TEXTE DES PRINCIPES

Partie I : Dispositions générales

Principe 1 : But des Principes

(1) Les Principes pour une économie des données sont destinés à être utilisés dans les systèmes juridiques en Europe, aux États-Unis et ailleurs. Ils sont conçus pour

(a) apporter de la cohérence au droit existant et aux concepts juridiques pertinents pour l'économie des données, et pour favoriser leur harmonisation ;

(b) servir de source pour inspirer et guider le développement futur du droit par les tribunaux et les législateurs du monde entier ;

(c) éclairer le développement des meilleures pratiques et guider l'élaboration de standards en formation, y compris des standards ou des codes de bonnes pratiques commerciales spécifiques à une industrie ou à un secteur industriel particulier ;

(d) faciliter la rédaction de contrats-types ou de dispositions à utiliser sur une base volontaire par les parties dans l'économie des données ;

(e) régir les contrats ou compléter le droit qui les régit dans la mesure où ils fournissent des règles dispositives ou que les parties à une transaction les ont incorporées dans leur contrat ou les ont désignées d'une autre manière pour régir leur relation ; et

(f) guider les réflexions des tribunaux d'arbitrage et autres instances de règlement des litiges.

(2) Ces Principes proposent un cadre juridique qui peut être mis en œuvre avec toute forme de règles relatives à la confidentialité ou à la protection des données, de règles relatives la propriété intellectuelle ou relatives aux secrets commerciaux. Ces Principes n'ont pas pour but de modifier ou de créer un tel régime juridique, mais ils peuvent contribuer à l'élaboration d'une telle loi. En cas de contradictions entre les présents Principes et ces

autres règles, qui ne peut être surmontée par l'interprétation, ces autres règles doivent prévaloir.

Principe 2 : Champ d'application de ces Principes

(1) Les Principes portent principalement sur les enregistrements de grandes quantités d'informations en tant qu'élément patrimonial, ressource ou marchandise négociable. Les Principes ne traitent pas des données fonctionnelles, c'est-à-dire des données dont le but principal est de fournir des fonctionnalités particulières (comme un programme informatique), et des données représentatives, c'est-à-dire des données dont le but principal est de représenter d'autres actifs ou valeurs (comme les crypto-actifs).

(2) Sous réserve du paragraphe 3, les présents Principes portent sur

(a) les contrats de données,

(b) les droits sur les données, et

(c) les aspects des points (a) et (b) concernant les tiers.

(3) Ces Principes ne sont pas conçus pour s'appliquer aux organismes publics dans la mesure où ces organismes exercent des pouvoirs souverains.

Principe 3 : Définitions

(1) Les définitions suivantes s'appliquent aux fins des présents Principes :

(a) "Données ": les informations enregistrées dans tout format lisible par une machine et se prêtant à un traitement automatisé, stockées sur tout support ou considéré alors qu'elles sont en cours de transmission ;

(b) "Copie" : toute manifestation physique de données sous quelque forme ou sur quelque support que ce soit ;

(c) "Traitement des données" : toute opération ou ensemble d'opérations effectuées sur des données, par des moyens automatisés ou non ; il comprend, entre autres, la structuration, la modification, le stockage, l'extraction, la transmission, la combinaison, l'agrégation ou l'effacement des données ;

(d) "Accès aux données" : le fait d'être en mesure de lire les données et de les utiliser, avec ou sans contrôle de ces données ;

(e) "Contrôle des données" : le fait d'être en mesure d'accéder aux données et de déterminer les finalités et les moyens de leur traitement ;

(f) "Maître des données" : la personne qui, seule ou conjointement avec d'autres personnes, a le contrôle des données ;

(g) "Gérant" : la personne qui, sans être maître des données, traite des données pour le compte du maître des données ;

(h) "Données cogénérées" : données à la création desquelles une personne autre que le maître des données a contribué, par exemple en étant le sujet de l'information ou le propriétaire ou l'exploitant de ce sujet, en exerçant une activité génératrice de données ou en possédant ou exploitant un dispositif générateur de données, ou en produisant ou développant un produit ou un service générateur de données ;

(i) "Données dérivées" : les données générées par le traitement d'autres données, y compris les données agrégées et les données déduites d'autres données à l'aide de règles de décision externes ;

(j) "Contrat de données" : un contrat dont l'objet est constitué de données ;

(k) "Droit aux données" : un droit à l'encontre d'un maître des données qui est spécifique à la nature des données et qui découle de la manière dont les données sont générées, ou de la loi pour des raisons d'intérêt public ;

(l) "Activités relatives aux données" : activités d'une personne concernant des données, telles que la collecte, l'acquisition, le contrôle, le traitement et d'autres activités, y compris la transmission ultérieure de données ;

(m) "Mise à disposition" de données : le fait de donner accès à des données à une autre personne ou de mettre des données sous le contrôle d'une autre personne ;

(n) "Fournisseur" de données : une partie qui fournit des données à une autre partie ou s'engage à le faire ;

(o) "Destinataire" des données : la partie à laquelle les données sont fournies ou doivent être fournies ;

(p) "Transfert" de données : la mise à disposition de données par laquelle le fournisseur met les données sous le contrôle du destinataire, que le fournisseur conserve ou non le contrôle des données ;

(q) "Portage" de données : le fait d'initier le transfert de données contrôlées par une autre partie vers soi-même ou vers un tiers désigné ;

(r) "Effacement des données" : prendre des mesures pour garantir, dans la mesure du possible, que les données soient définitivement inaccessibles ou illisibles d'une autre manière ; et

(s) "Notification" : le fait d'avoir connaissance d'un fait ou, compte tenu de tous les faits et circonstances dont une personne a connaissance, le fait d'être dans une situation telle que l'on peut raisonnablement s'attendre à ce que la personne ait connaissance du fait.

(2) Les termes "contrat de transfert de données", "contrat d'accès simple aux données", "contrat d'exploitation d'une source de données", "contrat d'autorisation d'accès", "contrat de mise en commun de données", "contrat de traitement de données", "contrat de fiducie de données", "contrat de dépôt fiduciaire de données" et "contrat de marché de données", ainsi que tous les termes désignant les parties à ces contrats, ont la signification qui leur est donnée dans les Principes 7 à 15.

(3) Les références à une "personne" incluent les personnes physiques et morales, privées ou publiques. Les références à une "opération" ou à une "activité" comprennent les opérations ou activités réalisées avec l'aide d'autres personnes ou de machines, y compris toute intelligence artificielle.

Principe 4 : Moyens de droit

(1) Les moyens de droit portant sur les contrats et les droit aux données, y compris relatif à la protection des tiers en cas d'activités relatives aux données, sont en principe fixés par le droit applicable.

(2) Lorsque les présents Principes ou le droit applicable imposent la restitution ou la remise de données par une partie (le défendeur) à une autre personne (le demandeur), le

défendeur devrait pouvoir satisfaire à l'obligation de restituer ou de remettre les données en effaçant toutes les copies de données auxquelles le défendeur a accès. Si le demandeur ne dispose pas d'une copie des données, le défendeur doit donner au demandeur le contrôle des données avant de les effacer.

Partie II : Contrats de données

Chapitre A : Règles et principes régissant les contrats de données

Principe 5 : Application des présents Principes aux contrats de données

Les contrats de données relevant de la Partie II doivent être régis, dans l'ordre de priorité suivant, par :

(a) les règles de droit auxquelles il ne peut être dérogé par convention ;

(b) l'accord des parties ;

(c) toute règle de droit autre que celles visées au paragraphe (a) qui a été élaborée pour être appliquée aux transactions de données du type concerné ;

(d) les clauses incluses dans les contrats en application des Principes 7 à 15 ;

(e) l'application par analogie de règles et de principes de droit dispositifs qui ne sont pas directement applicables aux opérations de données du type concerné, mais qui régiraient des opérations analogues ; et

(f) les principes généraux de droit.

Principe 6 : Interprétation et application du droit des contrats

Lors de l'interprétation et de l'application des règles et des principes du droit des contrats, il faut notamment prendre en compte les facteurs suivants :

(a) le fait que les données sont une combinaison (i) de manifestations physiques sur un support ou en état d'être transmises, et (ii) d'informations enregistrées ;

(b) la nature des données en tant que ressource dont il peut exister de multiples copies et qui peut être utilisée en parallèle par diverses parties pour des buts très divers;

(c) le fait que les données sont généralement dérivées d'autres données, et que l'ensemble de données originales et une multitude d'ensembles de données dérivées qui ressemblent plus ou moins à l'ensemble de données originales peuvent coexister ;

(d) le fait que, bien que l'emplacement physique de stockage des données puisse changer rapidement et facilement, les données sont normalement utilisées par le biais d'un accès à distance et l'emplacement physique de stockage des données est généralement de peu d'importance ; et

(e) l'importance élevée des effets cumulés et des phénomènes d'échelle.

Chapitre B : Contrats de fourniture ou de partage de données

Principe 7 : Contrats de transfert de données

(1) Un contrat de transfert de données est une transaction par laquelle le fournisseur s'engage à donner au destinataire le contrôle de données particulières en transférant les données sur un support sous le contrôle du destinataire ou en livrant au destinataire un support sur lequel les données sont stockées.

(2) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi doit prévoir que les clauses suivantes sont incluses dans un contrat de transfert de données :

(a) En ce qui concerne la manière dont le fournisseur doit exécuter son engagement décrit au paragraphe 1, les données seront transférées conformément aux instructions du destinataire, à moins que le mode de transfert indiqué ne soit déraisonnable (par exemple, à la lumière de préoccupations relatives à la sécurité des données), auquel cas le fournisseur devrait rapidement notifier ces préoccupations au destinataire afin que ce dernier puisse indiquer un mode de transfert de substitution.

(b) En ce qui concerne les caractéristiques des données fournies, notamment en ce qui concerne la nature, la quantité, l'exactitude, l'actualité, l'intégrité, la granularité et les formats, ainsi qu'en ce qui concerne l'inclusion de métadonnées, d'indications de domaines et d'autres spécifications nécessaires à l'utilisation des données, et en ce qui concerne la fréquence de la fourniture et des mises à jour :

(i) Les données fournies doivent être conformes à toute description ou représentation matérielle concernant les données faite ou adoptée par le fournisseur, ainsi qu'à tout échantillon ou modèle fourni ;

(ii) Si le fournisseur a connaissance de l'objectif particulier de l'acquéreur pour l'obtention des données et que l'acquéreur se fie à la compétence ou au jugement du fournisseur pour choisir les données fournies, les données fournies doivent être adaptées à l'objectif particulier de l'acquéreur ; et

(iii) si le fournisseur a pour activité de fournir des données du type de celles qui font l'objet du contrat ou s'il se présente comme ayant une expertise en la matière, les données fournies doivent être d'une qualité à laquelle on peut raisonnablement s'attendre dans une transaction du type en question.

(c) En ce qui concerne le contrôle des données fournies et les autres activités relatives à ces données :

(i) Si les données fournies sont protégées par le droit de la propriété intellectuelle ou un régime similaire, le fournisseur doit mettre le destinataire en mesure de disposer d'un droit légal, opposable aux tiers, suffisant pour que le destinataire puisse contrôler les données et exercer les autres activités relatives aux données que le responsable du traitement savait que le destinataire pouvait raisonnablement s'attendre à exercer. Si le fait de placer le destinataire dans cette position exige des mesures supplémentaires de la part du fournisseur, telles que l'exécution ou l'enregistrement d'un document requis, le fournisseur doit prendre ces mesures supplémentaires ;

(ii) Le fournisseur doit mettre le destinataire en mesure, au moment où les données sont fournies, d'exercer légitimement un contrôle sur les données et de se livrer légitimement à d'autres activités relatives aux données que le responsable du

traitement savait que le destinataire pouvait raisonnablement s'attendre à exercer ; si, après la fourniture des données, le contrôle des données ou d'autres activités relatives aux données par le destinataire deviennent illicites, cela ne donne pas lieu en soi à une réclamation du destinataire contre le fournisseur ;

(iii) Le fournisseur doit coopérer, dans la mesure où cela est raisonnablement nécessaire, aux actions qui peuvent être requises pour se conformer aux exigences légales concernant le contrôle des données ou d'autres activités liées aux données dont le responsable du traitement a eu connaissance du fait que le destinataire pourrait raisonnablement s'y livrer. En outre, le fournisseur doit fournir à l'acquéreur des informations sur toutes les exigences légales relatives à ces activités de données dont le fournisseur a connaissance et dont il ne peut pas être attendu que l'acquéreur ait connaissance ;

(iv) Le destinataire peut utiliser les données et toutes les données dérivées, y compris en les fournissant à d'autres, à toute fin légale et de toute manière qui ne porte pas atteinte aux droits du fournisseur ou de tiers, et qui ne viole pas les obligations du fournisseur vis-à-vis de tiers, à condition que le destinataire ait été informé de ces obligations au moment de la conclusion du contrat de transfert de données ;

(v) Entre les parties, les nouveaux droits de propriété intellectuelle ou droits similaires créés par le destinataire avec l'utilisation des données fournies appartiennent au destinataire ; et

(vi) le fournisseur peut conserver une copie des données et peut continuer à les utiliser, y compris en les fournissant à des tiers.

(3) Pour déterminer quelles règles et quels principes devraient s'appliquer par analogie, comme le prévoit le Principe 5, aux contrats de transfert de données, il convient de tenir compte en particulier de ce qui suit :

(a) si le contrat prévoit que le destinataire aura le contrôle des données pour une période illimitée ou pour une période limitée ; et

(b) si le contrat porte sur une fourniture unique de données, une fourniture répétée ou une fourniture continue sur une période donnée.

Principe 8 : Contrats d'accès simple aux données

(1) Un contrat d'accès simple aux données est un contrat en vertu duquel le fournisseur s'engage à fournir à l'acquéreur l'accès à des données particulières sur un support sous le contrôle du fournisseur et qui n'est pas un contrat de transfert de données en vertu du Principe 7. Cela inclut les contrats dans lesquels le fournisseur, en plus de permettre au destinataire de lire les données, s'engage à mettre le destinataire en mesure de traiter les données sur le support contrôlé par le fournisseur, ou de porter les données.

(2) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes sont incluses dans un contrat d'accès simple aux données :

(a) En ce qui concerne le mode d'accès du destinataire aux données :

(i) Le fournisseur doit fournir à l'acquéreur les identifiants d'accès nécessaires et supprimer tout obstacle technique à l'accès dont on pourrait raisonnablement s'attendre à ce qu'il soit supprimé dans une transaction du type concerné ;

(ii) Le fournisseur doit rendre les données accessibles dans un format structuré et lisible par machine d'un type qui peut être raisonnablement attendu dans une transaction du type concerné ;

(iii) Le fournisseur doit permettre au destinataire d'accéder aux données à distance, à moins que cela ne soit déraisonnable au regard de la sécurité des données ;

(iv) Le destinataire ne peut traiter les données auxquelles il a accès qu'à des fins compatibles avec les objectifs convenus dans le contrat ;

(v) Le destinataire peut porter les données auxquelles il a accès dans le cadre du contrat uniquement lorsque le portage de ces données peut raisonnablement être attendu dans le cadre d'une transaction du type concerné, et peut porter les données dérivées des activités de traitement du destinataire effectuées conformément au contrat (par exemple, les données dérivées de l'analyse des données) ; et

(vi) Le destinataire peut lire les données, les traiter ou les porter, selon le cas, par tout moyen, y compris des moyens automatisés, et peut le faire aussi souvent que le destinataire le souhaite pendant la période d'accès convenue.

(b) En ce qui concerne les caractéristiques des données auxquelles l'accès est fourni, les conditions énumérées au Principe 7, paragraphe 2, point b, pour les contrats de transfert de données s'appliquent également dans un contrat d'accès simple aux données.

(c) En ce qui concerne le contrôle de toute donnée transférée par le destinataire conformément au contrat et d'autres activités relatives aux données, les conditions énumérées au Principe 7, paragraphe 2, point c, pour les contrats de transfert de données s'appliquent également à un contrat d'accès simple aux données.

(3) Pour déterminer les règles et principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats d'accès simple aux données, il convient de tenir compte en particulier de la question de savoir si, et dans quelle mesure, le destinataire peut seulement visualiser les données, peut traiter les données sur le support sous le contrôle du fournisseur, ou peut porter les données.

Principe 9 : Contrats d'exploitation d'une source de données

(1) Un contrat d'exploitation d'une source de données est un contrat en vertu duquel le fournisseur s'engage à fournir à l'acquéreur l'accès aux données en lui donnant accès à un dispositif ou à une installation particulière par laquelle les données sont collectées ou générées d'une autre manière (la "source de données"), permettant à l'acquéreur de lire les données, de les traiter ou de les porter depuis la source de données.

(2) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes, en plus de celles prévuse au Principe 8, sont incluses dans un contrat d'exploitation d'une source de données :

(a) En ce qui concerne le mode d'accès du destinataire aux données de la source de données :

(i) Le destinataire peut porter toutes les données collectées ou générées par la source de données ; et

(ii) L'accès aux données est fourni en temps réel, au fur et à mesure que les données sont collectées ou générées par la source de données.

(b) En ce qui concerne les caractéristiques des données, il n'est pas nécessaire que le destinataire reçoive des données d'une qualité ou d'une quantité particulière.

(3) Pour déterminer les règles et principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats d'exploitation d'une source de données, il convient de prendre en compte notamment :

(a) le degré et la durée du contrôle que le destinataire doit recevoir sur la source de données ; et

(b) si, et dans quelle mesure, le destinataire peut porter les données.

Principe 10 : Contrats d'autorisation d'accès

(1) Un contrat d'autorisation d'accès aux données est un contrat en vertu duquel le fournisseur (la "partie autorisante") autorise l'accès aux données ou à une source de données par le destinataire, comprenant généralement le traitement ou le portage des données, mais où, à la lumière de la nature passive de la conduite prévue de la partie autorisante en vertu du contrat et de l'absence d'influence significative de la partie autorisante sur la transaction, on ne peut raisonnablement s'attendre à ce que la partie autorisante assume des responsabilités du type décrit dans les Principes 7 à 9.

(2) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que dans un contrat d'autorisation d'accès :

(a) En ce qui concerne le mode d'accès du destinataire, une clause selon laquelle l'autorisateur facilitera ou aidera le destinataire à obtenir l'accès n'est pas incluse, et l'autorisateur peut continuer à utiliser les données ou la source de données de quelque manière que ce soit, même si cela entrave l'accès du destinataire ou même le rend impossible ;

(b) En ce qui concerne les caractéristiques des données, il n'est pas exigé que le destinataire reçoive des données d'une qualité ou d'une quantité particulière ;

(c) En ce qui concerne le contrôle des données et toute autre activité liée aux données que le destinataire peut exercer, l'autorisateur n'est pas tenu de garantir que le destinataire aura des droits particuliers ;

(d) En ce qui concerne la partie autorisatrice et le destinataire, le destinataire est responsable du respect de toutes les obligations envers les tiers en vertu de la Partie IV, y compris les obligations incombant à un fournisseur de données en vertu du Principe 32 ; et

(e) Le destinataire doit indemniser la partie autorisante pour toute responsabilité à l'égard des tiers qui découle de l'autorisation de la partie autorisante d'accéder aux données, à moins que cette responsabilité ne puisse raisonnablement être prévue par le destinataire.

(3) Pour déterminer les règles et principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats d'autorisation d'accès aux données, il convient de considérer si l'objet central de l'accord entre les parties est l'accès aux données ou la fourniture d'une autre prestation (tel qu'un service numérique) au cours duquel l'accès aux données a lieu.

Principe 11 : Contrats de mise en commun de données

(1) Un contrat de mise en commun de données est un contrat par lequel deux parties ou plus (les "partenaires de données") s'engagent à partager des données dans un réservoir de données en

(a) transférant des données particulières sur un support contrôlé conjointement par les partenaires de données ou contrôlé par un fiduciaire de données, un dépositaire ou un autre tiers agissant au nom des partenaires de données ; ou

(b) en s'accordant mutuellement l'accès à certaines données ou la possibilité d'exploiter certaines sources de données, avec ou sans l'intervention d'un tiers.

(2) Le présent principe s'applique, avec les ajustements appropriés, aux principes directeurs de toute entité créée en vertu d'un contrat de mise en commun de données.

(3) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes sont incluses dans un contrat de mise en commun de données :

(a) Un partenaire de données peut utiliser les données du réservoir de données, ou les données dérivées de ces données, seulement

(i) à des fins convenues entre les partenaires de données dans le contrat de mise en commun des données ;

(ii) à des fins dont le partenaire de données concerné pouvait raisonnablement s'attendre à ce qu'elles soient acceptées par les autres partenaires de données, sauf si ces fins sont incompatibles avec un accord visé au point i) ; ou

(iii) si cela est nécessaire pour se conformer au droit applicable ;

(b) Un partenaire de données peut engager des gérants de données, mais ne peut autrement transmettre des données du réservoir de données, ou des données dérivées de ces données, à des tiers que dans les conditions convenues entre les partenaires de données ou requises par le droit applicable ;

(c) Entre les partenaires de données, les nouveaux droits de propriété intellectuelle ou droits similaires créés par l'utilisation des données du réservoir de données appartiennent au partenaire ou aux partenaires qui ont mené l'activité conduisant à la création du nouveau droit ;

(d) Si un partenaire de données quitte le réservoir de données, les données fournies par ce partenaire de données doivent lui être restituées, mais les données dérivées, à moins qu'elles ne soient essentiellement identiques aux données initialement fournies par ce partenaire de données, restent dans le réservoir de données. Lorsqu'il quitte le réservoir de données, un partenaire de données a le droit de recevoir une copie de toutes les données du réservoir de données qui ont été dérivées, en totalité ou en grande partie, des données fournies à l'origine par ce partenaire de données.

(4) Pour déterminer les règles et principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats de mise en commun de données, il faut se demander si la relation entre les partenaires de données est caractérisée par une confiance mutuelle, de sorte que les partenaires de données se doivent des obligations fiduciaires, ou plutôt si elle est caractérisée par des transactions sans lien de dépendance et sans obligations fiduciaires.

Chapitre C : Contrats de services relatifs aux données

Principe 12 : Contrats de traitement des données

(1) Un contrat de traitement de données est un contrat en vertu duquel un gérant s'engage à traiter des données pour le compte du maître des données. Ce traitement peut comprendre, entre autres

(a) la collecte et l'enregistrement de données (par exemple, le *scraping* de données) ;

(b) le stockage ou la récupération de données (par exemple, la fourniture d'espace en *cloud*) ;

(c) l'analyse des données (par exemple, les services d'analyse de données) ;

(d) organisation, structuration, présentation, modification ou combinaison de données (par exemple, services de gestion de données) ; ou

(e) l'effacement des données.

(2) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes sont incluses dans un contrat de traitement des données :

(a) Le gérant doit suivre les instructions du maître des données, y compris en autorisant le portage des données à la demande du maître des données à tout moment, et agir conformément aux finalités déclarées du traitement par le maître des données ;

(b) Le gérant doit assurer au moins le même niveau de sécurité des données et de protection des droits des tiers que celui que le maître des données était tenu d'assurer, et doit aider le maître des données à respecter toute obligation légale de protection des tiers à laquelle on pourrait raisonnablement s'attendre dans une situation de ce type ou dont le gérant avait connaissance au moment de la conclusion du contrat ;

(c) Le gérant ne doit pas transmettre les données à des tiers ;

(d) Le gérant ne peut traiter les données pour ses propres besoins, sauf dans la mesure raisonnablement nécessaire pour améliorer la qualité ou l'efficacité du service

concerné, à condition que cela ne porte pas atteinte aux intérêts légitimes du maître des données et ne soit pas incompatible avec les obligations de protection des tiers au sens du paragraphe 2, point b ; et

(e) Lors de la pleine exécution ou de la résiliation du contrat, le gérant doit transférer au maître des données toute donnée résultant du traitement qui n'a pas encore été transférée. Le gérant doit ensuite effacer toute donnée conservée, sauf dans la mesure où cela est raisonnablement nécessaire pour un litige existant ou probable ou dans la mesure où le gérant a un droit ou une obligation légale indépendante des présents Principes de conserver les données au-delà de ce moment.

(3) Pour déterminer les règles et principes à appliquer directement ou par analogie, comme le prévoit le Principe 5, aux contrats de traitement des données, il convient de prendre en considération la nature du service, par exemple si l'accent est mis sur la modification des données ou sur leur sécurité.

Principe 13 : Contrats de fiducie de données

(1) Un contrat de *fiducie* de données est un contrat conclu entre un ou plusieurs maîtres des données (les "mandants") et un tiers, en vertu duquel les mandants habilitent le tiers (le "fiduciaire") à prendre certaines décisions concernant l'utilisation ou la fourniture ultérieure de données (les "données confiées") en leur nom, dans la poursuite d'objectifs déclarés qui peuvent bénéficier aux mandants ou à un groupe plus large de parties prenantes (ces mandants ou parties prenantes étant appelés les "bénéficiaires").

(2) Un contrat de fiducie de données et les relations qu'il crée ne doivent pas nécessairement se conformer à une structure organisationnelle particulière et ne doivent pas inclure les caractéristiques et les obligations associées à un *trust* de *common law*. Le présent Principe s'applique, avec les ajustements appropriés, aux principes directeurs de toute entité créée en vertu d'un contrat de fiducie de données.

(3) Sous réserve de l'accord des parties et des règles qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes sont incluses dans un contrat de fiducie de données ou sont incorporées dans les principes directeurs de toute entité créée en vertu du contrat de fiducie de données :

(a) Le fiduciaire des données est, sous réserve des points b et c, habilité à prendre et à mettre en œuvre toutes les décisions relatives à l'utilisation ou à la fourniture ultérieure des données confiées, y compris les décisions concernant les droits de propriété intellectuelle et les droits fondés sur les lois sur la confidentialité des données ou la protection des données ;

(b) Le fiduciaire des données doit agir dans le cadre des objectifs déclarés du contrat de fiducie pour le bénéfice des bénéficiaires et, même si les mandants ne sont pas les bénéficiaires, d'une manière qui n'est pas incompatible avec les intérêts légitimes des mandants dont le fiduciaire des données a connaissance ;

(c) Le fiduciaire des données doit suivre toutes les instructions données par les mandataires, y compris en autorisant le portage des données à la demande des maîtres des données à tout moment, sauf dans la mesure où le fiduciaire des données sait que les instructions sont incompatibles avec les objectifs déclarés ou manifestement évidents de la fiducie de données ;

(d) Le fiduciaire des données doit s'abstenir de toute utilisation des données confiées à ses propres fins et doit éviter tout conflit d'intérêts ;

(e) Les mandants peuvent à tout moment mettre fin au pouvoir du fiduciaire en ce qui concerne les données qu'ils ont confiées ; toutefois, ce droit peut être limité dans la mesure nécessaire pour tenir compte de la confiance et d'autres intérêts légitimes similaires des bénéficiaires.

(f) si le fiduciaire a conservé des données confiées, ou des données dérivées de ces données, après la fin du contrat (qu'elle soit survenue par résiliation ou autrement), il doit restituer les données aux mandants et, lorsque cela est raisonnable, prendre des mesures pour empêcher toute utilisation ultérieure des données par les destinataires ultérieurs.

(4) Pour déterminer les règles et les principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats de fiducie de données, il convient de prendre en considération en particulier

(a) les objectifs déclarés du contrat de fiducie de données et la nature des données et des parties concernées ;

(b) la question de savoir si les objectifs du contrat de fiducie de données sont principalement au bénéfice des personnes concernées ou de groupes plus larges ; et

(c) la structure organisationnelle des relations créées par le contrat de fiducie de données.

Principe 14 : Contrats de dépôt fiduciaire de données

(1) Un contrat de dépôt fiduciaire de données est un contrat conclu entre une ou plusieurs parties qui prévoient d'utiliser des données (les "parties contractantes") et un tiers (le "dépositaire"), en vertu duquel le dépositaire s'engage à veiller à ce que les pouvoirs et les capacités de certaines ou de toutes les parties contractantes en ce qui concerne les données soient limités (les "parties restreintes") afin d'éviter tout conflit avec les exigences légales, telles que celles imposées par les lois antitrust [le droit des cartels] ou les lois sur la confidentialité ou la protection des données.

(2) Un contrat de dépôt fiduciaire de données et les relations qu'il crée ne doivent pas nécessairement se conformer à une structure organisationnelle particulière. Ce Principe s'applique, avec les ajustements appropriés, aux principes directeurs de toute entité créée en vertu d'un contrat de dépôt fiduciaire de données.

(3) Sous réserve de l'accord des parties et des autres principes qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivants sont incluses dans un contrat de dépôt fiduciaire de données ou sont incorporées dans les principes directeurs de toute entité créée en vertu du contrat d'entiercement de données :

(a) Le dépositaire dispose des pouvoirs relatifs aux données qui sont nécessaires à l'objectif déclaré du contrat de dépôt fiduciaire de données ;

(b) Le dépositaire doit agir dans le sens des objectifs déclarés du contrat de dépôt fiduciaire de données, même si cette action est incompatible avec les intérêts des parties contractantes qui sont distincts de l'objectif déclaré du contrat de dépôt fiduciaire de données ;

(c) Le dépositaire ne doit pas suivre les instructions données par une partie contractante qui sont incompatibles avec l'objectif déclaré ou manifestement évident du contrat de dépôt fiduciaire de données ;

(d) Le dépositaire doit s'abstenir d'utiliser ou de fournir ultérieurement les données confiées à ses propres fins et doit éviter tout conflit d'intérêts ; et

(e) Si le contrat de dépôt fiduciaire de données est résilié, chaque partie a l'obligation, pendant la liquidation de la relation, de ne pas prendre de mesures qui compromettent les objectifs déclarés du contrat de dépôt fiduciaire de données.

(4) Pour déterminer les règles et les principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats de dépôt fiduciaire de données, il convient de tenir compte en particulier des éléments suivants

(a) l'objectif déclaré du contrat de dépôt fiduciaire de données et la nature des données et des parties concernées ; et

(b) la structure organisationnelle des relations créées par le contrat de dépôt fiduciaire de données.

Principe 15 : Contrats de marché de données

(1) Un contrat de marché de données est un contrat entre une partie cherchant à conclure une transaction de données (le "client") et un fournisseur de marché de données, en vertu duquel le fournisseur de marché de données s'engage à permettre ou à faciliter la mise en relation entre le client et d'autres parties potentielles à des transactions de données et, dans certains cas, à fournir des services supplémentaires facilitant la transaction.

(2) Sous réserve de l'accord des parties et des autres principes qui ont la priorité en vertu du Principe 5, la loi devrait prévoir que les clauses suivantes sont incluses dans un contrat de marché de données :

(a) Dans la mesure où le fournisseur du marché des données s'engage à faciliter ou à permettre une étape particulière dans le cadre d'une transaction, il doit apporter un

soutien raisonnable au client dans le respect de toute obligation légale applicable à cette étape ;

(b) Le fournisseur du marché des données doit s'abstenir d'utiliser à ses propres fins les données reçues de son client qui font l'objet de la transaction prévue ; et

(c) Lors de la pleine exécution ou de la résiliation du contrat, le fournisseur du marché des données doit effacer toutes les données en sa possession qui font l'objet de la transaction prévue et qu'il a reçues de son client, ainsi que toutes les données dérivées de ces données.

(3) Pour déterminer les règles et principes à appliquer par analogie, comme le prévoit le Principe 5, aux contrats de marché de données, il convient de prendre en compte en particulier :

(a) si, et dans quelle mesure, le fournisseur du marché des données prend le contrôle des données concernées ; et

(b) si, et dans quelle mesure, le paiement ou toute autre prestation due au fournisseur du marché des données dépend du fait que la mise en relation donne lieu à une transaction de données.

Partie III : Droits relatifs aux données

Chapitre A : Règles et principes régissant les droits relatifs aux données

Principe 16 : Droits relatifs aux données

(1) Les droits relatifs aux données peuvent inclure le droit

(a) d'obtenir l'accès aux données par des moyens qui peuvent, dans des circonstances appropriées, inclure le portage des données ;

(b) d'exiger du maître des données qu'il mette fin aux activités relatives aux données ;

(c) d'exiger du maître des données qu'il corrige les données ; ou

(d) recevoir une part économique des bénéfices tirés de l'utilisation des données.

(2) Les droits relatifs aux données énoncés dans la Partie III ne sont pas exhaustifs ; un système juridique peut plutôt conclure que les parties devraient avoir des droits supplémentaires de ce genre. Par conséquent, aucune conclusion négative ne doit être tirée de l'absence de ces droits dans la Partie III.

(3) Les droits énoncés dans la Partie III le sont sans préjudice des droits autres que les droits sur les données qu'une personne peut avoir à l'encontre d'un maître des données en ce qui concerne ces données, tels que les droits découlant d'une rupture de contrat, d'un enrichissement sans cause, de la conversion de droits de propriété ou du droit de la responsabilité civile.

Principe 17 : Application des présents principes aux droits relatifs aux données

Les droits prévus à la Partie III devraient être régis, dans l'ordre de priorité suivant, par :

(a) les règles de droit auxquelles il ne peut être dérogé par convention, y compris les lois relarives à la confidentialité ou à la protection des données ;

(b) un accord entre les parties dans la mesure où le contrat est conforme aux Principes 18 à 27 ou si les parties sont libres de déroger aux Principes 18 à 27 en vertu du droit applicable ;

(c) toute règle de droit applicable, autre que celles visées au point a, qui a été élaborée pour être appliquée aux droits sur les données ; et

(d) les Principes 18 à 27.

Chapitre B : Droits relatifs aux données générées en commun

Principe 18 : Données cogénérées

(1) Les facteurs à prendre en compte pour déterminer si, et dans quelle mesure, les données doivent être traitées comme co-générées par une partie au sens des Principes 19 à 23 sont, dans l'ordre de priorité suivant :

(a) la mesure dans laquelle cette partie est le sujet des informations encodées dans les données, ou est le propriétaire ou l'exploitant d'un actif qui est le sujet de ces informations ;

(b) la mesure dans laquelle les données ont été produites par une activité de cette partie, ou par l'utilisation d'un produit ou d'un service appartenant à cette partie ou exploité par elle ;

(c) la mesure dans laquelle les données ont été collectées ou assemblées par cette partie d'une manière qui crée quelque chose d'une qualité nouvelle ; et

(d) la mesure dans laquelle les données ont été générées par l'utilisation d'un programme informatique ou d'un autre élément pertinent d'un produit ou d'un service, que cette partie a produit ou développé.

(2) Les facteurs à prendre en compte pour évaluer l'étendue d'une contribution comprennent le type de contribution, l'ampleur de la contribution (y compris par le biais d'un investissement), la proximité ou l'éloignement de la contribution, le degré de spécificité de la contribution et les contributions d'autres parties.

(3) Les contributions d'une partie qui sont insignifiantes dans les circonstances ne conduisent pas à considérer les données comme étant co-générées par cette partie.

Principe 19 : Facteurs généraux déterminant les droits sur les données générées conjointement

(1) Les droits sur les données co-générées découlent de considérations d'équité ; par conséquent, la manière dont ils sont intégrés dans les cadres juridiques existants en vertu du droit applicable et la mesure dans laquelle ils peuvent être levés ou modifiés par accord devraient être déterminés par le rôle que jouent ces considérations d'équité dans le système juridique pertinent.

(2) Dans le cas de données générées conjointement, une partie qui a joué un rôle dans la génération des données a un droit sur les données lorsque cela est approprié au vu des faits et des circonstances, ce qui est déterminé par la prise en compte des facteurs suivants :

(a) la part que cette partie a eue dans la génération des données pertinentes, compte tenu des facteurs énumérés au Principe 18 ;

(b) le poids des motifs, tels que ceux énumérés dans les Principes 20 à 23, que cette partie peut faire valoir pour se voir accorder le droit aux données ;

(c) le poids de tout intérêt légitime que le maître des données ou un tiers peut avoir à refuser le droit aux données ;

(d) le déséquilibre du pouvoir de négociation entre les parties ; et

(e) tout intérêt public, y compris l'intérêt d'assurer une concurrence loyale et efficace.

(3) Les facteurs énumérés au paragraphe 2 devraient également être pris en compte pour déterminer les spécifications ou les restrictions des droits sur les données, notamment en ce qui concerne les formats de données, le calendrier, la sécurité des données, le soutien supplémentaire requis pour que l'exercice du droit soit pleinement effectif, et la rémunération due.

Principe 20 : Accès ou portage en ce qui concerne les données co-générées

(1) Les motifs qui, sous réserve du Principe 19, peuvent donner lieu à un droit d'accès ou de portage de données co-générées comprennent les circonstances dans lesquelles l'accès ou le portage est

(a) nécessaire à l'utilisation normale, à l'entretien ou à la revente par l'utilisateur d'un produit ou d'un service conforme à sa finalité, lorsque le maître des données fait partie du réseau de distribution et que l'on peut raisonnablement s'attendre à ce qu'il ait prévu cette nécessité ;

(b) nécessaires au contrôle ou à l'amélioration de la qualité par le fournisseur d'un produit ou d'un service, conformément aux obligations de ce fournisseur, lorsque le maître des données fait partie du réseau d'approvisionnement et que l'on peut raisonnablement s'attendre à ce qu'il ait prévu cette nécessité ;

(c) nécessaires à l'établissement de faits, tels qu'une meilleure compréhension par une partie de ses propres opérations, y compris toute preuve de ces opérations que cette partie doit fournir à un tiers, lorsque cette partie en a un besoin urgent et que l'on

ne peut raisonnablement s'attendre à ce que l'accès aux données co-générées ou leur portage porte atteinte aux intérêts du maître des données ;

(d) nécessaires au développement d'un nouveau produit ou service par une partie lorsque ce développement devait, à la lumière des opérations commerciales antérieures de cette partie et du maître des données, du type de leurs contributions respectives à la génération des données et de la nature de leurs relations, être considéré principalement comme une opportunité commerciale de cette première partie ; ou

(e) nécessaire pour éviter les effets de verrouillage anticoncurrentiels au détriment d'une partie, par exemple en empêchant cette partie de changer légitimement de fournisseur de produits ou de services ou d'attirer d'autres clients.

(2) Conformément au Principe 19, paragraphe 3, un droit au titre du paragraphe 1 ne doit être accordé qu'avec des restrictions appropriées telles que la divulgation à un tiers de confiance, la désagrégation, l'anonymisation ou le brouillage des données, dans la mesure où l'octroi du droit sans ces restrictions serait incompatible avec les droits d'autrui ou avec les intérêts publics.

(3) Le maître des données doit se conformer aux obligations prévues par le Principe 32 pour la protection des tiers, et les restrictions prévues au paragraphe 2 doivent en tout cas lui permettre de le faire.

Principe 21 : Cessation des activités relatives aux données co-générées

Les motifs qui, sous réserve du Principe 19, peuvent donner lieu au droit d'une partie d'exiger que le responsable du traitement cesse toute activité relative à des données générées conjointement, jusqu'à un droit d'exiger l'effacement des données, devraient inclure les situations dans lesquelles

(a) les activités relatives aux données causent, ou sont raisonnablement susceptibles de causer, un préjudice important, y compris un préjudice non économique, à cette partie ; et

(b) la finalité des activités relatives aux données est incompatible avec la manière dont cette partie a contribué à la production des données, notamment parce que

(i) cette partie a été incitée à contribuer à la production des données dans un but entièrement différent et on n'aurait pas pu raisonnablement s'attendre à ce qu'elle contribue à la production des données si elle avait connu ou prévu la finalité des activités relatives aux données menées par le responsable du traitement ; ou

(ii) le consentement de cette partie à sa contribution à la production des données pour cette finalité a été obtenu d'une manière incompatible avec les doctrines qui défendent des politiques publiques importantes, y compris celles qui protègent les parties contre des comportements ou des accords excessifs.

Principe 22 : Correction des données co-générées

Les motifs qui, sous réserve du Principe 19, peuvent donner lieu au droit d'une partie d'exiger que le responsable du traitement corrige les erreurs dans les données générées conjointement, y compris le caractère incomplet des données, devraient inclure les situations dans lesquelles le contrôle ou le traitement des données incorrectes peut causer un préjudice plus qu'insignifiant, y compris un préjudice non économique, aux intérêts légitimes de cette partie ou d'une autre partie, et les coûts de la correction ne sont pas disproportionnés par rapport au préjudice qui pourrait autrement en résulter.

Principe 23 : Part économique des bénéfices tirés des données co-générées

(1) Une partie n'a normalement pas droit à une part économique des bénéfices tirés par une autre partie de l'utilisation de données générées en commun, à moins qu'il n'existe une base contractuelle ou légale pour une telle revendication ou qu'elle fasse partie d'un arrangement individuel en vertu du Principe 19, paragraphe 3.

(2) Nonobstant le paragraphe 1, dans des cas exceptionnels, une partie peut avoir droit à une part économique des bénéfices tirés par un maître des données cogénérées de l'utilisation de ces données lorsque

(a) la contribution de cette partie à la génération des données

(i) était suffisamment unique pour ne pas pouvoir être remplacée, d'un point de vue économique, par les contributions d'autres parties ; ou

(ii) a occasionné à cette partie des efforts ou des dépenses significatifs ; et

(b) les bénéfices tirés par le responsable du traitement sont exceptionnellement élevés ; et

(c) la partie qui cherche à obtenir une part économique n'était pas, au moment où elle a contribué à la production des données, en mesure de négocier efficacement sa rémunération.

Chapitre C : Droits relatifs aux données dans l'intérêt public

Principe 24 : Justification des droits et obligations en matière de données

(1) La loi doit accorder des droits sur les données pour des raisons indépendantes de la part que la partie à laquelle les droits sont accordés a eue dans la production des données ("droits sur les données pour l'intérêt public"), uniquement si l'empiètement sur les intérêts légitimes du responsable du traitement ou de tout tiers est nécessaire, approprié et proportionné à l'intérêt public poursuivi.

(2) Le paragraphe 1 n'a pas pour objet de traiter des relations intergouvernementales.

(3) Le critère de proportionnalité visé au paragraphe 1 devrait également s'appliquer pour déterminer les spécifications ou les restrictions des droits sur les données, par exemple en ce qui concerne les formats de données, le calendrier, la sécurité des données, le soutien supplémentaire nécessaire pour que l'exercice du droit soit pleinement effectif et la rémunération due.

(4) Si la loi n'accorde pas de droit sur les données mais impose une obligation de partage des données fonctionnellement équivalente, les Principes du présent chapitre s'appliquent avec les ajustements appropriés.

Principe 25 : Octroi de l'accès aux données par le maître des données

(1) Si la loi accorde un droit d'accès aux données au sens du Principe 24, elle doit prévoir que le responsable du traitement doit fournir l'accès dans des conditions équitables, raisonnables et non discriminatoires au sein de la catégorie de parties auxquelles le droit a été accordé.

(2) Conformément au Principe 24, paragraphe 3, un droit d'accès aux données ne doit être accordé qu'avec des restrictions appropriées telles que la divulgation à un tiers de confiance, la désagrégation, l'anonymisation ou le brouillage des données, dans la mesure où l'octroi du droit sans ces restrictions serait incompatible avec les droits d'autrui ou avec les intérêts publics.

(3) Le maître des données doit se conformer aux obligations prévues par le Principe 32 pour la protection des tiers, et les restrictions prévues au paragraphe 2 doivent en tout cas lui permettre de le faire.

Principe 26 : Activités relatives aux données par le destinataire

(1) Si la loi accorde à une partie un droit d'accès aux données au sens du Principe 24, la loi doit prévoir que, sous réserve du paragraphe 2, la partie peut utiliser les données qu'elle reçoit de toute manière et à toute fin licite qui ne soit pas incompatible avec

(a) l'intérêt public pour lequel le droit a été accordé, à condition que le destinataire ait eu connaissance de cet intérêt ;

(b) les restrictions pour la protection d'autrui imposées en vertu du Principe 25, paragraphe 2 ; ou

(c) tout accord entre les parties, y compris un accord concernant les devoirs et les restrictions imposés par le contrôleur au destinataire en vertu du Principe 32.

(2) Une partie à qui un droit d'accès aux données est accordé en vertu du Principe 24 ne peut utiliser ces données d'une manière qui porte atteinte aux intérêts légitimes du maître des données initial plus qu'il n'est inhérent à l'objectif pour lequel le droit a été accordé.

Principe 27 : Réciprocité

Si la loi accorde un droit d'accès aux données au sens du Principe 24 à une partie contre un responsable du traitement, il s'agit d'un argument fort pour accorder un droit d'accès aux données similaire au maître des données initial contre la première partie dans des circonstances comparables. La question de savoir si cet argument doit prévaloir dépend, entre autres, de la question de savoir si l'octroi d'un tel droit réciproque serait incompatible avec l'objectif de fournir l'accès à la première partie.

Partie IV : Aspects des activités relatives aux données qui concernent les tiers

Chapitre A : Protection des tiers contre les activités relatives aux données

Principe 28 : Caractère illicite des activités relatives aux données vis-à-vis d'une autre partie

(1) Les activités relatives aux données sont illicites vis-à-vis d'une autre partie (une "partie protégée") si :

(a) elles violent un droit de la partie protégée qui a un effet de tiers en soi au sens du Principe 29 ;

(b) elles ne sont pas conformes aux limitations contractuelles des activités relatives aux données, applicables par la partie protégée, du type décrit au Principe 30 ; ou

(c) l'accès aux données a été obtenu de la partie protégée par des moyens non autorisés au sens du Principe 31.

(2) Pour déterminer si les activités relatives aux données sont illicites, il convient de tenir compte des conditions dans lesquelles ces activités sont exercées, telles que la fourniture d'un niveau adéquat de sécurité des données ou le respect de toute obligation en vertu du Principe 32.

(3) La mise en œuvre de cette règle devrait tenir compte des doctrines de justification applicables, telles que la liberté d'information et d'expression.

Principe 29 : Droits ayant un effet de tiers en soi

(1) Aux fins du Principe 28, paragraphe 1, point a, les droits ayant un effet de tiers en soi comprennent ce qui suit :

(a) les droits de propriété intellectuelle et les droits similaires ;

(b) les droits relatifs à la confidentialité et à la protection des données et les droits similaires ; et

(c) tous les autres droits qui, en vertu de la loi applicable, ont des effets similaires sur les tiers.

(2) La mesure dans laquelle les droits au sens du paragraphe 1 limitent les activités relatives aux données, ainsi que l'effet de ces limitations, sont déterminés par le droit applicable.

Principe 30 : Limitations contractuelles

(1) Aux fins du Principe 28, paragraphe 1, lettre b, une limitation contractuelle des activités relatives aux données est une clause contractuelle qui limite les activités relatives aux données de toute partie au contrat, notamment en limitant l'utilisation ou le transfert ultérieur des données.

(2) Pour déterminer si une limitation contractuelle des activités relatives aux données est en conflit avec les règles de droit impératives qui défendent des politiques publiques importantes et avec celles qui protègent les parties contre une conduite ou des conventions excessives, les facteurs à prendre en compte comprennent la question de savoir si l'entente

(a) limite indûment les libertés d'une partie contractante, en tenant compte, entre autres, des limites comparables de la protection de la propriété intellectuelle ;

(b) limite indûment les activités d'intérêt public ; ou

(c) a des effets discriminatoires ou anticoncurrentiels injustifiés.

Principe 31 : Accès non autorisé

(1) Aux fins du Principe 28, paragraphe 1, lettre c, l'accès aux données a été obtenu par des moyens non autorisés s'il a été obtenu :

(a) par le contournement des mesures de sécurité ;

(b) en profitant d'une erreur évidente, telle qu'une faille de sécurité dont la personne accédant aux données ne pouvait raisonnablement pas croire que le maître des données l'avait prévue ; ou

(c) l'interception par des moyens techniques de transmissions non publiques de données, y compris les émissions électromagnétiques d'un support transportant des données.

(2) L'accès aux données n'a pas été obtenu par des moyens non autorisés si

(a) l'accès aux données est autorisé en vertu d'un accord entre la personne qui accède aux données et le maître des données ; ou

(b) la personne accédant aux données avait un droit qui, en vertu d'une autre loi (telle que la loi relative à la liberté d'information et d'expression), prévaut sur le droit du responsable du traitement en vertu du présent Principe.

Chapitre B : Effets de la transmission ultérieure sur la protection d'autrui

Principe 32 : Obligations d'un fournisseur dans le cadre d'une fourniture ultérieure

(1) Lorsqu'une partie fournissant des données à un destinataire peut les transmettre mais est tenue de respecter des obligations et des restrictions au sens du chapitre A, la loi devrait exiger du fournisseur qu'il

(a) impose les mêmes obligations et restrictions au destinataire (à moins que celui-ci ne soit déjà lié par elles), y compris l'obligation de faire de même si le destinataire fournit les données à d'autres parties ; et

(b) prenne des mesures raisonnables et appropriées (y compris des garanties techniques) pour s'assurer que le destinataire, et toute partie à laquelle le destinataire peut fournir les données, se conformera à ces restrictions.

(2) Lorsque le fournisseur prend connaissance ultérieurement de faits qui indiquent des activités de données illicites au sens du Principe 28 de la part d'un destinataire, ou qui rendent les activités de données du destinataire illicites ou qui nécessiteraient autrement que des mesures soient prises au profit d'une partie protégée, le fournisseur doit prendre des mesures raisonnables et appropriées pour mettre fin aux activités illicites ou pour prendre d'autres mesures appropriées au profit d'une partie protégée.

(3) Aucune disposition du présent Principe n'exclut la responsabilité indirecte stricte d'un responsable du traitement pour les activités liées aux données menées par un gérant en vertu de la loi applicable.

(4) La question de savoir si les obligations du fournisseur en vertu du présent Principe peuvent être levées par la partie protégée ou modifiées par accord au détriment de cette partie est déterminée par la nature des obligations et restrictions pertinentes en vertu du chapitre A et de toute règle de droit applicable qui rend ces obligations non levables par la partie protégée.

Principe 33 : Action directe contre le destinataire en aval

Lorsqu'un destinataire immédiat de données avait l'obligation, en vertu du Principe 32, vis-à-vis de son fournisseur, d'imposer des conditions particulières à un destinataire en aval auquel le destinataire immédiat fournira les données, et lorsque le destinataire immédiat a respecté cette obligation mais que le destinataire en aval viole les conditions qui lui ont été imposées, le fournisseur initial peut agir directement contre le destinataire en aval après en avoir avisé le destinataire immédiat.

Principe 34 : Effet de l'illicéité à l'égard de l'acquéreur en aval

(1) Outre l'illicéité découlant directement du chapitre A, une activité relative à des données exercée par un destinataire en aval qui a reçu les données d'un fournisseur est illicite lorsque (i) le contrôle exercé par ce fournisseur était illicite, (ii) ce fournisseur a agi de manière illicite en transmettant les données ou (iii) ce fournisseur a agi de manière illicite en n'imposant pas au destinataire en aval une obligation ou une restriction en vertu du Principe 32 qui aurait exclu l'activité relative aux données, et que le destinataire en aval

(a) a été informé de l'action fautive du fournisseur au moment où l'activité relative aux données est menée ; ou

(b) n'a pas effectué, au moment de la réception des données, l'enquête à laquelle on pouvait raisonnablement s'attendre dans les circonstances.

(2) Le paragraphe 1 ne s'applique pas lorsque

(a) l'illicéité de la part du fournisseur n'était pas importante dans les circonstances et on ne pouvait raisonnablement s'attendre à ce qu'elle cause un préjudice important à une partie protégée en vertu du chapitre A ;

(b) le destinataire en aval n'a été informé qu'après la fourniture des données, et les intérêts du destinataire en aval en matière de confiance l'emportent clairement, dans ces circonstances, sur les intérêts légitimes d'une partie protégée par le chapitre A ; ou

(c) les données étaient généralement accessibles aux personnes qui traitent normalement le type d'informations en question.

(3) Les paragraphes 1 et 2 s'appliquent, avec les ajustements appropriés, aux activités relatives aux données menées par une partie qui n'a pas reçu les données d'un fournisseur, mais qui a autrement obtenu l'accès aux données par l'intermédiaire d'une autre partie.

Chapitre C : Effets des autres activités relatives aux données sur la protection des tiers

Principe 35 : Devoirs d'un maître des données en matière de traitement des données et de données dérivées.

(1) Si un maître des données peut traiter des données mais qu'il est tenu de respecter des devoirs et des restrictions au sens du chapitre A, il doit, lorsqu'il traite ces données, faire preuve de la diligence raisonnable en fonction des circonstances pour

(a) déterminer les moyens et les finalités du traitement qui sont compatibles avec les obligations et les restrictions ; et

(b) vérifier quels devoirs et restrictions s'appliquent aux données dérivées et prendre des mesures raisonnables et appropriées pour s'assurer que les devoirs et restrictions sont respectés.

(2) La question de savoir si les obligations et restrictions relatives aux données originales s'appliquent également aux données dérivées, ou si des obligations et restrictions moindres ou supplémentaires s'appliquent, doit être déterminée par les règles et principes régissant la source de protection pertinente en vertu du chapitre A. En cas de doute, les considérations à prendre en compte sont notamment les suivantes :

(a) le degré de différence entre les données dérivées et les données originales, par exemple si les données originales peuvent être reconstituées à partir des données dérivées au moyen de mesures raisonnables de désagrégation ou d'ingénierie inverse ; et

(b) le degré auquel les données dérivées présentent un risque pour une partie protégée par rapport au risque posé par les données originales.

(3) Si le traitement des données originales n'était pas illicite, mais que des événements ultérieurs se produisent qui rendraient le même type de traitement illicite, cela ne rend pas rétroactivement le traitement antérieur illicite.

Principe 36 : Traitement illicite

(1) Lorsque le traitement des données est illicite, le maître des données doit prendre toutes les mesures raisonnables et appropriées pour annuler le traitement, par exemple en désagrégeant les données ou en supprimant les données dérivées, même si les obligations et les restrictions prévues aux chapitres A et B ne s'appliquent pas, conformément au Principe 35, aux données dérivées.

(2) Dans la mesure où il n'est pas possible d'annuler le traitement dans les cas couverts par le paragraphe 1 ou lorsque cela signifierait une destruction de valeurs qui n'est pas raisonnable à la lumière des circonstances donnant lieu à l'illicéité de la part du responsable du traitement et des intérêts légitimes de toute partie protégée en vertu du chapitre A, une allocation peut être faite en argent chaque fois et dans la mesure où cela est raisonnable dans les circonstances et peut être combinée avec des restrictions à

l'utilisation ultérieure des données dérivées. Les facteurs à prendre en compte scomprennent

(a) la question de savoir si le responsable du traitement avait connaissance de l'illicéité au moment du traitement ;

(b) les finalités du traitement ;

(c) si l'illicéité était importante dans les circonstances ou si l'on pouvait s'attendre à ce qu'elle cause un préjudice important à une partie protégée en vertu du chapitre A ; et

(d) le montant de l'investissement réalisé dans le traitement, et la contribution relative des données originales aux données dérivées.

(3) Les paragraphes 1 et 2 s'appliquent avec des ajustements appropriés aux produits ou services développés à l'aide des données originales.

Principe 37 : Effet de la non-conformité non matérielle

(1) Si un maître des données exerce des activités relatives aux données concernant un grand ensemble de données, et que ces activités ne sont pas conformes aux obligations et aux restrictions prévues au chapitre A en ce qui concerne certaines des données, la loi devrait prévoir que ces activités ne sont pas illicites en ce qui concerne l'ensemble des données si

(a) la non-conformité n'est pas importante dans les circonstances, par exemple lorsque les données concernées ne représentent qu'une partie insignifiante de l'ensemble de données à l'égard duquel les activités relatives aux données ont lieu ;

(b) le maître des données a fait les efforts que l'on pouvait raisonnablement attendre, dans les circonstances, pour se conformer aux obligations et aux restrictions ; et

(c) les activités relatives aux données ne sont pas liées à la finalité pour laquelle les obligations ou les restrictions prévues au chapitre A sont imposées et on ne peut raisonnablement s'attendre à ce qu'elles causent un préjudice important à une partie protégée.

(2) Lorsque le paragraphe 1 s'applique, le maître des données doit, dès la notification, retirer les données concernées de l'ensemble de données aux fins d'activités de données futures, à moins que cela ne soit déraisonnable dans les circonstances.

Partie V : Questions concernant plusieurs États

Principe 38 : Application des règles d'élection de droit établies du forum

(1) Lorsqu'une question relève du champ d'application territorial de la loi de plus d'un État, la loi applicable à cette question est déterminée par les règles de choix de la loi du for. Les présents Principes ne déterminent pas le champ d'application territorial de la loi d'un État.

(2) La loi applicable aux contrats de données en vertu de la Partie II devrait être la loi de l'Etat qui serait choisi en vertu des règles de choix de la loi applicable aux contrats du for.

(3) Pour toute autre question découlant des présents Principes, la loi applicable à cette question devrait être

(a) la loi de l'Etat qui serait choisi en vertu des règles de conflit de lois du for si ces règles prévoient une règle claire pour déterminer la loi applicable à cette question ; ou

(b) si les règles de conflit de lois du for ne prévoient pas de règle claire pour déterminer la loi applicable à cette question, la loi déterminée par l'application du Principe 39.

Principe 39 : Questions non couvertes par les règles établies de choix de la loi du for

(1) La loi applicable aux questions qui ne sont pas déjà couvertes par le Principe 38 devrait être la loi de l'État qui présente le lien le plus significatif avec la question juridique en cause. Les contacts à prendre en compte pour déterminer l'État qui présente le lien le plus significatif sont les suivants

(a) le lieu où les activités relatives aux données (i) sont destinées à produire des effets sur les intérêts pertinents ou (ii) produisent effectivement des effets ;

(b) le domicile, la résidence, la nationalité, le lieu de constitution et l'établissement de la partie qui fait valoir un droit et de la partie contre laquelle il est fait valoir ; et

(c) la loi de l'État qui régit, le cas échéant, un rapport juridique préexistant entre la partie qui fait valoir un droit et la partie contre laquelle il est fait valoir ; et

(d) le lieu où les données sont générées.

(2) Les parties peuvent, par accord mutuel conclu après la naissance d'un litige, choisir l'État dont la loi régira leur relation juridique en ce qui concerne une question juridique traitée par les présents Principes, à moins que cela ne soit incompatible avec la nature de la question juridique ou des considérations d'ordre public.

Principe 40 : Pertinence du lieu de stockage

(1) Sous réserve du paragraphe 2, aux fins du choix de la loi applicable, le lieu de stockage des données n'est pertinent en tant que facteur de rattachement que lorsque la question en cause porte sur le stockage ou les droits sur le support.

(2) Le lieu de stockage des données peut être pertinent aux fins du choix de la loi applicable en tant que facteur de rattachement de nature résiduelle, par exemple en l'absence d'autres facteurs de rattachement ou lorsque l'examen d'autres facteurs de rattachement est indéterminé.

(3) Le fait que les données soient stockées en dehors d'un État ne soulève généralement pas en soi de problèmes d'exercice extraterritorial de la compétence ou d'application du droit, tant qu'il existe des liens suffisants entre l'État et les activités relatives aux données qu'il cherche à réglementer ou les droits relatifs aux données qu'il cherche à faire respecter.

Translation as of 30 June 2022, still to be partially revised.

Pascal Pichonnaz / Benoît de Mestral