

Conformément à la résolution ACHPR/Res.620 (LXXXI) 2024

**LIGNES DIRECTRICES AFRICAINES
SUR LA PROMOTION ET L'EXPLOITATION DE L'ACCÈS AUX DONNÉES COMME OUTIL
DE PROMOTION DES DROITS DE L'HOMME ET LE DÉVELOPPEMENT DURABLE
À L'ÈRE NUMÉRIQUE**

Table of Contents

AVANT-PROPOS	3
DÉFINITIONS	7
PRINCIPES CLÉS	10
Mesures générales	12
Exemptions et garanties	16
Application	18
ACCÈS, ÉTHIQUE ET IA	20
MISE EN ŒUVRE	21
ANNEXE A : MESURES CONCERNANT DES DONNÉES SPÉCIFIQUES	22
ANNEXE B : MESURES INSTITUTIONNELLES	25
ANNEXE C : ARCHITECTURE INSTITUTIONNELLE POUR L'ACCÈS AUX DONNÉES	26

AVANT-PROPOS

Les présentes Lignes Directrices, sont publiées par la Commission africaine des droits de l'homme et des peuples (la Commission africaine) conformément à la résolution 620 intitulée « Promouvoir et exploiter l'accès aux données comme outil de promotion des droits de l'homme et de développement durable à l'ère numérique », adoptée par la Commission africaine lors de sa 81e session ordinaire.

La résolution 620 reconnaît qu'à l'ère numérique, les données ne sont pas simplement une ressource à gérer, mais une condition préalable à la réalisation des droits de l'homme et à la mise en œuvre du développement durable. La résolution invite les États parties à adopter des mesures garantissant l'accès aux données détenues tant par les acteurs publics que par les acteurs privés concernés, dans le but de promouvoir les droits de l'homme et le développement durable. La résolution charge le Rapporteur Spécial sur la liberté d'expression et l'accès à l'information en Afrique de mener de larges consultations à travers le continent et d'élaborer des normes appropriées pour encadrer la collecte, l'utilisation et l'accès aux données. Les présentes Lignes Directrices sont publiées en application de ce mandat.

Les Lignes Directrices sont le fruit de consultations approfondies avec les parties prenantes, notamment les acteurs étatiques, du secteur public et privé, les organisations de la société civile, les défenseurs des droits numériques et les chercheurs à travers le continent. Elles reflètent la diversité des expériences africaines et l'engagement commun à garantir que la transformation numérique serve la jouissance des droits de l'homme et le développement.

L'objectif des Lignes Directrices est d'élaborer des mesures politiques, juridiques et institutionnelles, en réponse à un contexte dans lequel :

- Les cadres existants en matière d'accès à l'information, bien qu'essentiels, ne répondent pas de manière adéquate aux défis de mise en œuvre spécifiques posés par le volume, la complexité et la nature propriétaire des données, ainsi que par la prédominance du secteur privé dans le contrôle et l'accès aux données ;
- Sans une transparence, une surveillance ou des voies de recours adéquates, l'intelligence artificielle fondée sur les données, les systèmes algorithmiques et la prise de décision automatisée peuvent porter gravement atteinte aux droits de l'homme ;
- Les flux transfrontaliers de données, notamment la position dominante des entreprises technologiques transnationales dans le traitement et le stockage des données, posent des défis particuliers pour l'application des cadres juridiques nationaux ;
- L'accès inégal aux infrastructures numériques, à la connectivité et à la culture numérique – tant entre les États africains qu'au sein de ceux-ci – exacerbe les inégalités existantes et exclut les communautés marginalisées des avantages d'une gouvernance et d'un développement fondés sur les données ;
- Les femmes et les filles, les personnes handicapées, les jeunes, les peuples autochtones, les communautés rurales et d'autres groupes marginalisés sont exposés à des risques accrus de préjudices liés aux données et se heurtent à des obstacles spécifiques pour accéder aux données essentielles à la réalisation de leurs droits ;
- Les lois sur la protection des données et de la vie privée, bien qu'essentiels, ont parfois été utilisées pour bloquer l'accès légitime à des données d'intérêt public, entravant ainsi la transparence, la responsabilité et le droit à l'information ;
- De nombreux États africains pourraient tirer profit de la mise en place d'institutions de contrôle efficaces et indépendantes, dotées du pouvoir de statuer sur l'accès aux données, d'ordonner des mesures correctives et de garantir le respect des obligations en matière d'accès.

Dans ce contexte, les Lignes Directrices proposent des mesures qui, ensemble, serviront à promouvoir et à exploiter l'accès aux données comme un outil pour la promotion des droits de l'homme et du développement durable à l'ère numérique. Elles constituent un instrument de droit non contraignant qui offre une interprétation faisant autorité des obligations des États parties au titre de la Charte africaine, en particulier des articles 9 (droit de recevoir des informations) et 22 (droit au développement). Elles s'appuient sur la jurisprudence existante de la Commission en matière d'accès à l'information, de vie privée, de démocratie, de développement et de droits numériques. Les Lignes Directrices visent à soutenir :

- Les États parties : en tant que modèle pour les réformes législatives, politiques et institutionnelles, ainsi que référence pour le respect des obligations découlant de la Charte africaine ;
- Les organes judiciaires et quasi-judiciaires : en tant qu'aide à l'interprétation pour statuer sur les litiges relatifs à l'accès aux données ;
- Les institutions nationales des droits de l'homme et la société civile : en tant que cadre pour le suivi, le plaidoyer et la responsabilisation ;
- Les acteurs du secteur privé : en tant que guide sur les meilleures pratiques en matière de transparence, de responsabilité et de gouvernance responsable des données ;
- Les institutions régionales et sous-régionales : en tant que référence pour aligner les instruments de gouvernance numérique sur les normes en matière de droits de l'homme et pour élaborer des approches africaines transnationales.

Le droit d'accès aux données n'est pas un luxe que l'on peut se permettre de reporter. Il est fondamental pour la dignité humaine, la gouvernance démocratique et la poursuite collective d'une Afrique juste et prospère. Veillons à ce que l'accès aux données soit conçu de manière à garantir que la transformation numérique ne laisse personne de côté.

Madame la Commissaire Geereesha Topsy-Sonoo,
Rapporteur Spécial sur la liberté d'expression et l'accès à l'information en Afrique

PRÉAMBULE

Réaffirmant son mandat en vertu de l'article 45 de la Charte africaine des droits de l'homme et des peuples (la Charte africaine), y compris le pouvoir de formuler et d'établir des principes et des règles sur lesquels les États africains peuvent fonder leur législation ;

Rappelant la résolution 620 intitulée « Promouvoir et exploiter l'accès aux données comme outil de promotion des droits de l'homme et du développement durable à l'ère numérique », qui reconnaît l'importance des données pour la promotion des droits de l'homme et du développement durable et qui charge le Rapporteur Spécial sur la liberté d'expression et l'accès à l'information en Afrique d'élaborer des normes appropriées en conséquence ;

Rappelant l'article 9 de la Charte africaine, qui garantit à toute personne le droit d'accès à l'information, et reconnaissant en outre que, à l'ère numérique, ce droit inclut l'accès aux données ;

Rappelant l'article 22 de la Charte africaine, qui affirme le droit au développement, et reconnaissant en outre que l'accès aux données est essentiel à la réalisation de ce droit, notamment en permettant une participation éclairée à la planification du développement, à la prise de décision et aux opportunités économiques ;

Rappelant en outre que les droits consacrés par la Charte africaine sont indivisibles, interdépendants et étroitement liés, et que l'accès aux données est nécessaire à la jouissance effective des droits civils, politiques, économiques, sociaux et culturels ;

Reconnaissant les articles 19 et 21 de la Déclaration Universelle des Droits de l'Homme et les articles 19 et 25 du Pacte International relatif aux Droits Civils et Politiques, qui garantissent le droit d'accès à l'information et le droit de participer à des élections périodiques, véritables, libres, équitables et crédibles ;

Rappelant la Déclaration de Principes sur la liberté d'expression et l'accès à l'information en Afrique, la Loi type sur l'accès à l'information pour l'Afrique et les Lignes Directrices sur l'accès à l'information et les élections en Afrique, ainsi que diverses autres résolutions, qui, ensemble, établissent le cadre normatif sous-tendant les droits dont jouissent les citoyens grâce aux écosystèmes de l'information sur le continent, y compris les droits à l'accès à l'information, à la vie privée et à la protection des données, à la participation politique et à la liberté d'expression ;

Reconnaissant la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel ainsi que le Cadre de politique de l'Union africaine en matière de données, qui constituent d'importants cadres régionaux pour la gouvernance des données ;

Affirmant que l'accès aux données et la protection des données à caractère personnel sont des obligations complémentaires, et que toute restriction d'accès doit être prévue par la loi, poursuivre un but légitime et être strictement nécessaire et proportionnée dans une société démocratique ;

Rappelant en outre la résolution 473 sur la nécessité de mener une étude sur les droits de l'homme et des peuples et l'intelligence artificielle (IA), la robotique et d'autres technologies nouvelles et émergentes en Afrique, qui souligne l'engagement de la Commission envers les technologies émergentes ayant une incidence sur l'accès aux données ;

Prenant note de la Stratégie de transformation numérique pour l'Afrique (2020-2030) de l'Union africaine et de l'Agenda 2063, pour lesquels l'accès aux données est fondamental pour le développement inclusif, l'innovation et l'intégration continentale ;

Reconnaissant que les droits de l'homme consacrés par la Charte africaine dépendent de plus en plus de l'accès aux données à l'ère numérique ;

Réaffirmant que l'accès aux données pour le bien public peut favoriser la réalisation des droits de l'homme et l'innovation sociétale, ainsi que soutenir les progrès vers la réalisation du droit au développement, des objectifs de développement durable et de l'Agenda 2063 : *L'Afrique que nous voulons* ;

Préoccupée par le fait que, malgré la prolifération des technologies fondées sur les données, il n'existe pas de lignes directrices adaptées à l'intention des gouvernements africains et des acteurs privés sur la promotion et l'exploitation de l'accès aux données, comme le prévoit la Résolution 620 ;

La Commission africaine des droits de l'homme et des peuples, réunie en [...] session ordinaire, tenue [...]

Adopte les Lignes Directrices africaines sur l'accès aux données, un instrument visant à promouvoir et à exploiter l'accès aux données en tant qu'outil de promotion des droits de l'homme et du développement durable à l'ère numérique.

DÉFINITIONS

La Charte africaine désigne la Charte africaine des droits de l'homme et des peuples.

La Commission africaine désigne la Commission africaine des droits de l'homme et des peuples.

L'anonymisation désigne le processus consistant à modifier des enregistrements de manière qu'ils ne se rapportent pas à une personne physique identifiée ou identifiable, ou le processus consistant à rendre des données à caractère personnel anonymes de manière à ce que la personne concernée ne soit pas ou ne soit plus identifiable.

L'intelligence artificielle (IA) désigne un logiciel capable d'effectuer des tâches qui requièrent généralement l'intelligence humaine, notamment en faisant preuve d'une capacité à imiter l'apprentissage, le raisonnement et la prise de décision humains. La prise de décision automatisée dans le cadre de l'IA désigne les décisions prises sans intervention humaine significative. Tous les systèmes d'IA dépendent de données tant pour leurs modèles d'apprentissage que pour leurs applications ultérieures, telles que les inférences en temps réel et les résultats génératifs.

Les données englobent la représentation sous forme électronique d'informations à un niveau granulaire, avec un potentiel de conversion en signification de niveau supérieur. Elles comprennent généralement des signaux et des enregistrements sous toutes leurs formes, collectés, stockés, traités ou partagés dans des formats structurés ou non structurés, y compris du texte, des images, du son, de la vidéo et des impulsions de capteurs. Elles intègrent des données à caractère personnel (relatives à une personne identifiée ou identifiable) et des données non personnelles (telles que des données environnementales ou statistiques). L'information elle-même peut être traitée comme des données en vue d'opérations ultérieures de conversion des connaissances.

Un ensemble de données désigne une collection de données, généralement organisée sous forme de tableaux, de tableaux de données ou de formats spécifiques, tels que CSV ou JSON, afin de faciliter la récupération et l'analyse. Les ensembles de données sont essentiels pour l'analyse de données, l'apprentissage automatique, l'IA et d'autres applications qui nécessitent des données fiables et accessibles. Avec l'IA générative, les ensembles de données peuvent également être constitués à partir de données non structurées, élargissant ainsi les possibilités d'organisation et d'utilisation des données en tant que ressource.

L'accès aux données désigne le droit légal ou la capacité technique de récupérer, consulter, utiliser, déplacer ou manipuler des données dans le cadre du droit plus large à l'information, y compris auprès de détenteurs de données relevant d'organismes publics et privés, et est rendu possible par la disponibilité, l'intégrité et la facilité d'utilisation de ces données. L'accès peut être obtenu par le téléchargement des données ou par leur traitement ailleurs, y compris sur site, avec la possibilité d'enregistrer les résultats de ce traitement.

L'écosystème des données désigne l'intégration et l'interaction entre les différentes parties prenantes concernées, notamment les détenteurs de données, les producteurs de données, les intermédiaires de données et les personnes concernées, qui sont impliqués dans les accords d'accès et de partage des données ou affectés par ceux-ci en fonction de leurs différents rôles, responsabilités et droits, technologies et modèles économiques. La capacité et l'engagement de l'État sont nécessaires pour promouvoir l'accès à cet écosystème et garantir que les droits de l'homme et la souveraineté nationale ne soient pas compromis.

Les détenteurs de données désignent les entités ou les personnes physiques qui ont l'autorité légale d'autoriser le partage et l'accès aux données. Ils peuvent être des responsables du traitement au sens des lois sur la protection des données, et sont tenus de rendre compte des opérations de traitement des données.

On entend par **«intermédiaires de données»** les entités intervenant dans les mécanismes d'accès aux données et de partage de données qui facilitent l'accès aux données et/ou le partage de données, ou l'échange commercial de données.

La culture des données désigne la capacité du public à reconnaître et à faire valoir ses droits en ce qui concerne les opportunités et les risques liés aux questions relatives aux données, sur la base de ses connaissances et de ses compétences ainsi que de sa compréhension des paramètres juridiques, éthiques et institutionnels applicables.

Le partage de données désigne le fait de fournir un accès aux données à des fins d'utilisation par des tiers, sous réserve des exigences techniques, financières, juridiques ou organisationnelles applicables. Le partage peut s'effectuer

directement ou par l'intermédiaire d'un intermédiaire de données et peut s'inscrire dans le cadre de diverses conditions de licence.

La personne concernée désigne une personne physique identifiable ou un groupe identifiable auquel se rapportent les données, y compris les communautés relevant du droit coutumier ou national, et qui a le droit de consentir à la collecte, au traitement et à la diffusion de ses données.

Les données dynamiques désignent des enregistrements sous forme numérique, soumis à des mises à jour fréquentes ou en temps réel, notamment en raison de leur volatilité ou de leur obsolescence rapide ; les impulsions électriques générées par des capteurs sont généralement considérées comme des données dynamiques.

Les ensembles de données à haute valeur ajoutée désignent des enregistrements dont la réutilisation est associée à des avantages importants pour la société, l'environnement et l'économie, notamment en raison de leur aptitude à permettre la création de services à valeur ajoutée, d'applications et d'emplois nouveaux, de haute qualité et décents, ainsi qu'en raison du nombre de bénéficiaires potentiels des services à valeur ajoutée et des applications basés sur ces ensembles de données.

L'information comprend tout document original ou copie de documents, quelles que soient ses caractéristiques physiques, tels que les dossiers, la correspondance, les faits, les opinions, les conseils, les publicités, les mémorandums, les données, les statistiques, les livres, les dessins, les plans, les cartes, les diagrammes, les photographies, les enregistrements audio ou visuels, ainsi que tout autre matériel tangible ou intangible, quelle que soit la forme ou le support sous lequel il est conservé.

L'intégrité de l'information désigne l'exactitude, la cohérence et la fiabilité du contenu, des processus et des systèmes d'information afin de maintenir un écosystème d'information digne de confiance, et elle repose fondamentalement sur l'intégrité sous-jacente des données.

L'interopérabilité désigne la facilité technique permettant à deux ou plusieurs espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin d'exercer leurs fonctions.

Par « **format lisible par machine** », on entend un format de fichier structuré telle manière que les applications logicielles peuvent facilement identifier, reconnaître et extraire des données spécifiques, y compris des déclarations de fait individuelles, ainsi que leur structure interne.

Les métadonnées désignent des informations descriptives sur les données primaires. Les métadonnées peuvent inclure des données à caractère personnel.

Par « **format ouvert** », on entend un format de fichier indépendant de toute plateforme et mis à la disposition du public sans aucune restriction entravant sa réutilisation.

Les données ouvertes désignent les données mises à disposition dans un format lisible par machine, gratuitement et sous une licence ouverte qui autorise l'utilisation, la réutilisation et la redistribution sans restriction.

Les données à caractère personnel désignent toute information se rapportant à une personne physique identifiée ou identifiable, permettant d'identifier cette personne, directement ou indirectement, notamment par le biais d'identifiants tels que le nom, le numéro d'identification, les données de localisation ou l'identifiant en ligne, ou de facteurs propres à l'identité physique, juridique, physiologique, mentale, économique, culturelle ou sociale d'une personne.

La pseudonymisation désigne le traitement des données à caractère personnel de telle manière que ces données ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne soient pas attribuées à une personne physique identifiée ou identifiable.

Par « **Organisme privé** », on entend : (a) une personne physique qui exerce ou a exercé une activité commerciale, industrielle, artisanale ou libérale, mais uniquement à ce titre ; (b) une société de personnes qui exerce ou a exercé une

activité commerciale, industrielle, artisanale ou libérale ; ou (c) toute personne morale ou tout ayant droit ; à l'exclusion des organismes publics et des organismes privés concernés.

La divulgation proactive désigne un flux régulier d'informations consistant à fournir systématiquement des informations au public sans que celui-ci ait à en faire la demande.

On entend par «**Autorités publiques**» les personnes morales, les organes législatifs et les autorités judiciaires, dans la mesure où ils exercent des fonctions administratives, telles que définies par le droit national.

On entend par «**Organisme public**» toute autorité administrative aux niveaux national, régional et local (par exemple, le gouvernement central, les gouvernements provinciaux et autres collectivités locales, la police, les autorités chargées de la santé publique et de l'éducation, les services d'archives publiques, etc.) ainsi que les autorités publiques.

L'intérêt public est un critère qui désigne les avantages partagés par la société dans son ensemble (par exemple, les services publics et les infrastructures) plutôt que la promotion exclusive d'intérêts individuels, collectifs ou privés. Ces avantages sont promus et protégés par tous, et en particulier par les organismes publics. Déterminer l'intérêt public implique de comparer des évaluations contradictoires de l'impact potentiel et d'examiner les compromis à long terme.

La valeur publique désigne la valeur créée pour le grand public et l'intérêt social, y compris le secteur public, comme l'utilisation des données pour la participation aux politiques publiques et à d'autres fins d'intérêt public, afin de garantir la durabilité, l'équité ou l'inclusivité, ainsi qu'un impact positif sur la société, l'économie et l'environnement.

Publier signifie mettre à disposition sous une forme et d'une manière facilement accessibles au public, ce qui inclut la fourniture de copies ou la mise à disposition d'informations par le biais de la radiodiffusion et des moyens de communication électroniques.

Par « **Organisme privé concerné** », on entend tout organisme qui serait autrement un organisme privé au sens des présentes Lignes Directrices et qui est (a) détenu en tout ou en partie, ou contrôlé ou financé, directement ou indirectement, par des fonds publics, mais uniquement dans la mesure de ce financement ; ou (b) exerçant une fonction statutaire ou publique ou un service statutaire ou public, mais uniquement dans la mesure de cette fonction statutaire ou publique ou de ce service statutaire ou public.

Les données de recherche désignent les documents sous forme numérique, autres que les publications scientifiques, qui sont collectés ou produits dans le cadre d'activités de recherche scientifique et qui sont utilisés comme éléments de preuve dans le processus de recherche, ou qui sont communément acceptés au sein de la communauté scientifique comme nécessaires pour valider les conclusions et les résultats de la recherche.

Les droits sui generis en matière de propriété intellectuelle désignent l'application, dans certaines juridictions, de droits uniques à des catégories spécifiques de propriété intellectuelle, telles que la protection des bases de données lorsque celles-ci ne donnent pas lieu à des droits en vertu des lois traditionnelles sur la propriété intellectuelle, comme le droit des brevets ou le droit d'auteur.

Les données sensibles désignent les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, les informations relatives à la santé, les données biométriques ou génétiques, ou toute autre information nécessitant une protection renforcée.

PRINCIPES CLÉS

Les présentes Lignes Directrices s'inspirent directement de la Résolution 620, qui reconnaît que l'accès aux données constitue un élément essentiel du droit à l'information et est vital en tant qu'outil pour les droits de l'homme, la démocratie et le développement durable. Les mesures énoncées dans ces Lignes Directrices s'appuient sur les principes suivants, directement inspirés de la Résolution de la Commission :

Les données en tant qu'atout stratégique : les données constituent un atout public stratégique doté d'un potentiel transformateur pouvant être utilisé dans l'intérêt public, pour créer de la valeur publique, promouvoir la démocratie et la bonne gouvernance, et contribuer à la réalisation des objectifs de développement convenus au niveau international et africain. Les données doivent donc servir à soutenir les politiques, les services ou les interventions qui améliorent le bien-être de la société, la transparence et la responsabilité.

Accès aux données dès la conception : les systèmes de collecte, de stockage et de diffusion des données doivent être conçus avec des fonctionnalités de divulgation proactive, des normes d'accessibilité, ainsi que des dispositions en matière d'interopérabilité et de sécurité par défaut.

Divulgation proactive : l'accès sans qu'il soit nécessaire de formuler une demande active devrait s'appliquer, au minimum, aux ensembles de données clés d'intérêt public tels que les données relatives aux budgets, aux marchés publics, à la santé, à l'éducation et à l'environnement, et être mis à disposition dans des formats ouverts et réutilisables.

Divulgation maximale : le principe de divulgation maximale devrait être la norme par défaut pour toutes les données publiques et pour les données pertinentes des organismes privés. La divulgation devrait être présumée, sauf si elle est manifestement préjudiciable. Les restrictions d'accès doivent constituer une exception étroite, strictement justifiée par les normes internationales en matière de droits de l'homme.

Justice et équité en matière de données : Les individus ont le droit d'obtenir des informations pertinentes sur la provenance, la logique, la portée, les conséquences et les catégories de données utilisées dans les processus décisionnels automatisés qui affectent leurs droits ; ils ont également le droit de contester les décisions fondées exclusivement sur un traitement automatisé et de demander un réexamen par un être humain. En outre, les initiatives en matière de données doivent être conçues pour lutter contre les inégalités structurelles et garantir que les communautés marginalisées et vulnérables bénéficient d'un accès équitable aux données, à leur gouvernance et aux avantages découlant de leur utilisation.

Intégrité des données et intégrité de l'information : pour être significatif, le droit d'accès aux données exige que celles-ci présentent une intégrité en termes d'exactitude, de cohérence et de fiabilité des processus et des systèmes, ce qui renforce encore l'intégrité de l'information et un écosystème d'information digne de confiance.

Complémentarité entre l'accès aux données et la protection des données : L'accès aux données et la protection des données à caractère personnel sont des obligations complémentaires. Aucune ne doit être poursuivie au détriment de l'autre. Les cadres de protection des données doivent prévoir des exceptions pour l'accès légitime aux données d'intérêt public, et les cadres d'accès doivent intégrer des garanties visant à protéger les données à caractère personnel contre toute utilisation abusive, toute discrimination et toute surveillance illégale.

Transparence, responsabilité et éthique : La collecte, le traitement et l'utilisation des données doivent être transparents et responsables. Des principes éthiques doivent être intégrés dans toutes les initiatives relatives aux données, avec des mécanismes permettant de remédier aux biais dans les données et la prise de décision automatisée. En outre, les données constituent un outil indispensable à la responsabilité et doivent donc être accessibles aux journalistes et aux chercheurs pour les questions d'intérêt public, afin de demander des comptes aux pouvoirs publics et de favoriser un débat public bien informé.

Responsabilité du secteur privé : Les États parties ont l'obligation positive de réglementer les acteurs privés dont les pratiques en matière de données ont une incidence sur la jouissance des droits de l'homme. Les présentes Lignes Directrices s'étendent aux données détenues par des entités privées lorsque ces données sont nécessaires à l'exercice des droits de l'homme, présentent un intérêt public significatif, en plus des cas d'entités privées pertinents définis ci-

dessus. Les cadres juridiques imposant des obligations de transparence, de responsabilité et d'accès doivent englober les acteurs du secteur privé lorsque les données sont impliquées dans des atteintes ou des avantages pour les droits de l'homme.

Recours effectifs : Toute personne à qui l'on refuse le droit d'accéder à des données devrait avoir droit à un recours effectif devant un organisme indépendant ayant le pouvoir d'ordonner la divulgation, d'imposer des sanctions et d'accorder une réparation appropriée.

MESURES

Mesures générales

Afin de garantir un cadre solide et cohérent pour la gouvernance des données, qui accorde une attention adéquate aux questions d'accès et s'aligne sur les normes régionales et internationales, les orientations fixées par les Lignes Directrices définissent 12 mesures à prendre :

1. Transposer la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel ainsi que le Cadre de politique des données de l'Union africaine dans le droit national afin d'assurer la cohérence et de faciliter l'interopérabilité régionale.
2. Adopter une approche pangouvernementale des cadres de données afin de permettre une coordination efficace des politiques et une participation globale de toutes les parties prenantes.
3. Créer ou renforcer un cadre national intégré de gestion des données (détaillé ci-dessous) qui favorise la production et l'accès aux données pertinentes pour les droits de l'homme et le développement, et qui favorise la circulation équitable et sécurisée des données entre le gouvernement, les particuliers, la société civile, le monde universitaire et le secteur privé, tout en protégeant contre les violations de la sécurité des données ainsi que contre les formes d'extraction et de traitement qui violent les droits de l'homme.
4. Élaborer et mettre en œuvre une politique nationale en matière de données ouvertes qui oblige les institutions publiques et les organismes bénéficiant de fonds publics à rendre les données accessibles au public de manière proactive.
5. Normaliser les procédures d'accès aux données publiques et privées, y compris en imposant des exigences cohérentes en matière de justification en cas de non-divulgateion.
6. Veiller à ce que les détenteurs et les sous-traitants de données obtiennent le consentement éclairé lorsque cela est requis, limitent l'utilisation des données à des finalités bien définies et respectent les droits des personnes concernées en matière d'accès, de rectification et de suppression.
7. Mettre en place un cadre juridique clair qui définit de manière précise les circonstances dans lesquelles les organismes du secteur public et d'autres parties prenantes peuvent accéder aux données détenues par des organismes privés dans des situations d'intérêt public supérieur réel et démontrable (telles que les urgences publiques, les crises sanitaires avérées ou le contrôle électoral prévu par la loi). Cet accès doit être soumis à des critères stricts de nécessité et de proportionnalité, à un contrôle indépendant ou à un contrôle juridictionnel, ainsi qu'à des protocoles rigoureux de sécurité des données et à des garanties en matière de responsabilité.
8. Créer ou désigner officiellement une institution publique telle qu'une commission de l'information ou une autorité de protection des données (ou une entité hybride ou équivalente), et la doter de pouvoirs juridiques, de capacités techniques et de ressources financières suffisants pour superviser la gouvernance des données. Cette institution devrait veiller à ce que toutes les activités de collecte, de traitement et de partage des données soient conformes aux lois nationales et internationales applicables, favoriser un équilibre entre la vie privée, l'accès et d'autres enjeux, et offrir des voies de recours efficaces en cas de violation des droits concernés.
9. Donner la priorité au stockage des données publiques ouvertes dans des centres de données nationaux ou régionaux afin de promouvoir la souveraineté.
10. Promouvoir l'accès aux données concernant l'étendue des pratiques durables sur le plan environnemental, telles que les sources d'énergie utilisées pour les centres de données et la gestion, le recyclage et l'élimination des déchets électroniques.

11. Prendre des mesures pour garantir l'accès aux données afin d'évaluer si les ensembles de données utilisés pour l'IA et la prise de décision algorithmique sont représentatifs, validés en termes d'exactitude et contrôlés quant à leur partialité, et évaluer la provenance des données et les contraintes d'utilisation.
12. Coopérer au niveau régional et sous-régional africain afin d'élaborer des approches transnationales communes visant à garantir l'accès aux données collectées et détenues par des acteurs transnationaux du secteur privé.

Mesures juridiques, politiques et programmatiques

Afin de s'aligner sur un cadre juridique conforme aux droits de l'homme en matière d'accès aux données, les mesures correspondantes garantiront que :

13. La législation et la réglementation existantes soient interprétées de manière à englober les données :

- a. Les dérogations en matière d'accès à l'information soient expressément comprises comme englobant les « données » et les « ensembles de données » en tant que formes d'information soumises au droit d'accès, avec des dispositions applicables en matière de divulgation proactive, de formats, de refus d'accès, de contrôle et d'application.
- b. Toute disposition contradictoire dans les règles juridiques existantes (par exemple, les lois sur le secret d'État, les lois sur la cybersécurité) susceptible d'avoir un impact inutile sur l'accès aux données puisse être identifiée et traitée.

14. Le droit d'accès aux données soit codifié :

En tant que composante du droit d'accès à l'information garanti par la loi, l'accès aux données devrait être couvert par les principes suivants dans les dispositions juridiques actuelles ou nouvelles :

- a. Toute personne a le droit d'accéder rapidement et à moindre coût aux données détenues par les organismes publics et les organismes privés concernés.
- b. Toute personne a le droit d'accéder, rapidement et à moindre coût, aux données d'autres organismes privés susceptibles de l'aider à exercer ou à protéger un droit quelconque.
- c. Le droit d'accès aux données doit être guidé par les principes de divulgation proactive et de divulgation maximale, limités par des exceptions strictement définies, qui doivent être prévues par la loi et se conformer strictement au droit international des droits de l'homme et aux normes internationales en la matière.
- d. Les mesures juridiques régissant le consentement doivent inclure des droits clairs d'adhésion et de retrait concernant la collecte, le traitement et l'accès, de telle manière que les personnes conservent un contrôle effectif sur leurs données à caractère personnel.
- e. Les données devraient être librement disponibles, faciles à trouver, accessibles, utilisables, partageables et diffusables par quiconque à toutes fins utiles, sans être limitées par des exceptions restrictives.
- f. Les transferts transfrontaliers de données doivent se conformer aux lois nationales sur la protection des données et aux accords internationaux afin de garantir une protection équivalente.
- g. Lorsque l'accès aux données sert un intérêt public supérieur (par exemple, la santé, l'environnement, les élections, les interventions en cas de catastrophe, la lutte contre la violence sexiste), les obligations de divulgation devraient être absolues.
- h. Des dispositions légales sont nécessaires pour prévoir des recours en cas de refus d'accès aux données, par exemple en prévoyant un contrôle administratif par un organisme de surveillance ou un médiateur, ainsi que la possibilité d'un recours judiciaire.

15. Les divulgations d'intérêt public soient protégées :

- a. Nul ne doit faire l'objet de sanctions civiles, pénales, administratives, professionnelles ou autres, ni subir de préjudice, pour avoir divulgué des données relatives à des actes répréhensibles ou révélant une menace grave pour la santé, la sécurité ou l'environnement, ou dont la divulgation est dans l'intérêt public.

16. Il existe une obligation de créer, de conserver, d'organiser et de maintenir les données :

- a. Des dispositions légales sont nécessaires pour exiger que les organismes publics et les organismes privés concernés créent, conservent, organisent et gèrent les données de manière à garantir leur intégrité et à faciliter l'exercice du droit d'accès.
- b. La conservation des données doit respecter les principes de proportionnalité, et les ensembles de données à long terme essentiels aux droits et au développement (par exemple, population, environnement, archives publiques) doivent être conservés au-delà des délais administratifs habituels.
- c. Les organismes publics et privés concernés doivent être tenus de tenir à jour et de publier des catalogues des ensembles de données qu'ils détiennent, en indiquant clairement les métadonnées et les conditions d'utilisation.

17. La valeur publique est au cœur de l'accès aux données :

- a. Pour concrétiser la valeur publique, il est nécessaire d'impliquer de manière inclusive les parties prenantes concernées de l'écosystème des données – y compris les groupes vulnérables, sous-représentés ou marginalisés – lors de la conception, de la mise en œuvre et du suivi des cadres de gouvernance des données, notamment en ce qui concerne les dispositions relatives à l'accès aux données.
- b. La transparence des modalités d'accès et de partage des données est nécessaire pour encourager l'adoption des pratiques responsables de gouvernance des données tout au long du cycle de valeur des données, y compris en ce qui concerne le respect des codes de conduite, des principes éthiques et des réglementations en matière de confidentialité et de protection des données.
- c. Lorsque des données à caractère personnel sont en jeu, il est nécessaire de se conformer aux cadres de protection de la vie privée et des données en ce qui concerne les données à caractère personnel auxquelles on accède et qui sont partagées, y compris avec qui elles sont partagées, à quelles fins et dans quelles conditions l'accès peut être accordé à des tiers.
- d. Il est utile d'encourager et de faciliter des modèles innovants de partage des données, y compris, mais sans s'y limiter, les dons de données et les pools de données, en impliquant notamment des chercheurs, des scientifiques des données et des journalistes.

18. Les marchés des données soient concurrentiels et fonctionnent pour tous :

- a. Des marchés concurrentiels des données nécessitent une politique de concurrence et une réglementation solides, qui traitent de l'exploitation éventuelle d'une position dominante sur le marché et prévoient des mécanismes d'application et de recours renforçant l'autonomie et le contrôle des parties prenantes, afin d'assurer une protection adéquate des consommateurs, des droits de propriété intellectuelle, des intérêts légitimes en matière de sécurité, ainsi que de la vie privée et de la protection des données à caractère personnel.
- b. La gouvernance doit encourager les partenariats de partage de données neutres sur le plan de la concurrence, y compris les partenariats public-privé (PPP), lorsque le partage de données entre les secteurs public et privé peut créer une valeur ajoutée pour la société.
- c. Pour faciliter le partage des données entre les secteurs public et privé, des mesures nécessaires doivent être prises afin d'éviter les conflits d'intérêts, notamment en veillant à ce que :
 - i. Les organismes publics n'accordent pas d'accès exclusif aux données qui porte atteinte à la concurrence loyale, mais traitent tous les acteurs du marché selon des conditions équitables, raisonnables et non discriminatoires, en tenant compte de manière équilibrée des régimes d'accès différencié et de partenariat

afin de répartir la valeur au-delà des entités les mieux dotées en ressources et d'apporter des avantages inclusifs ;

- ii. Les partenariats public-privé et privé-privé n'aboutissent pas à l'appropriation de données publiques à des fins commerciales privées au détriment d'un accès public généralisé.
- d. Les États membres de l'UA peuvent élaborer des Lignes Directrices sectorielles en matière de concurrence pour des marchés de données spécifiques, notamment dans des domaines tels que les plateformes numériques et les intermédiaires en ligne ; la publicité ; les services de télécommunications et de connectivité ; les services financiers et les technologies financières ; les données de santé et les services de santé numériques ; et les données agricoles et les technologies agricoles.

19. Faciliter l'utilisation des données :

- a. Il est nécessaire de favoriser la facilité de recherche, l'accessibilité, l'interopérabilité et la réutilisabilité des données entre les organisations, y compris au sein des secteurs public et privé et entre ceux-ci. Cela nécessite en particulier des efforts pour garantir que :
 - i. les données soient fournies avec toutes les métadonnées, la documentation, les modèles de données et les algorithmes requis, de manière transparente et en temps opportun, et s'appuient sur des mécanismes appropriés de contrôle de l'accès aux données, y compris des interfaces de programmation d'applications (API) ;
 - ii. Le développement et l'adoption de spécifications interopérables pour un accès, un partage et une utilisation efficaces des données, y compris des normes communes pour les formats et les modèles de données ainsi que des implémentations open source et des formats ouverts.
- b. Les cadres de gouvernance des données prévoient des programmes publics visant à sensibiliser aux avantages d'un accès ouvert et interopérable aux données.

20. Des procédures soient en place pour les demandes d'accès aux données :

- a. Lorsque l'accès aux données est soumis à une demande :
 - i. L'accès doit être accordé aussi rapidement que possible, et dans les délais fixés par la législation nationale (ne dépassant pas 30 jours pour les demandes standard, sous réserve d'une prolongation limitée dans des circonstances justifiées).
 - ii. L'accès doit être fourni à moindre coût, les frais étant limités aux coûts marginaux de reproduction et de diffusion, le cas échéant. L'accès aux données générées par les utilisateurs et aux données présentant un intérêt public significatif doit être gratuit.
 - iii. Les données doivent être fournies dans des formats ouverts, interopérables et lisibles par machine, y compris, le cas échéant, dans des formats accessibles aux personnes handicapées.
 - iv. Aucun demandeur ne devrait être tenu de démontrer un intérêt juridique ou personnel spécifique pour les données demandées ni de justifier sa demande, sauf disposition contraire de la loi pour des catégories spécifiques de données sensibles.
 - v. Les demandeurs ont le droit de bénéficier d'une aide pour formuler leurs demandes oralement ou par écrit, une assistance appropriée étant fournie aux personnes analphabètes et aux personnes handicapées afin qu'elles puissent présenter leurs demandes sur un pied d'égalité avec les autres.
 - vi. Tout refus de divulgation de données doit être notifié en temps utile et par écrit, être dûment motivé et se fonder sur le droit international et les normes internationales. Le refus doit préciser l'exception applicable, le préjudice que causerait la divulgation et les considérations d'intérêt public qui ont été prises en compte.
- b. Pour les données mises à disposition par des moyens automatisés, y compris les interfaces de programmation d'applications (API), les portails ou les flux en temps réel, les directives suivantes s'appliquent :
 - i. Les mécanismes d'accès doivent être clairement documentés, accessibles au public et accompagnés d'une assistance technique le cas échéant.

- ii. L'accès ne doit pas être soumis à des obstacles techniques déraisonnables, à un verrouillage propriétaire ou à des conditions discriminatoires injustes.
- iii. Les utilisateurs devraient avoir le droit d'accéder aux données par le biais d'API sans être tenus de justifier la finalité de cet accès, sauf lorsque cela est nécessaire pour prévenir des violations de droits ou protéger la sécurité.
- c. Lorsque les données sont dynamiques ou font l'objet de mises à jour fréquentes (notamment les données de capteurs, les données de surveillance en temps réel ou les données en continu), les mécanismes d'accès doivent permettre une récupération rapide. Les États et les organismes privés concernés doivent veiller à ce que les données dynamiques présentant un intérêt public significatif (par exemple, les données de surveillance environnementale, de santé publique ou d'intervention en cas de catastrophe) soient accessibles en temps réel ou en temps quasi réel lorsque cela est techniquement possible.
- d. Les procédures d'accès devraient établir une distinction entre :
 - i. Ensembles de données complets : lorsque l'accès à des ensembles de données complets est demandé, les procédures devraient faciliter le téléchargement en masse ou l'accès via une API.
 - ii. Les données granulaires ou spécifiques : lorsque l'accès n'est demandé ou accordé que pour des enregistrements de données spécifiques, les procédures devraient permettre une récupération précise sans nécessiter l'accès à l'ensemble du jeu de données.
- e. Les États peuvent mettre en place des procédures de demande standardisées, y compris des portails en ligne et des formulaires électroniques, afin de rationaliser l'accès. Ces procédures ne doivent pas créer d'obstacles indus et doivent prévoir des solutions de rechange pour les personnes ne disposant pas d'un accès à Internet ou de compétences numériques.
- f. Tout refus, retard ou divulgation partielle de données devrait pouvoir faire l'objet d'un recours devant un organe de contrôle indépendant désigné en vertu des présentes lignes directrices (voir annexe C). L'organe de contrôle peut ordonner la divulgation, imposer des délais ou accorder des mesures de réparation.

Exemptions et garanties

21. Exceptions

- a. Les données ne peuvent être légitimement retenues que lorsque le préjudice causé à l'intérêt protégé par l'exemption concernée l'emporte manifestement sur l'intérêt public à la divulgation de l'information. Ces données ne peuvent être retenues que pendant la période au cours de laquelle le préjudice pourrait se produire.
- b. Lorsqu'une partie d'un ensemble de données contenant les données demandées est exemptée de divulgation, la partie exemptée doit être supprimée ou caviardée et l'accès accordé au reste de l'ensemble de données.
- c. Les lois régissant la classification des données doivent fixer la durée maximale de la classification et limiter celle-ci au strict nécessaire, jamais à une durée indéterminée.
- d. En général, les données ne peuvent être légitimement retenues au titre d'une exemption que si leur divulgation :
 - i. entraîner la divulgation injustifiée des informations personnelles d'un tiers ;
 - ii. causer un préjudice substantiel à un intérêt commercial ou financier légitime des parties prenantes concernées ou d'autres tiers ;
 - iii. Mettre en danger la vie, la santé ou la sécurité d'une personne ;
 - iv. causer un préjudice substantiel à la sécurité nationale et à la défense de l'État ;
 - v. porter gravement atteinte aux relations internationales lorsque les données concernent des informations devant rester confidentielles en vertu du droit international, la position de l'État dans le cadre de

- négociations internationales, ainsi que la correspondance diplomatique ou officielle avec des États ou des organisations internationales et des missions diplomatiques ou consulaires ;
 - vi. Porter atteinte à l'application de la loi, en particulier à la prévention et à la détection des infractions, à l'arrestation ou à la poursuite des auteurs d'infractions et à l'administration de la justice ;
 - vii. entraîner la divulgation de communications confidentielles entre un médecin et son patient, un avocat et son client, un journaliste et ses sources, ou de toute autre information protégée par le secret professionnel dans le cadre d'une procédure judiciaire ; ou
 - viii. compromettre l'intégrité d'un examen professionnel ou d'un processus de recrutement.
- e. Exceptions spécifiques aux données : Outre les exceptions susmentionnées, les données peuvent être retenues lorsque :
- i. La divulgation de données anonymisées créerait un risque significatif de réidentification d'individus ou de groupes, et ce risque ne peut être atténué de manière adéquate par des mesures techniques ou organisationnelles.
 - ii. La divulgation d'algorithmes, de code source ou de modèles propriétaires compromettrait de manière substantielle l'intégrité, la sécurité ou le fonctionnement des systèmes algorithmiques, à condition que cette non-divulgation n'empêche pas une responsabilité significative pour les décisions affectant les droits individuels.
 - iii. La divulgation des spécifications techniques, des protocoles d'accès ou des mesures de sécurité créerait un risque substantiel d'accès non autorisé, de manipulation ou de préjudice aux systèmes de traitement des données.
 - iv. La divulgation porterait atteinte aux droits de propriété intellectuelle protégés par le droit national, à condition que ces droits ne soient pas utilisés pour empêcher l'accès légitime à des données d'intérêt public ou pour faire obstacle au droit d'accès aux données générées par les utilisateurs.
- f. Les exemptions énoncées dans les sections ci-dessus doivent être interprétées de manière restrictive. Lorsque l'intérêt public à la divulgation l'emporte sur le préjudice causé à l'intérêt protégé, les données doivent être divulguées.

22. Garanties

Les organismes publics sont tenus de mettre en place des garanties pour l'accès ou la réutilisation des données publiques, selon lesquelles :

- a. L'accès n'est accordé que lorsque l'organisme du secteur public ou l'organisme compétent, à la suite de la demande, s'est assuré que les données ont été anonymisées dans le cas de données à caractère personnel.
- b. Dans le cas d'informations commercialement confidentielles, y compris les secrets d'affaires ou les contenus protégés par la propriété intellectuelle, l'accès peut dépendre de la modification, de l'agrégation ou du traitement des données par d'autres méthodes de contrôle de la divulgation.
- c. Les organismes publics devraient imposer des conditions préservant l'intégrité des données, en se réservant le droit de vérifier le processus, les moyens et les résultats du traitement des données effectué par le réutilisateur, ainsi que le droit de limiter l'utilisation des résultats du traitement qui portent atteinte aux droits et intérêts de l'organisme public ou de tiers, sans pour autant prévaloir sur l'intérêt public.
- d. Conformément à la Convention de l'Union africaine sur la prévention et la lutte contre la corruption, il devrait exister des protections contre les représailles, ainsi que des garanties d'anonymat et d'immunité juridique en ce qui concerne les divulgations de bonne foi par des lanceurs d'alerte signalant des pratiques de gestion des données qui restreignent arbitrairement les droits d'accès aux données.

Garanties pour les acteurs privés :

- a. Les acteurs privés soumis à des obligations d'accès en vertu des présentes lignes directrices doivent, conformément à la législation nationale, garantir les mesures de protection suivantes :
 - i. L'accès aux données à des fins de réutilisation ne doit être accordé que lorsque l'acteur privé s'est assuré que les données à caractère personnel ont été anonymisées, sauf si l'accès est motivé par un intérêt public nécessitant des données à caractère personnel ;
 - ii. Les informations commercialement confidentielles, y compris les secrets d'affaires ou la propriété intellectuelle, doivent être modifiées, agrégées ou traitées par toute autre méthode de contrôle de la divulgation, sauf si la divulgation est requise par un intérêt public supérieur ;
 - iii. Lorsque l'accès est fourni par le biais d'un environnement de traitement sécurisé, l'acteur privé doit préserver l'intégrité et la sécurité de cet environnement et se réserve le droit de vérifier le processus, les moyens et les résultats du traitement effectué par le réutilisateur ;
 - iv. Toute condition imposée à l'accès ou à la réutilisation doit être accessible au public, clairement énoncée et appliquée de manière non discriminatoire.
- b. Les acteurs privés doivent inclure des conditions contractuelles ou autres conditions juridiquement contraignantes interdisant aux réutilisateurs d'utiliser les données consultées à des fins de :
 - i. une surveillance illégale ou une discrimination ;
 - ii. La violation des droits à la vie privée ou à la protection des données ;
 - iii. du harcèlement ;
 - iv. Toute fin qui violerait le droit international relatif aux droits de l'homme.

Application

23. Responsabilité :

L'organisme de contrôle désigné, de préférence la Commission de l'information ou son équivalent (voir annexe C), est chargé de faire respecter les présentes Lignes Directrices, c'est-à-dire de contrôler leur application, d'enquêter sur les violations et d'émettre des directives.

24. Conformité et audits

- a. La surveillance devrait encourager, et peut exiger, que les organismes publics et privés procèdent à des audits réguliers afin de renforcer les pratiques proactives de divulgation des données. Dans le cadre de ce processus, les institutions peuvent être encouragées à publier, au moins une fois par an, une liste des ensembles de données dont elles ont la garde, comprenant des informations sur leur statut d'accessibilité (ouvert, restreint ou confidentiel), ainsi que les justifications de toute restriction.
- b. L'autorité de contrôle doit mener des audits et des inspections réguliers afin de garantir le respect des normes en matière de gestion des données, de divulgation et d'éthique.

25. Sanctions et recours

- 26. Les États devraient adopter des mesures politiques, réglementaires ou administratives pour remédier aux manquements aux obligations de divulgation proactive ou aux demandes de données. Ces mesures devraient porter sur :
 - a. La destruction, l'endommagement, l'altération, la dissimulation ou la falsification délibérés ou par négligence de données, ainsi que l'entrave ou l'ingérence dans l'exercice des fonctions d'un détenteur de données ou d'un mécanisme de contrôle, en reconnaissant ces actes comme des infractions passibles de mesures correctives appropriées et en les érigeant en infractions punissables par la loi.
 - b. Les institutions, les agents et les dirigeants d'institutions qui ont systématiquement manqué à leurs obligations de divulgation proactive ou ont systématiquement entravé la divulgation peuvent être sanctionnés conformément aux cadres réglementaires. Un organisme de contrôle indépendant est habilité à publier des rapports sur les cas de manquement systématique aux obligations de divulgation proactive ou d'entrave systématique à la divulgation, ainsi que sur les sanctions applicables.

27. Les mesures doivent être proportionnées et soumises à un cadre progressif à plusieurs niveaux suivant :
- a. Niveau 1 : Transparence – L'organisme de contrôle indépendant publie un rapport public identifiant la nature et l'étendue de la non-conformité et recommandant des mesures correctives.
 - b. Niveau 2 : Mesures correctives – L'entité se voit accorder un délai raisonnable, d'au moins 90 jours, pour remédier au manquement. L'organisme de contrôle peut fournir une assistance technique pour faciliter la mise en conformité.
 - c. Niveau 3 : Recours civils – Les personnes concernées, les organisations de la société civile et les institutions nationales des droits de l'homme sont habilitées à demander des mesures injonctives, des dommages-intérêts ou des mesures déclaratoires devant une cour ou un tribunal indépendant pour les préjudices résultant de la non-conformité.
 - d. Niveau 4 : Sanctions judiciaires – Lorsque la non-conformité est persistante, flagrante et n'a pas été corrigée après l'épuisement des niveaux 1 à 3, des sanctions proportionnées peuvent être imposées, mais uniquement :
 - i. Sur ordonnance d'un tribunal indépendant et impartial ;
 - ii. À la suite de la constatation d'un non-respect persistant, flagrant et non corrigé ;
 - iii. La sanction étant proportionnée à la nature et à la gravité de la violation.
 - e. Conditions :
 - i. Les autorités administratives n'ont pas le pouvoir d'imposer des sanctions financières, des retraits de licence, des restrictions opérationnelles ou des interdictions d'accès à la plateforme sans autorisation judiciaire indépendante préalable.
 - f. Les mesures de responsabilité prévues au présent article ne peuvent être utilisées à des fins de :
 - i. Une persécution politique;
 - ii. Censurer arbitrairement la liberté d'expression ;
 - iii. Exercer une coercition économique ;
 - iv. Surveiller ou harceler les utilisateurs, les journalistes ou les défenseurs des droits de l'homme.
28. Refus :
- a. Les demandeurs dont la demande de divulgation de données est rejetée doivent recevoir une motivation écrite et pouvoir engager une procédure de réexamen interne, sans frais, dans un délai raisonnable, par exemple entre 30 et 45 jours.
 - b. L'examen de ces recours doit avoir lieu dans un délai maximal de 90 jours et être communiqué dans des formats clairs et accessibles. Les demandeurs conservent le droit de former un recours supplémentaire auprès d'instances judiciaires ou d'autres organismes indépendants, conformément aux procédures nationales.
 - c. Les décisions relatives aux recours et aux réexamens doivent être communiquées dans des formats accessibles, sans frais administratifs.
 - d. Les personnes concernées, les organisations de la société civile et les institutions nationales des droits de l'homme doivent avoir la qualité pour agir afin de former un recours auprès d'instances judiciaires ou d'autres instances indépendantes, par exemple pour obtenir une mesure injonctive, des dommages-intérêts ou une décision déclaratoire devant une cour ou un tribunal indépendant, pour les préjudices résultant d'un manquement.

ACCÈS, ÉTHIQUE ET IA

Les ensembles de données utilisés pour l'IA doivent être exacts, représentatifs et gérés de manière sécurisée, avec des mesures de protection visant à empêcher tout accès non autorisé, toute manipulation ou toute violation. Le public devrait avoir accès aux données relatives au respect de ces normes éthiques.

29. Mesures recommandées :

- a. Les systèmes d'IA utilisés dans la prestation de services publics ou la gouvernance devraient être tenus de présenter des évaluations d'impact sur les droits de l'homme qui englobent les données concernées. Cela est essentiel pour identifier et atténuer les biais liés aux données qui pourraient exacerber les inégalités structurelles et la discrimination ; et le public a le droit d'accéder aux données relatives à ces évaluations.
- b. Les fournisseurs de services d'IA peuvent être tenus de rendre compte de la manière dont ils identifient et atténuent les risques éthiques et liés aux droits avant le déploiement, y compris la manière dont les problèmes de qualité et d'accès aux données peuvent être impliqués dans les biais liés aux données, les biais algorithmiques, l'explicabilité et la responsabilité. Le public a le droit d'accéder aux données contenues dans ces rapports.
- c. Les droits d'accès aux données peuvent être étendus aux acteurs privés, y compris les plateformes numériques, dont l'utilisation de l'intelligence artificielle et des systèmes de prise de décision automatisés est susceptible d'affecter les droits fondamentaux. Pour les plateformes numériques, les évaluations d'impact sur les droits de l'homme requises peuvent inclure des évaluations des données et de l'accès aux données concernant la manière dont la modération des contenus, le classement et les systèmes de recommandation ont un impact sur les droits d'accès à l'information, à la vie privée, à la liberté d'expression et à la non-discrimination. Le public a le droit d'accéder à ces évaluations.
- d. Les parties prenantes, y compris les communautés concernées, devraient être associées à la conception, au déploiement et à l'évaluation des systèmes d'IA afin de garantir leur conformité avec les valeurs et les attentes de la société, notamment en ce qui concerne l'accès aux données ainsi que leur provenance, leur qualité, leur représentativité et leur sécurité.
- e. La coopération régionale et sous-régionale en Afrique favorisera l'application effective de ces normes au niveau national.

MISE EN ŒUVRE

30. La mise en œuvre des présentes Lignes Directrices comprendra plusieurs étapes :

- a. Des mesures législatives, administratives, judiciaires, budgétaires et autres doivent être prises afin de donner effet aux présentes lignes directrices et de faciliter leur diffusion.
- b. Ces Lignes Directrices sont conçues pour être mises en œuvre dans le cadre d'une approche multipartite, garantissant la participation effective des pouvoirs publics, du secteur privé, de la société civile, des médias, du monde universitaire, de la communauté technique et des communautés concernées à la conception, à la mise en œuvre et au suivi des politiques et des pratiques.
- c. Les États peuvent collaborer avec la société civile, les médias, le monde universitaire, le secteur privé et les communautés pour concevoir, mettre en œuvre et surveiller les politiques et pratiques relatives aux données, y compris en matière d'accès aux données. En outre, les États peuvent collaborer activement avec le Rapporteur Spécial sur la liberté d'expression et l'accès à l'information en Afrique au fur et à mesure de leurs avancées, en fournissant des perspectives nationales afin d'illustrer comment les données constituent un puissant moteur pour les droits de l'homme, la transparence, l'inclusion et le développement à travers l'Afrique.
- d. Il est nécessaire de mettre en place des programmes nationaux de culture des données et de compétences numériques afin de permettre au public de comprendre ses droits en matière de données, et de faire en sorte que les régulateurs évaluent les systèmes de recommandation en ligne basés sur les données et de modération des contenus, ainsi que les modèles économiques des plateformes.
- e. Le développement professionnel continu est essentiel pour les fonctionnaires dans les domaines de la gouvernance des données, de l'accès, de la gestion de la qualité et de l'utilisation éthique, afin d'éclairer la prise de décision fondée sur des données factuelles.
- f. Des ressources dédiées et durables sont nécessaires pour améliorer la qualité, l'intégrité et l'exhaustivité des données publiques dans tous les secteurs, car des données de mauvaise qualité constituent un obstacle majeur à la valeur que l'accès public aux données permet de dégager.
- g. Les États peuvent adopter et appliquer périodiquement des indicateurs de performance mesurables pour la mise en œuvre de l'accès aux données dans le cadre des dispositifs de gouvernance des données, élaborés à l'issue d'une consultation publique.
- h. Les cadres d'accès aux données et leur mise en œuvre devraient faire l'objet d'examens périodiques, au moins tous les trois à cinq ans, afin de s'adapter aux évolutions technologiques et aux enseignements tirés de la mise en œuvre. Les conclusions de ces examens devraient être rendues publiques et officiellement communiquées au parlement ou à un organe de contrôle équivalent afin de garantir la transparence et la responsabilité.
- i. Conformément à l'article 62 de la Charte africaine, chaque rapport périodique soumis à la CADHP peut fournir des informations détaillées sur les mesures prises pour faciliter le respect des dispositions des présentes lignes directrices.

Le Rapporteur Spécial encouragera les examens nationaux des cadres d'accès aux données et pourra participer à l'élaboration de nouvelles orientations et à la soumission volontaire de rapports par les États ou les institutions sur les progrès réalisés dans la mise en œuvre de la Résolution 620.

ANNEXE A : MESURES CONCERNANT DES DONNÉES SPÉCIFIQUES

1. Catégories de données sélectionnées :

- a. Les données sensibles doivent être cryptées, leur accès limité, et elles ne doivent être traitées qu'à des fins explicitement autorisées.
- b. L'accès aux données relatives aux enfants doit être conforme à la Convention des Nations Unies relative aux droits de l'enfant et à la nécessité d'une gouvernance des données adaptée aux enfants, y compris des mécanismes de consentement et de protection.
- c. Des garanties doivent être mises en place contre la stigmatisation ou l'utilisation abusive des données relatives aux groupes marginalisés, conformément aux Lignes directrices des Nations Unies sur la désagrégation des données pour les ODD ainsi qu'aux principes de CARE en matière de souveraineté des données autochtones.
- d. Les données ventilées par sexe sont essentielles pour soutenir l'égalité des sexes, conformément à l'ensemble minimal d'indicateurs de genre de l'ONU Femmes.

2. Données budgétaires et fiscales :

- a. Les exigences peuvent prévoir la publication d'ensembles de données lisibles par machine sur les marchés publics, les dépenses fiscales et la dette, conformément aux normes de l'Open Budget Index et de l'International Budget Partnership.

3. Données de recherche issues de financements publics :

- a. Les politiques nationales et les mesures institutionnelles peuvent préciser les régimes d'accès aux données de recherche issues de financements publics conformément aux objectifs et principes suivants :
 - i. Ouverture : trouver un équilibre entre l'intérêt d'un accès libre aux données pour améliorer la qualité et l'efficacité de la recherche et de l'innovation, et la nécessité de restrictions justifiées tenant compte des droits de propriété intellectuelle, de la protection des données à caractère personnel et de la confidentialité, de la sécurité et des intérêts commerciaux légitimes
 - ii. Transparence : mettre à disposition et rendre accessibles des informations claires sur les organismes producteurs de données, la documentation relative aux données qu'ils produisent et les spécifications des conditions liées à l'utilisation de ces données.
 - iii. Responsabilité formelle : promouvoir des règles institutionnelles explicites et formelles concernant les responsabilités des différentes parties impliquées dans les activités liées aux données, notamment en matière de paternité, de crédit des producteurs, de propriété, de restrictions d'utilisation, d'arrangements financiers, de règles éthiques, de conditions de licence et de responsabilité.
 - iv. Conformité juridique : accorder l'attention nécessaire, lors de la conception des régimes d'accès aux données de recherche numériques, aux exigences juridiques nationales en matière de sécurité nationale et de vie privée.
 - v. Protection de la propriété intellectuelle : décrire les moyens d'obtenir un accès libre dans le cadre des différents régimes juridiques du droit d'auteur ou d'autres lois sur la propriété intellectuelle applicables aux bases de données ainsi qu'aux secrets d'affaires.
 - vi. Interopérabilité : accorder l'attention nécessaire aux exigences des normes internationales pertinentes pour une utilisation multiple, en coopération avec les organisations internationales.
 - vii. Qualité et sécurité : promouvoir les bonnes pratiques en matière de méthodes, de techniques et d'outils utilisés pour la collecte, la diffusion et l'archivage accessible des données, afin de permettre le contrôle de la qualité par l'évaluation par les pairs et d'autres moyens visant à garantir l'authenticité, l'originalité, l'intégrité et la sécurité des données, ainsi qu'à établir la responsabilité.
 - viii. Efficacité : améliorer encore la rentabilité au sein du système scientifique africain et mondial en encourageant les bonnes pratiques en matière de gestion des données, d'accès et de services de soutien spécialisés.

- ix. Responsabilité : évaluer les performances des régimes d'accès aux données afin de maximiser le soutien à l'accès libre au sein de la communauté scientifique et de la société dans son ensemble.
- b. Les établissements de recherche doivent élaborer des politiques de gestion des données de recherche. Ces politiques doivent établir des règles et des lignes directrices sur la manière dont les données de recherche doivent être collectées, stockées et partagées, conformément aux meilleures pratiques nationales et internationales en matière de réutilisation à des fins commerciales ou non commerciales, dans la mesure où elles sont financées par des fonds publics, et les rendre accessibles au public par le biais d'un dépôt institutionnel ou thématique permettant l'accès aux données et leur partage.
- c. Tous les établissements universitaires et de recherche, ainsi que toute entité traitant des données universitaires, doivent établir, mettre en œuvre et rendre publics des protocoles clairs pour la conservation, l'anonymisation et la destruction de ces données. Ces protocoles doivent inclure des mesures de protection spécifiques visant à empêcher la réutilisation illicite des travaux soumis par les étudiants et d'autres résultats de recherche.

Données de santé :

- a. Créer un écosystème de santé numérique interopérable qui facilite l'échange sécurisé de données tout en préservant la vie privée des patients. Une approche fondée sur les opportunités et les risques peut servir de base à des procédures d'examen et d'approbation claires ainsi qu'à des processus d'approbation rationalisés impliquant plusieurs organisations.
- b. Il convient de distinguer les données de santé publique agrégées (qui devraient être ouvertes) des données de santé personnelles (qui doivent être protégées), en s'appuyant sur les principes de gouvernance des données de santé de l'Organisation mondiale de la Santé (OMS).
- c. Les mesures suivantes garantiront l'accès aux données de santé en vue de leur réutilisation :
 - i. Apporter des améliorations concrètes en matière de confidentialité et de transparence, car la confiance du public est essentielle pour obtenir les données des patients.
 - ii. Mettre en place un environnement de données centralisé et sécurisé pour normaliser le traitement des données des patients, imposer un stockage et une conservation normalisés d'un catalogue d'ensembles de données couramment utilisés, avec des directives claires sur les entités autorisées à y accéder.
 - iii. Créer une bibliothèque en ligne pour fournir le code de conservation des données, des tests et de la documentation afin de garantir l'accès à des données bien conservées.
 - iv. Élaborer une carte unique détaillant toutes les procédures d'approbation avec l'ensemble des organisations concernées, garantissant la transparence des critères d'approbation, des agences de réglementation chargées de l'approbation et des délais clairs et transparents pour les décisions d'accès.
 - v. Créer une application commune pour les questions d'éthique, les conseils en matière d'information et les autorisations d'accès.

Données environnementales :

- a. Il devrait exister des obligations claires en matière de divulgation proactive des données environnementales, conformes aux cadres continentaux et régionaux tels que le principe 10 de la Déclaration de Rio et la Convention d'Aarhus de la Commission économique des Nations Unies pour l'Europe (CEE-ONU), et alignées sur les instruments nationaux de gouvernance relatifs aux ressources naturelles.
- b. Des exigences doivent être imposées aux autorités publiques et aux entreprises privées, en particulier celles opérant dans les industries extractives et à fort impact, afin qu'elles publient de manière ouverte et exhaustive les données relatives à l'impact environnemental et social. Cette divulgation doit inclure des évaluations de référence, des rapports de suivi et des mesures d'atténuation des risques, garantissant ainsi que les communautés et les parties prenantes aient un accès en temps opportun aux informations qui affectent leurs droits, leurs moyens de subsistance et leur environnement. Conformément à l'Initiative pour la transparence

dans les industries extractives (ITIE), des données ventilées devraient être exigées en fonction de l'impact sur les entreprises, les projets et les communautés.

- c. Il est essentiel de prévoir des dispositions permettant un accès en temps réel ou quasi réel aux données concernant les risques environnementaux (par exemple, la pollution, la déforestation).
- d. L'accès aux données est nécessaire concernant la consommation d'énergie des centres de données pour le stockage et le traitement, ainsi que sur la gestion, le recyclage et l'exposition aux déchets électroniques.

Données privées d'intérêt public :

- a. Pour libérer la valeur des données dans l'ensemble de l'économie, il est nécessaire de prendre des mesures visant à garantir que les données du secteur privé soient disponibles, accessibles et utilisables de manière appropriée à des fins d'intérêt public et dans l'ensemble de l'économie, tout en protégeant les droits relatifs aux données et la propriété intellectuelle du secteur privé.
- b. La gouvernance devrait garantir la disponibilité de normes de données ouvertes et interopérables pour permettre au secteur privé de divulguer de manière proactive des informations, afin de faciliter l'utilisation des données dans l'intérêt public.
- c. Il est nécessaire de sensibiliser les organisations du secteur privé aux avantages sociétaux de la divulgation proactive et du partage des données par le biais d'engagements réguliers avec le secteur privé.
- d. Les États peuvent envisager des mesures incitatives, telles que des programmes de reconnaissance publique, afin d'accroître la divulgation proactive des données du secteur privé et le partage de données par le secteur privé sur une base volontaire.
- e. Des mesures sont nécessaires pour promouvoir la transparence dans toutes les collaborations de partage de données, y compris en ce qui concerne les données utilisées et l'impact de la collaboration.

Orientations sectorielles :

Il est utile de disposer de mécanismes d'autorégulation ou de corégulation – notamment des lignes directrices volontaires, des normes, des codes de conduite et des modèles au niveau sectoriel pour les accords d'accès aux données et de partage de données.

8. Accès aux données détenues par les plateformes numériques dans l'intérêt public :

- a. Les plateformes doivent s'engager à faire preuve d'une plus grande transparence concernant leurs pratiques de collecte de données, leurs processus décisionnels algorithmiques et leurs conditions d'utilisation en matière d'accès aux données.
- b. Les États africains peuvent surmonter leur désavantage en matière de pouvoir face aux plateformes numériques en garantissant une approche panafricaine de la gouvernance des entreprises multinationales qui détiennent des volumes importants de données, y compris une coopération visant à élaborer un code de conduite continental concernant l'accès des parties prenantes aux données dans l'intérêt public.
- c. Ce code de conduite, adapté et régulièrement mis à jour au niveau national par la Commission de l'information (ou son équivalent), peut inclure, sans s'y limiter, les dispositions suivantes :
 - i. Ces plateformes s'engagent à s'abstenir d'intenter, de poursuivre ou de menacer d'intenter une action en justice contre les chercheurs, journalistes et acteurs de la société civile africains qui procèdent à la collecte automatisée (scraping) des données accessibles au public à partir de leurs services à des fins légitimes d'intérêt général, en particulier lorsque la plateforme ne propose aucun autre mécanisme d'accès.
 - ii. Les plateformes doivent être tenues de développer et de fournir activement des mécanismes d'accès robustes, sécurisés, vérifiables et non discriminatoires (par exemple, des API, des accords de partage de données, des environnements sandbox) pour les parties prenantes recherchant des données non accessibles au public ou un accès structuré aux données destinées au public. Ces mécanismes doivent être proposés à un prix raisonnable (le cas échéant) pour les utilisations à but non lucratif et doivent offrir un accès rapide aux données en temps réel.

- iii. Des critères clairs sont définis pour déterminer ce qui constitue une « recherche d'intérêt public légitime », englobant des domaines tels que, sans s'y limiter, les études sur les biais algorithmiques, les atteintes aux droits de l'homme en ligne, la désinformation et/ou les discours de haine, la concurrence sur le marché, les aspects socio-économiques et psychologiques, ainsi que la compréhension scientifique au sens large.
- iv. Ces recherches doivent respecter les directives éthiques, les lois sur la protection des données et les normes d'intégrité académique, journalistique ou professionnelle.
- v. Des mécanismes existent pour vérifier que les demandes de données de bonne foi sont fondées sur des critères d'intérêt public et des normes éthiques, ainsi que pour l'application des décisions, le règlement des litiges et l'examen périodique du respect du présent code de conduite, gérés soit par l'autorité de régulation de l'information (ou son équivalent), l'office national de statistique, soit par un organisme de recherche national (ou son équivalent).

ANNEXE B : MESURES INSTITUTIONNELLES

Divulgaration proactive

1. Les organismes publics devraient être tenus, même en l'absence de demande spécifique, de publier de manière proactive les données d'intérêt public, y compris les informations concernant leurs fonctions, leurs pouvoirs, leur structure, leurs responsables, leurs décisions, leurs budgets, leurs dépenses et toute autre information relative à leurs activités.
2. Lorsque des organismes privés mènent des activités pour le compte d'organismes publics, et pour lesquelles des fonds publics sont utilisés ou des fonctions ou services publics sont exercés, les organismes publics devraient exiger de ces organismes privés qu'ils publient de manière proactive les données issues de ces activités dans l'intérêt public ; ou faciliter la publication de ces données dans l'intérêt public.

Priorisation de la publication des ensembles de données à haute valeur ajoutée

3. Les organismes publics devraient divulguer de manière proactive et gratuitement des « ensembles de données à haute valeur ajoutée » (HVD), dans des formats lisibles par machine et accessibles via des interfaces de programmation d'applications (API).
4. Les catégories thématiques des HVD comprennent notamment les données géospatiales, statistiques, relatives à la propriété des entreprises et météorologiques.

Formats ouverts, interopérables et lisibles par machine

5. Les organismes du secteur public devraient mettre à disposition les documents et les données en vue de leur réutilisation dans des formats ouverts et lisibles par machine. Cette mesure vise à faciliter une réutilisabilité et une interopérabilité sans faille à l'échelle de l'UA.

Transparence sur les conditions de réutilisation

6. Les organismes publics doivent faire preuve de transparence quant aux conditions de réutilisation des données. Cela implique notamment de publier la licence standard ou toute autre licence ouverte et de rendre les informations sur les données disponibles, y compris les métadonnées, facilement accessibles en ligne.

Accès équitable et non discriminatoire

7. Il est interdit aux organismes du secteur public de conclure des accords exclusifs pour la réutilisation des données publiques, sauf dans des circonstances exceptionnelles et très limitées, afin de garantir une concurrence loyale sur le marché des services basés sur les données.

Politiques d'accès aux données

8. Les politiques des organismes publics en matière d'accès aux données doivent couvrir la collecte, le stockage, le partage, la qualité, la conservation, l'élimination et la sécurité, dans le cadre de dispositions plus larges et exhaustives en matière de gestion des données. Afin de protéger les données contre tout accès non autorisé, toute violation ou toute perte, des mesures techniques et organisationnelles solides doivent être mises en place, notamment un stockage sécurisé, le chiffrement et le contrôle d'accès.

Facturation au coût marginal

9. Les données du secteur public devraient être disponibles gratuitement. Dans les cas où des frais sont appliqués, ils se limitent généralement aux coûts marginaux engagés pour la reproduction et la diffusion.

ANNEXE C : ARCHITECTURE INSTITUTIONNELLE POUR L'ACCÈS AUX DONNÉES

Organisme de contrôle indépendant :

Un mécanisme de contrôle indépendant et impartial, idéalement une commission de l'information (ou un organisme hybride ou équivalent) établi par la loi, a pour mandat de surveiller, promouvoir et protéger le droit d'accès à l'information et aux données, ainsi que de résoudre les litiges. Cela implique que :

- a. L'indépendance d'un tel organisme doit être garantie par la loi, qui doit prévoir un processus de nomination transparent et participatif, un mandat clair et précis, une rémunération et des ressources adéquates, ainsi qu'une responsabilité finale devant le pouvoir législatif. La Commission de l'information a besoin d'un capital humain adéquat, c'est-à-dire de personnes possédant des compétences à jour pour utiliser les données, concevoir des politiques et des réglementations.
- b. Les organismes publics et les organismes privés concernés sont tenus de reconnaître les décisions de la Commission de l'information comme juridiquement contraignantes pour toutes les questions relatives à l'accès aux données, y compris le règlement des litiges.
- c. Les pouvoirs de la Commission de l'information comprennent notamment celui de rendre des ordonnances à l'encontre des organismes publics, les obligeant à divulguer des informations, ainsi que la possibilité de prendre des mesures disciplinaires à l'encontre des fonctionnaires qui refusent de s'y conformer.
- d. La Commission de l'information accrédite les intermédiaires de données afin de faciliter le respect des normes en matière de gouvernance et d'accès aux données et de favoriser un marché concurrentiel dans le domaine du courtage de données.
- e. La Commission de l'information veille à ce que les parties prenantes soient tenues de rendre compte, en fonction de leurs rôles, de l'intégrité des données qu'elles mettent à disposition et de la mise en œuvre systématique de mesures de gestion des risques tout au long du cycle de valeur des données, y compris des mesures visant à protéger la sécurité, la confidentialité, la qualité et la disponibilité des données. À cet effet, la Commission de l'information veillera à :
 - i. Promouvoir l'adoption d'analyses d'impact et d'audits, ainsi qu'une gestion responsable de l'accès aux données.
 - ii. Superviser l'adoption de normes de service public (par exemple, délais de réponse, procédures de recours), mettra en place des mécanismes de consultation, instaurera une culture de confiance au sein de la fonction publique et découragera toute aversion excessive au risque en matière de divulgation des données.
 - iii. Clarifier les rôles et les responsabilités des organismes détenteurs de données au sein des institutions publiques, soutenir le renforcement des capacités, l'allocation de ressources et le développement des compétences dans ce domaine, et promouvoir des partenariats pour soutenir ces efforts.

- iv. Inclure dans ses fonctions la promotion de la culture des données auprès du grand public ainsi que dans les programmes de formation de la fonction publique.
- v. Mettre en place un mécanisme de publication régulière de rapports sur l'état de l'ouverture des données et des demandes d'accès, et fournir des rapports de transparence sur son propre fonctionnement en matière de traitement et de promotion de l'accès aux données.

Offices nationaux de statistique :

- a. Le rôle des offices nationaux de statistique (ONS) des États en tant que collecteurs de données devrait être renforcé afin qu'ils puissent jouer le rôle de gestionnaires et de coordinateurs centraux des données dans un cadre national intégré de gestion des données.
- b. L'ONS doit collaborer avec les détenteurs de données, les intermédiaires de données et les organismes publics pour faciliter l'accès aux données et leur partage, en veillant à ce que les ressources de données d'un pays soient utilisées de manière efficace et éthique pour le bien public.
- c. L'ONS doit établir et maintenir des normes pour la collecte, le traitement et la diffusion des données, et collaborer avec la Commission de l'information (ou son équivalent) afin de favoriser le développement des compétences au sein des organismes publics pour la mise en œuvre des normes de données, et contribuer à garantir que les données provenant de différentes sources soient cohérentes, homogènes et interopérables.
- d. Afin d'encourager et de promouvoir l'adoption de normes dans l'ensemble du secteur public, l'ONS doit évaluer et exposer clairement les avantages de l'adoption de normes en matière de données, formuler et mettre en œuvre des processus visant à identifier et à mettre en avant la mise en œuvre des normes, ou des projets pilotes de nouvelles normes afin de démontrer l'intérêt de leur adoption.
- e. Aux fins de la mise en œuvre du Cadre national intégré de gestion des données, l'ONS veille à (soutenir) :
 - i. la confiance entre les parties prenantes afin de préserver les données pour maximiser la valeur publique tout en prévenant les utilisations abusives.
 - ii. le financement d'initiatives en faveur de l'accès aux données et de leur utilisation, y compris le financement des infrastructures et des compétences
 - iii. des incitations adéquates pour que les organismes publics produisent, protègent et partagent des données.
 - iv. des mesures adéquates pour garantir la capacité de demande de données et une culture de l'utilisation des données.

Conseil consultatif national sur les données :

- a. Les États peuvent envisager de créer un Conseil consultatif national sur les données ou tout autre organisme similaire, relevant de la compétence de la Commission de l'information existante ou des régulateurs nationaux chargés des données et de l'information. Le Conseil contribuera à l'élaboration du Cadre national intégré de gestion des données, conseillera le gouvernement national, la Commission de l'information (ou son équivalent), l'Office national de statistique et les institutions nationales de recherche. Il devra assurer un suivi et formuler des recommandations.
- b. Le Conseil sera composé de représentants du gouvernement, de la Commission de l'information (ou de son équivalent), de l'Office national de statistique et de l'organisme national de recherche, ainsi que de parties prenantes non étatiques issues du secteur privé, du monde universitaire, des médias et de la société civile.

Pouvoir judiciaire :

- a. Les autorités judiciaires favorisent la transparence de la justice en facilitant le partage et l'accès aux données grâce à la publication en temps opportun des décisions judiciaires dans des formats ouverts, ainsi qu'à la publication proactive des moyens permettant aux personnes d'accéder à la justice.
- b. Afin de concilier le droit d'accès aux données avec d'autres droits et obligations, les décisions judiciaires relatives à l'accès s'aligneront sur les normes internationales suivantes : (i) l'adéquation (la mesure doit être

adaptée à la réalisation de l'objectif souhaité); (ii) la nécessité (un moyen moins restrictif doit être utilisé s'il est tout aussi efficace); et (iii) la proportionnalité au sens strict (la mesure ne doit pas être excessive par rapport à l'objectif).

Organismes de gestion électorale et données :

- a. Les organismes de gestion électorale (OGE) sont instamment invités à établir et à appliquer un ensemble convenu de principes relatifs aux données susceptibles de contribuer à promouvoir la transparence électorale, et à définir des normes et des attentes claires à l'intention des partis politiques, des candidats et des médias, en ce qui concerne la création, la gestion et l'accès aux données applicables.
- b. Les OGE peuvent élaborer et mettre en œuvre des mesures visant à mettre en avant les données exactes et les sources de données officielles sur les plateformes numériques.
- c. Ces organismes peuvent mettre en place des cadres standardisés pour préserver l'intégrité des données électorales, assurer une diffusion responsable des données et le partage d'informations sur les tendances en matière de désinformation, les contre-mesures efficaces et l'opinion publique.
- d. Il convient de garantir l'existence de canaux de communication efficaces entre les plateformes en ligne et les parties prenantes du processus électoral, et de mettre en place des mesures algorithmiques visant à donner la priorité à l'accès à des données précises sur les élections.
- e. Les OE facilitent l'établissement de relations efficaces avec les organisations de surveillance électorale, la société civile, les chercheurs, les journalistes et les autres parties prenantes du processus électoral ainsi qu'avec les plateformes numériques afin de permettre un accès rapide aux données électorales et des réponses rapides aux menaces pesant sur l'intégrité des données et à la désinformation fondée sur les données.
- f. Il est nécessaire de renforcer les obligations législatives nationales imposées aux plateformes, y compris les plateformes publicitaires, qui sont de grands détenteurs de données, de sorte qu'elles soient légalement tenues de fournir des données sur :
 - i. leurs évaluations d'impact sur les droits de l'homme en matière d'élections ;
 - ii. leurs plans d'atténuation des risques électoraux ;
 - iii. leurs accords de coopération, notamment avec les organes électoraux, les médias, la société civile et les vérificateurs de faits.