est définie par le responsable du traitement, mais cette règle ne s'applique pas si la finalité n'est pas associée à l'un des motifs légitimes autorisant le responsable à traiter les données.

59. Dès la collecte des données, la finalité doit répondre à certaines caractéristiques, qui sont mentionnées dans les documents d'orientation internationaux analysés. Ainsi, elle doit être explicite, spécifique, légitime et pertinente. Une fois réunies les conditions établies dans la réglementation pour définir la ou les finalités, ces caractéristiques permettront de délimiter les activités de traitement auxquelles les données personnelles pourront être soumises.

60. Selon ce principe, les données ne peuvent être utilisées que dans les limites de la finalité pour laquelle elles ont été collectées. Il s'agit là d'une restriction applicable aux différentes activités de traitement, de la collecte jusqu'au transfert, en passant par la conservation, la modification et la communication, ainsi que pour tout autre traitement des données, jusqu'à leur suppression.

61. Par conséquent, aucune activité de traitement ne doit aller au-delà de ce qui est autorisé conformément aux finalités initialement définies, comme indiqué dans les différents documents d'orientation [21], sauf autorisation expresse dans la réglementation applicable et sous réserve des garanties appropriées. À titre d'exemple, le Cadre sur la vie privée de l'APEC[22] prévoit la possibilité d'utiliser les données à d'autres fins à condition que celles-ci soient compatibles avec les finalités initialement définies.

62. Le principe de finalité est établi dans tous les documents analysés[23], qui en précisent ses caractéristiques et la conséquence de son application dans la pratique. Il

---

[17] Agence espagnole de protection des données. *Adecuación al Reglamento General de Protección de Datos de tratamientos que incorporan inteligencia artificial: una introducción,* février 2020, p. 24. Disponible sur : https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[18] Article 16.3 des Normes ibéro-américaines ; article 12.1 du Règlement général ; article 21 du Cadre sur la vie privée de l'APEC.

[19] Article 16.3 des Normes ibéro-américaines ; article 12.1 du Règlement général.

[20] Article 16.4 des Normes ibéro-américaines ; paragraphe 12 des Lignes directrices de l'OCDE ; article 21 du Cadre sur la vie privée de l'APEC.

[21] Article 5.4 b) de la Convention 108 modernisée ; article 3 des Principes directeurs des Nations Unies ; article 17 des Normes ibéro-américaines ; article 5.1 b) du Règlement général ; paragraphe 9 des Lignes directrices de l'OCDE ; articles 24 et 25 du Cadre sur la vie privée de l'APEC ; principe 1 des Principes de l'OEA.

[22] Article 25, titre IV du Cadre sur la vie privée de l'APEC.

[23] Article 5.4 b) de la Convention 108 modernisée ; article 3 des Principes directeurs des Nations Unies ; article 17 des Normes ibéro-américaines ; article 5.1 b) du Règlement général ;

est étroitement lié au principe de légalité et licéité, étant donné que la légitimité des fins poursuivies est l'une de ces caractéristiques.

63. Les documents d'orientation internationaux énoncent les caractéristiques que la finalité doit réunir pour permettre le traitement des données à caractère personnel. Comme le montre le tableau ci-dessous, la finalité doit être explicite, spécifique, légitime et pertinente :

paragraphe 9 des Lignes directrices de l'OCDE ; articles 24 et 25 du Cadre sur la vie privée de l'APEC ; principe 1 des Principes de l'OEA.

Tableau 4
Caractéristiques de la finalité

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article*	*Paragraphe*	*Principe(s)*	*Principe*
Explicite	5.4 b)	3	17	5.1 b)	9	24 et 25	1
Spécifique	5.4 b)	3	17	5.1 b)	9	24 et 25	
Légitime	5.4 b)	3	17	5.1 b)		24 et 25	1
Pertinente	5.4 b)	3	17	5.1 b)	9	24 et 25	

64. En ce qui concerne la légitimité, seul le paragraphe 9 des Lignes directrices de l'OCDE ne la mentionne pas en tant que caractéristique des finalités du traitement des données. Cette absence peut être due à un simple choix rédactionnel, tout comme au fait d'omettre un élément qui en principe paraît implicite dans l'analyse de l'ensemble de ce document d'orientation.

65. Dans le cas des Principes de l'OEA, et bien qu'elles ne figurent pas explicitement dans l'énoncé du principe 1, toutes les caractéristiques de la finalité sont mentionnées dans l'annotation dudit principe.

66. Quant à la spécificité du traitement par rapport à une finalité donnée, il convient de noter que le Règlement général (article 5.1), les Normes ibéro-américaines (article 17.3), la Convention 108 modernisée [article 5.4 b)]et les Principes de l'OEA (principe 4) prévoient la possibilité d'utiliser les données à des fins autres que celles pour lesquelles elles ont été collectées, pour autant qu'elles aient un but statistique, historique ou scientifique.

67. Comme indiqué plus haut, la ou les finalités légitimes qui ont autorisé le traitement délimitent les actions du responsable du traitement des données et, le cas échéant, du sous-traitant. Par conséquent, la légitimité de la poursuite du traitement devient caduque une fois la finalité expirée ou atteinte, sauf si la réglementation applicable le prévoit expressément, ce qui fonde un nouveau motif légitime.

Principe de loyauté

68. Ce principe signifie que les données personnelles doivent être traitées dans le respect absolu de toutes les règles et conditions qui ont autorisé leur collecte, et que les moyens de traitement utilisés doivent contribuer à cette exigence.

69. Nous analyserons dans ce qui suit les documents d'orientation internationaux dans lesquels ce principe est réglementé.

70. L'article 1 des Principes directeurs des Nations Unies établit le principe de licéité et de loyauté, dont l'objectif est que les données ne soient pas obtenues ou traitées à l'aide de procédés illicites ou déloyaux, ni utilisées à des fins contraires aux principes de la Charte des Nations Unies. Plus généralement, cela implique que la personne concernée ne fasse pas l'objet de discrimination arbitraire, que le traitement des données soit effectué conformément aux normes et principes internationaux, et que les droits des personnes soient strictement respectés.

71. Aux termes des Normes ibéro-américaines, ce principe est dit de fidélité (art. 15). Selon ce principe, le responsable du traitement a l'obligation de privilégier la protection des intérêts de la personne concernée et de s'abstenir de traiter les données par des moyens trompeurs ou frauduleux. Les traitements qui entraînent une discrimination injuste ou arbitraire à l'encontre des personnes concernées sont considérés comme déloyaux.

72. De même, l'article 5.1 a), du Règlement général dispose que l'un des principes à respecter dans le traitement des données à caractère personnel est celui de la loyauté, au même titre que les principes de licéité et de transparence.

73. Les Lignes directrices de l'OCDE font référence à la loyauté dans le cadre du principe de la limitation en matière de collecte des données (par. 7). Cet article couvre deux aspects : a) les limites en matière de collecte ; b) les prescriptions relatives aux méthodes de collecte, aspect pour lequel il est précisé que les données devraient être obtenues par des moyens licites et loyaux.

74. Pour sa part, le Cadre sur la vie privée de l'APEC, dans son article 24, évoque d'une certaine manière le principe de loyauté en précisant que les méthodes de collecte doivent être licites et honnêtes.

75. Par ailleurs, la Convention 108 modernisée ne définit pas expressément ce principe, mais on peut en déduire qu'il est établi lorsqu'elle prévoit, dans son article 5.4 a), que les données faisant l'objet d'un traitement doivent être utilisées loyalement, sans limiter cette condition à la première activité, à savoir la collecte, mais à toute activité qui implique un traitement des données.

76. La loyauté figure dans le titre du premier des Principes de l'OEA, « Finalités légitimes et loyauté », qui stipule que « les données personnelles ne devraient être collectées qu'à des fins légitimes et par des moyens loyaux et licites ». Ici, la loyauté est expressément prescrite en ce qui concerne les moyens utilisés pour la collecte des données à caractère personnel.

77. Dans les Principes de l'OEA, il est précisé que « la loyauté est contextuelle et dépend des circonstances ». Cela suppose qu'il faut offrir aux personnes concernées des modalités adaptées quant à la manière et au moment de communiquer leurs données, en excluant l'obtention de celles-ci par la fraude, la tromperie et sous de faux prétextes.

78. La loyauté doit être assurée dans toutes les activités de traitement des données à caractère personnel. Le fait que les documents d'orientation internationaux mettent l'accent sur l'activité de collecte souligne que l'emploi de toute méthode inappropriée ou illicite lors de cette étape initiale peut entacher et influencer les activités de traitement ultérieures.

79. Il ne fait aucun doute que la loyauté doit caractériser le comportement du responsable du traitement et du sous-traitant tout au long du cycle de vie des données à caractère personnel, quels que soient le contexte et la technologie utilisée. Agir de manière loyale implique la responsabilité, l'éthique et le respect de la loi applicable, au regard des différents principes.

Principe de proportionnalité

80. Le principe de proportionnalité impose des limitations au traitement des données à caractère personnel. Conformément à ce principe, 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[24].

81. Il convient de garder à l'esprit que ce principe doit être respecté à tous les stades du traitement, dès qu'il est décidé de l'effectuer ou non, et ce afin que l'étape de la collecte soit menée de manière appropriée et licite.

82. Deux autres principes sont étroitement liés à la proportionnalité : le principe de finalité en vertu duquel les données doivent être traitées de manière compatible avec la finalité pour laquelle elles ont été collectées, et le principe de minimisation qui prévoit que les données utilisées doivent être limitées au minimum nécessaire pour atteindre la finalité définie.

83. Parmi les exigences du principe de proportionnalité figure l'évaluation que le responsable du traitement doit conduire afin de choisir, parmi les différents traitements qui lui permettent d'atteindre la finalité autorisée, le moins attentatoire à

[24] Articles 5.1 et 5.4 c) de la Convention 108 modernisée ; article 18.1 des Normes ibéro-américaines ; article 24 du Cadre sur la vie privée de l'APEC ; article 5.1 c) du Règlement général ; article 3 a) des Principes directeurs des Nations Unies ; paragraphe 9 des Lignes directrices de l'OCDE ; principes 3 et 4 des Principes de l'OEA.

la vie privée et à l'intimité. Cette évaluation devient particulièrement nécessaire en cas de recours à certaines technologies de l'information et de la communication qui pourraient menacer les droits fondamentaux.

84. Ce principe est encadré par tous les documents d'orientation internationaux analysés, soit de manière spécifique comme dans le cas des Normes ibéro-américaines (art. 18), soit dans le cadre d'autres principes. Dans les Principes directeurs des Nations Unies, il est contenu dans le principe de finalité [art. 3 a)] ; dans la Convention 108 modernisée, il l'est dans l'article sur la légitimité du traitement et la qualité des données [art. 5.1 et 5.4 c)] ; dans le Règlement général, il est mentionné avec le principe de minimisation des données [article 5.1 c)] ; le Cadre sur la vie privée de l'APEC le réglemente dans le cadre du principe de limitation de la collecte (art. 24) ; dans les Lignes directrices de l'OCDE, il est traité dans le cadre du principe de spécification des finalités (par. 9) ; enfin, dans les Principes de l'OEA, il est contenu dans le principe de pertinence et de nécessité (principe 3) et dans celui relatif à la limitation du traitement et de la conservation (principe 4).

85. Comme le montre le tableau 5 ci-après, on constate que les Normes ibéro-américaines, le Règlement général, les Principes directeurs des Nations Unies et les Principes de l'OEA font référence à la pertinence des données au regard de la finalité. Par ailleurs, la Convention 108 modernisée, les Normes ibéro-américaines, le Règlement général et les Principes de l'OEA précisent que les données doivent être en adéquation avec la finalité.

86. Tous les documents d'orientation internationaux analysés, à l'exception des Principes directeurs des Nations Unies, indiquent d'une manière ou d'une autre que les données doivent être limitées et ne doivent pas être excessives par rapport à la finalité pour laquelle elles ont été collectées. Les Normes ibéro-américaines, le Règlement général, le Cadre sur la vie privée de l'APEC et les Principes de l'OEA prévoient que les données doivent être limitées à ce qui est nécessaire par rapport à la finalité.

87. La Convention 108 modernisée indique que les données ne doivent pas être excessives au regard des finalités pour lesquelles elles sont traitées, en précisant aussi qu'elles doivent être pertinentes par rapport à la finalité et que le traitement devra être proportionné à la finalité légitime poursuivie. Les Lignes directrices de l'OCDE soulignent que l'utilisation des données devrait être limitée à l'atteinte des finalités déterminées au moment de leur collecte, ou à d'autres fins qui ne soient pas incompatibles avec les précédentes.

Tableau 5
Limites qui définissent le principe de proportionnalité

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article*	*Paragraphe*	*Principe*	*Principe*
Adéquation aux finalités	5.4.c)		18.1	5.1 c)			3
Pertinence au regard des finalités	5.4.c)	3.a)	18.1	5.1 c)			3
Données limitées et non excessives au regard de la finalité	5.4.c.)		18.1	5.1 c)	9	24	3

88. En ce qui concerne le principe de proportionnalité, on peut observer que certains documents d'orientation internationaux font expressément référence aux « données à caractère personnel », par exemple les Normes ibéro-américaines, le Cadre sur la vie privée de l'APEC, le Règlement général et les Principes directeurs des Nations Unies. Les Lignes directrices de l'OCDE évoquent le « traitement » de ces données, et les autres documents se réfèrent aussi bien aux données personnelles qu'au traitement dont elles font l'objet, à l'image de la Convention 108 modernisée et des Principes de l'OEA.

89. Toutefois, et en tenant compte de l'intégralité du texte des documents d'orientation internationaux, en règle générale, le principe de proportionnalité doit être respecté tant en ce qui concerne les données à caractère personnel collectées que pour les activités de traitement auxquelles elles seront soumises puisque, dans les deux cas, le caractère adéquat, pertinent et limité aux fins légitimes pour lesquelles les données ont été collectées est prescrit.

Principe de minimisation

90. La minimisation est le principe selon lequel les données doivent à tout moment être limitées à ce qui est nécessaire pour atteindre la finalité définie.

91. Par conséquent, ce principe est étroitement lié au principe de finalité qui constitue la référence pour délimiter la quantité de données à traiter.

92. Le Règlement général est le seul document qui réglemente explicitement le principe de minimisation (art. 5.1 c), en précisant que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Dans les autres documents analysés[25], la teneur de ce principe est englobée dans le principe de proportionnalité ou un autre principe.

93. Le principe de minimisation est également lié à certaines obligations que le Règlement général impose au responsable du traitement et au sous-traitant, comme la protection des données dès la conception et la protection des données par défaut. En tant que mesure de prévention, la minimisation contribue à réduire le risque de failles de sécurité et leur impact sur les bases de données.

94. Ainsi que le stipule l'article 25.2 du Règlement général, « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. »

95. Le principe de minimisation doit être respecté avec la plus grande rigueur, compte tenu de l'utilisation croissante des technologies de l'information et de la communication pour le traitement des données à caractère personnel.

Principe de qualité

96. Le principe de qualité implique que les données doivent être précises, exactes, complètes et tenues à jour, ce qui oblige les responsables du traitement à mettre en place des mesures pour s'y conformer. Dans certains documents d'orientation

[25] Article 18 des Normes ibéro-américaines ; article 3 des Principes directeurs des Nations Unies ; articles 5.1 et 5.4 c) de la Convention 108 modernisée ; article 24 du Cadre sur la vie privée de l'APEC ; paragraphe 9 des Lignes directrices de l'OCDE ; principes 3 et 4 des Principes de l'OEA.

internationaux, cette disposition est aussi appelée principe d'exactitude [26] ou d'intégrité[27].

97. Comme indiqué dans le tableau 6 ci-dessous, les données à caractère personnel doivent être précises, complètes et exactes tout au long du processus de traitement et elles doivent être mises à jour chaque fois que nécessaire, soit d'office par le responsable du traitement ou le sous-traitant, soit à la demande de la personne concernée.

[26] Article 2 des Principes directeurs des Nations Unies et principe 7 des Principes de l'OEA.
[27] Article 27 du Cadre sur la vie privée de l'APEC.

Tableau 6
Caractéristiques de la qualité des données

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article*	*Paragraphe*	*Principe*	*Principe*
Précises/exactes	5. 4.d)	2	19.1	5.1.d)	8	27	7
Tenues à jour	5. 4.d)	2	19.1	5.1.d)	8	27	7
Complètes		2	19.1		8	27	7

98. L'article 5.4 d) de la Convention 108 modernisée fait référence à la nécessité d'exactitude et de mise à jour des données. L'article 2 des Principes directeurs des Nations Unies mentionne l'obligation de vérifier l'exactitude et la pertinence des données, de veiller à ce qu'elles demeurent aussi complètes que possible pour éviter les erreurs par omission et qu'elles soient mises à jour périodiquement.

99. Les cinq documents d'orientation internationaux cités ci-dessous lient expressément le principe de qualité au principe de finalité du traitement.

100. Les Normes ibéro-américaines, dans leur article 19, font obligation au responsable de prendre « les mesures nécessaires pour que les données personnelles en sa possession demeurent identiques, complètes et à jour, de sorte que leur véracité ne soit pas modifiée pour la réalisation des fins qui ont motivé leur traitement ».

101. Le Règlement général précise que les données doivent être exactes et, si nécessaire, tenues à jour ; [et que] toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder [art. 5.1 d)].

102. Les Lignes directrices de l'OCDE (par. 8) et le Cadre sur la vie privée de l'APEC (art. 27) disposent que les données doivent être exactes, complètes et tenues à jour. De même, en ce qui concerne le principe d'exactitude, les Principes de l'OEA disposent que les données « devraient demeurer exactes, complètes et à jour, dans la limite nécessaire aux finalités du traitement, de telle sorte que leur validité ne soit pas compromise » (principe 7).

103. 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. Veiller à la qualité des données est un gage de responsabilité pour l'atteinte des finalités autorisées.

104. Afin de pleinement respecter le principe de qualité, les responsables du traitement et les sous-traitants doivent mettre en œuvre, au sein de leurs organisations, des mesures visant à garantir que les données à caractère personnel qu'ils collectent et gèrent sont précises, exactes, complètes ou exhaustives et tenues à jour. L'objectif sera de réaliser les finalités autorisées dans le respect des droits des personnes concernées, ce qui est dans l'intérêt des responsables du traitement et des sous-traitants. Ce qui précède est indépendant des actions que la personne concernée par les données à caractère personnel décide d'entreprendre et qui visent à assurer la qualité de ses données personnelles, lorsque celles-ci sont traitées par une autre personne.

Principe de responsabilité

105. Le principe de responsabilité peut être analysé selon deux aspects : d'une part, les responsables du traitement des données et les sous-traitants doivent mettre en œuvre des mécanismes qui permettent de respecter les principes relatifs à la protection des données et de la vie privée, en préservant et en garantissant les droits et libertés des personnes concernées. D'autre part, ces responsables et sous-traitants doivent être en mesure de garantir et de démontrer le respect de ces principes.

106. Parmi les documents d'orientation internationaux analysés, on constate que ce principe est établi à l'article 20 des Normes ibéro-américaines, aux termes duquel le responsable doit mettre en œuvre les mécanismes nécessaires pour prouver le respect des principes et obligations établis dans ces Normes, ainsi que pour rendre des comptes sur le traitement des données personnelles en sa possession à la personne concernée et à l'autorité de contrôle. Pour ce faire, il pourra appliquer des normes, de bonnes pratiques nationales ou internationales, des schémas d'autorégulation, des

systèmes de certification ou tout autre mécanisme qu'il juge approprié à ces fins. Ceci s'applique aussi lorsque les données personnelles seront traitées par une personne au nom du responsable, ainsi qu'au moment d'effectuer des transferts de données personnelles.

107. L'article 20.3 des Normes ibéro-américaines fournit une liste de mécanismes que le responsable pourra adopter pour respecter le principe de responsabilité, mécanismes qu'il devra examiner et évaluer à tout moment afin de mesurer leur niveau d'efficacité quant au respect de la législation nationale applicable.

108. Dans le Règlement général, le principe dit de « responsabilité » fait l'objet de l'article 5.2. Il peut être défini comme la nécessité ou l'obligation pour le responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données personnelles est effectué conformément au Règlement (art. 24), et en particulier dans le respect des principes de licéité, loyauté et transparence, de limitation des finalités, de minimisation, d'exactitude, de limitation de la conservation, et d'intégrité et confidentialité (art. 5.1). Pour cela, le responsable doit mettre en place des mécanismes qui permettent de garantir le respect de la réglementation et de démontrer que celle-ci est effectivement appliquée et respectée (art. 5.2).

109. Le Règlement général prévoit un certain nombre de dispositions pour respecter le principe de responsabilité, et notamment : la protection des données dès la conception et la protection des données par défaut (art. 25) ; la tenue d'un registre des activités de traitement (art. 30) ; la mise en œuvre de mesures de sécurité du traitement (art. 32) ; la notification à l'autorité de contrôle et à la personne concernée de violations de données à caractère personnel (art. 33 et 34) ; la réalisation d'une analyse d'impact relative à la protection des données (art. 35) ; la désignation d'un délégué à la protection des données (art. 37).

110. En nous intéressant particulièrement à l'une des dispositions susvisées, à savoir l'analyse d'impact relative à la protection des données, on observe que le Règlement général la rend obligatoire (art. 35, par. 1, 3 et 4) quand le traitement comporte un risque élevé pour les libertés et les droits des personnes concernées[28]. Ceci peut s'avérer particulièrement pertinent lorsqu'une nouvelle technologie est introduite pour le traitement des données des personnes physiques.

111. Le moment où le responsable du traitement procède à cette évaluation doit être antérieur au traitement des données à caractère personnel, de manière à faciliter la prise de décision utile et en cohérence avec les principes de protection des données dès la conception et de protection des données par défaut[29].

112. Le principe de responsabilité exige des organisations qu'elles analysent les données qu'elles traitent, les finalités en vue desquelles elles les traitent et le type d'opérations de traitement qu'elles effectuent. À partir de ces informations, ces

---

[28] Article 35 du Règlement général : « 3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :
a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; c) la surveillance systématique à grande échelle d'une zone accessible au public. »

[29] Lignes directrices concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679. WP.248, avril 2017, p. 16 et 17.

organisations doivent déterminer expressément comment seront mises en œuvre les mesures requises par le Règlement général, en veillant à ce que ces mesures et procédures soient adaptées pour respecter la protection des données, et s'assurer qu'elles peuvent le démontrer aux personnes concernées et à l'autorité de contrôle. Ce principe exige des organisations qu'elles adoptent une méthode consciencieuse, diligente et proactive pour tous les traitements de données personnelles qu'elles effectuent[30].

113. Dans le même ordre d'idées, les Principes de l'OEA mettent l'accent sur l'adoption, la mise en œuvre de mesures de sécurité et la démonstration de leur application, la responsabilité portant sur la sécurité des données à caractère personnel ainsi que sur les communications et transferts internationaux de données. Il appartient aux responsables du traitement de garantir un degré continu de protection, conformément aux principes énoncés dans ce document (principe 10).

114. Les Lignes directrices de l'OCDE attribuent la responsabilité du respect des règles et décisions relatives à la protection de la vie privée au responsable du traitement, qui doit mener ses activités conformément aux principes établis (par. 14).

115. Le Cadre sur la vie privée de l'APEC réglemente ce principe en se focalisant principalement sur les transferts de données (art. 32). Ainsi, lorsque des données personnelles doivent être transférées à une autre personne ou organisation, au niveau national ou international, les responsables du traitement doivent obtenir le consentement de la personne concernée. À défaut d'obtenir ce consentement, ils doivent s'assurer que le destinataire protégera les informations de manière satisfaisante en prenant des mesures raisonnables pour garantir que les données seront protégées après le transfert, et ce dans le respect des principes.

116. La Convention 108 modernisée prévoit que les responsables ou sous-traitants doivent prendre des mesures techniques et organisationnelles tenant compte des implications du droit à la protection des données à caractère personnel à tous les stades du traitement des données (art. 10.1 et 10.3). Le rapport explicatif de la Convention mentionne plusieurs mesures que le responsable ou le sous-traitant pourra être amené à prendre, et notamment : la formation des employés, la mise en place de procédures appropriées de notification (indiquant par exemple quand des données doivent être effacées du système), l'établissement de clauses contractuelles particulières en cas de délégation du traitement visant à donner effet à la Convention, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité[31].

117. Enfin, il convient de noter qu'à l'exception des Principes directeurs des Nations Unies, tous les documents d'orientation internationaux analysés stipulent explicitement le principe de responsabilité. Par ailleurs, seuls les Normes ibéro-américaines et le Règlement général définissent des mécanismes ou des mesures à mettre en œuvre pour le respecter, comme on peut le voir dans le tableau 7 ci-dessous.

---

[30] Agence espagnole de protection des données personnelles, « ¿Qué es el principio de responsabilidad proactiva? », https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva.

[31] Rapport explicatif de la Convention 108 modernisée, à propos de l'article 10 (alinéa 85). Disponible sur : https://rm.coe.int/16808ac91b.

Tableau 7
Principe de responsabilité et mécanismes pour assurer son respect

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
	Article	*Article*	*Article*	*Article(s)*	*Paragraphe*	*Principe*	*Principe*
Mention explicite du principe de responsabilité	10.1		20	5.2	14	32	10
Définition de mécanismes ou mesures à mettre en œuvre pour respecter le principe			20.3	5.1, 24, 25, 30, 32, 33, 34, 35 et 37			

118. En fin de compte, 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, qui incombe aux responsables et aux sous-traitants dans la conduite de toutes leurs activités de traitement, 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.

Principe de sécurité

119. La sécurité est fondamentale pour la protection des données ; il ne peut y avoir de protection des données sans sécurité.

120. Pour respecter ce principe, il convient de recenser, évaluer et documenter les risques qui peuvent survenir au cours du cycle de vie des données afin de mettre en œuvre les mesures de sécurité nécessaires, de manière à éviter la matérialisation de ces risques et à pouvoir garantir la confidentialité, l'intégrité et la disponibilité des données à caractère personnel.

121. Tous les documents d'orientation internationaux analysés font référence à ce principe, de façon plus ou moins explicite, en prévoyant la nécessité de mettre en place des mesures de sécurité appropriées, suffisantes, opportunes, raisonnables ou adéquates pour prévenir différents types de risques tels que l'accès non autorisé, la perte, la modification, la destruction ou la divulgation des données à caractère personnel, entre autres[32].

122. Le tableau 8 détaille les types de mesures de sécurité et de risques spécifiés dans chacun des documents d'orientation internationaux. Il précise également ceux des documents qui mentionnent les éléments à prendre en compte pour déterminer les mesures à prendre, ainsi que les documents qui incluent l'obligation de notifier les violations de la sécurité des données.

[32] Ces informations figurent dans le tableau présenté à l'appui de ce point, qui détaille les types de mesures de sécurité et de risques définis dans les différents documents (article 7.1 de la Convention 108 modernisée ; article 7 des Principes directeurs des Nations Unies ; article 21.1 des Normes ibéro-américaines ; article 5.1 f) du Règlement général ; paragraphe 11 des Lignes directrices de l'OCDE ; article 28 du Cadre sur la vie privée de l'APEC ; principe 6 des Principes de l'OEA).

Tableau 8
Principe de sécurité

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
Type de mesures de sécurité	Mesures de sécurité appropriées Art. 7.1	Mesures appropriées Art. 7	Mesures administratives, physiques et techniques suffisantes Art. 21.1	Mesures techniques ou organisationnelles appropriées Art. 5.1 f)	Garanties de sécurité raisonnables Par. 11	Mesures appropriées Art. 28	Garanties de sécurité techniques, administratives ou organisationnelles raisonnables et adéquates Principe 6
Type de risques	Risques tels que l'accès accidentel ou non autorisé aux données personnelles, leur destruction, perte, utilisation, modification ou divulgation Art. 7.1	Risques naturels, tels que la perte accidentelle ou la destruction par sinistre, ou que les risques humains tels que l'accès non autorisé, l'utilisation détournée de données ou la contamination par des virus informatiques Art. 7	Dommage, perte, altération, destruction, accès et, en général, toute utilisation illégale ou non autorisée de données personnelles Art. 22.1	Traitement non autorisé ou illicite, perte, destruction ou dégâts d'origine accidentelle Art. 5.1 f)	Risques comme la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés Par. 11	Perte ou accès non autorisé, destruction, utilisation ou modification ou divulgation non autorisée ou tout autre usage indu Art. 28	Traitements non autorisés ou illégaux, y compris l'accès, la perte, la destruction, les dommages ou la divulgation, même si cela se produit de manière accidentelle Principe 6
Éléments à prendre en compte pour déterminer les			Art. 21.2	Art. 32		Art. 28	

	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel	*Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés*	*Normes de protection des données personnelles du Réseau ibéro-américain de protection des données*	*Règlement général sur la protection des données de l'Union européenne*	*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE*	*Cadre sur la vie privée de l'APEC*	*Principes actualisés du Comité juridique interaméricain sur la vie privée et la protection des données personnelles, avec annotations de l'OEA*
mesures à prendre							
Notification de violations de la sécurité à l'autorité de contrôle	Art. 7.2		Art. 22	Art. 33	Par. 15 c)	Art. 54	
Notification de violations de la sécurité aux personnes concernées			Art 22	Art 34	Par. 15 c)	Art. 54	

123. Les mesures de sécurité doivent être proportionnées à l'ampleur du risque, être régulièrement revues et actualisées, et peuvent également faire l'objet d'un audit afin de les améliorer et d'éviter leur obsolescence[33].

124. Les Principes de l'OEA disposent que ces mesures de sécurité devraient être vérifiées et actualisées en permanence (principe 6), tandis que les Normes ibéro-américaines indiquent que le responsable du traitement doit mener régulièrement des actions pour assurer le suivi, l'examen, le maintien et l'amélioration continue des mesures de sécurité applicables au traitement des données personnelles (art. 21.3). Le Cadre sur la vie privée de l'APEC précise quant à lui que les mesures de sécurité doivent faire l'objet d'un examen et d'une réévaluation périodiques (art. 28).

125. Certains documents d'orientation internationaux imposent l'obligation de notifier les violations de sécurité à l'autorité de contrôle, comme la Convention 108 modernisée (art. 7.2), les Normes ibéro-américaines (art. 22), le Règlement général (art. 33), les Lignes directrices de l'OCDE [par.15 c)] et le Cadre sur la vie privée de l'APEC (art. 54). En outre, à l'exception de la Convention 108 modernisée, tous les documents imposent aussi l'obligation d'informer les personnes concernées des violations de sécurité.

126. Il convient de souligner l'importance des notifications à l'autorité de contrôle ou éventuellement aux personnes concernées. D'une part, elles permettent à l'autorité de contrôle de vérifier que des mesures appropriées sont prises lorsqu'une violation de sécurité se produit et que cette violation est circonscrite dans les plus brefs délais. D'autre part, elles garantissent que les personnes concernées par la violation de sécurité sont informées que celle-ci s'est produite, ainsi que des dommages qui pourraient en découler.

127. L'Agence espagnole de protection des données rappelle que, en vertu du principe de sécurité défini au Règlement général, « les personnes qui traitent des données doivent effectuer l'analyse de risque nécessaire afin de déterminer les mesures techniques et organisationnelles à prendre pour garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel qu'ils traitent »[34].

128. Les Normes ibéro-américaines (art. 21.2), le Règlement général (art. 32) et le Cadre sur la vie privée de l'APEC (art. 28) énoncent des éléments ou des facteurs permettant de déterminer les mesures de sécurité à prendre, comme nous le verrons plus loin, mais aucun de ces documents ne fixe les mesures spécifiques à appliquer, étant donné que toute énumération risque de devenir obsolète.

129. Le Règlement général précise que, afin de déterminer les mesures appropriées pour assurer un niveau de sécurité adapté au risque, le responsable du traitement et le sous-traitant doivent tenir compte : « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques » (art. 32).

130. De même, les Normes ibéro-américaines mentionnent ces facteurs et y ajoutent ce qui suit : « les transferts internationaux de données personnelles exécutés ou destinés à être exécutés », « le nombre de titulaires », « les conséquences possibles qui résulteraient d'une violation des droits pour les titulaires et les violations antérieures qui ont eu lieu » (art. 21.2)

131. Le Cadre sur la vie privée de l'APEC indique que les mesures de sécurité devraient être proportionnées à la probabilité et à la gravité des dommages qui

[33] Principe 6 des Principes de l'OEA.

[34] Agence espagnole de protection des données, « Principes », 25 novembre 2021, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios.

pourraient survenir, à la sensibilité des données et au contexte dans lequel elles sont conservées (art. 28). Contrairement aux autres documents d'orientation internationaux, ce texte n'impose l'obligation de mettre en œuvre et d'actualiser les mesures de sécurité – en tenant compte des facteurs susvisés – qu'au responsable du traitement, sans évoquer les sous-traitants.

132. Dans les Principes de l'OEA, le texte portant sur le principe de sécurité est moins explicite. Cependant, dans les annotations relatives à ce principe, il est précisé que « les mesures adoptées pour protéger les données à caractère personnel doivent être déterminées en tenant compte, entre autres, des facteurs suivants : i) l'impact possible sur les droits des personnes concernées, notamment la valeur éventuelle des données pour un tiers non autorisé à les traiter ; ii) les coûts de leur mise en œuvre ; iii) les finalités du traitement ; iv) la nature des données personnelles traitées, en particulier les données sensibles. » (principe 6, annotation).

133. Parmi les documents d'orientation internationaux analysés, le Règlement général est le seul à fournir des exemples de mesures techniques et organisationnelles visant à garantir un niveau de sécurité adapté au risque, à savoir : « a) la pseudonymisation et le chiffrement des données à caractère personnel ; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » (art. 32.1).

134. En outre, l'article 32.3 du Règlement général prévoit que l'application d'un code de conduite ou d'un mécanisme de certification peut servir d'élément pour démontrer le respect des exigences.

135. Tout responsable du traitement ou sous-traitant doit prendre des mesures pour assurer la sécurité et protéger les données à caractère personnel contre des risques tels que l'accès non autorisé, la perte, la modification, la destruction, la divulgation ou d'éventuels dommages. En l'absence de ces mesures de sécurité, les données personnelles deviennent exposées à de tels risques, ce qui peut entraîner une atteinte grave aux droits des personnes concernées. C'est pourquoi tous les documents d'orientation internationaux analysés estiment nécessaire de mettre en place différents types de mesures face aux risques qui pourraient surgir. Et, dans certains cas, ils fournissent des éléments permettant de déterminer les mesures de sécurité appropriées sans pour autant indiquer les mesures spécifiques à appliquer, étant donné que l'évolution des technologies et des risques de violations est trop rapide pour pouvoir s'accompagner de l'actualisation correspondante de la réglementation.

136. La diversité des technologies et leur constante évolution, qui accroissent les capacités de collecte et de traitement des données, doivent être prises en compte pour évaluer de manière responsable et éthique les risques et les mesures de sécurité appropriées. Cette tâche incombe aux responsables du traitement des données, en vertu de l'habilitation légitime qui leur est conférée, ainsi que de la nécessité incontestable de préserver la confidentialité des données à caractère personnel qui sont traitées sous leur responsabilité.

137. Garantir l'intégrité, la disponibilité et la confidentialité des données à caractère personnel est une tâche essentielle et une obligation qui incombe aux responsables du traitement et aux sous-traitants, afin d'éviter les atteintes graves aux droits des personnes concernées. Néanmoins, si de telles atteintes devaient se produire, elles devraient avoir le moins d'impact possible sur les droits, grâce à l'établissement de

lignes directrices à appliquer dans de tels cas, comme les notifications obligatoires à l'autorité de contrôle et aux personnes concernées.

III. Conclusions

138. 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.

139. 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.

140. 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.

141. Le principe de transparence doit être respecté quelle que soit la base juridique qui légitime le traitement.

142. 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.

143. 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.

144. 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.

145. 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.

146. 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.

147. 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.

148. 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.

149. 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.

150. 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.