Lignes directrices sur la protection des données à caractère personnel pour l'Afrique

Une initiative conjointe de l'Internet Society
et de la Commission de l'Union africaine

9 Mai 2018

Internet Society

African Union

Introduction

En 2014, les membres de l'Union africaine (UA) ont adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (« la Convention »)[1]. Les ministres de l'UA en charge de la communication et des technologies de l'information et de la communication (CICT) et des services postaux ont confirmé leur engagement envers la Convention au sein du Comité technique spécialisé de l'Union africaine sur la communication et la déclaration ministérielle sur les TIC (UA/CCICT-2)[2].

La Déclaration a fixé un objectif important d'action africaine en matière de cybersécurité et de protection des données à caractère personnel pour offrir des avantages à l'Afrique. En particulier, la Commission de l'Union africaine est appelée à élaborer des lignes directrices sur la protection des données à caractère personnel (paragr. 31).

Pour faciliter la mise en œuvre de la Convention, la Commission de l'Union africaine a demandé à l'Internet Society d'élaborer conjointement les Lignes directrices sur la protection de la vie privée et des données à caractère personnel pour l'Afrique (« les Lignes directrices »). Ont contribué à l'élaboration des Lignes directrices des experts régionaux et mondiaux de la protection de la vie privée, y compris des spécialistes de la protection de la vie privée, des universitaires et des groupes de la société civile.

Les Lignes directrices soulignent l'importance d'assurer la confiance dans les services en ligne, en tant que facteur clé du maintien d'une économie numérique productive et bénéfique. Elles offrent également des conseils sur la façon d'aider les particuliers à prendre une partie plus active à la protection de leurs données à caractère personnel, tout en reconnaissant que dans de nombreux domaines, les résultats positifs pour les particuliers dépendent des actions positives des autres parties prenantes.

Les Lignes directrices énoncent 18 recommandations, regroupées sous trois rubriques :

- Deux principes fondamentaux pour créer la confiance, protéger la vie privée et assurer l'utilisation responsable des données à caractère personnel
- Huit recommandations d'action par les parties prenantes suivantes :
    - Gouvernements et décideurs
    - Autorités de protection des données (DPA)
    - Contrôleurs de données et responsables du traitement des données
- Huit recommandations sur les thèmes suivants :
    - Solutions multipartites
    - Bien-être du citoyen numérique
    - Mesures d'habilitation et de soutien

La protection de la vie privée et des données à caractère personnel est un domaine vaste et en constante évolution. Les Lignes directrices ne sont pas une fin en soi. Elles représentent un plan d'action relatif à un processus évolutif d'élaboration d'orientations stratégiques et opérationnelles et de pratiques exemplaires, qui prend en compte les circonstances et les exigences émergentes du moment.

1 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
2 https://au.int/sites/default/files/newsevents/reports/33025-rp-addis_ababa_declaration_of_the_stc-cict-2_en.pdf (Para.31)

Table des matières

Résumé analytique

Cette partie résume les principaux rôles et responsabilités des principaux groupes de parties prenantes, en ce qui concerne la protection des données à caractère personnel.

Gouvernements et décideurs

Rôle : responsabiliser les citoyens numériques et assurer que l'environnement en ligne soit fiable, sûr et bénéfique pour toutes les parties prenantes.

Responsabilités :

- Accroître leur compréhension des avantages et des dangers de l'économie fondée sur les données.
- Comprendre les forces économiques et sociales en œuvre dans l'écosystème des données à caractère personnel.
- Cultiver le cadre social à long terme pour la confiance dans l'économie numérique, en veillant à ce que les bénéfices soient équitablement répartis.

Ce sont les objectifs des principes fondamentaux et les mesures d'habilitation et de soutien.

Autorités de protection des données (DPA)

Rôle : accroître la sécurité juridique, en appliquant les lois sur la protection des données, en enquêtant sur les violations présumées de la vie privée, en imposant des sanctions, le cas échéant, et en travaillant avec les groupes de parties prenantes et d'autres DPA.

Résponsabilités :

- Fournir des conseils d'expert aux gouvernements sur les politiques et les lois relatives à la protection des données.
- Donner des orientations claires aux contrôleurs de données et aux fabricants/développeurs de produits et de services.
- Assurer l'application effective des règlements de protection des données, y compris les enquêtes et les sanctions.
- Fournir des conseils et de l'aide aux personnes concernées.
- Se concerter avec d'autres DPA pour une cohérence des règles de protection des données transfrontalières et une application uniforme.

Les contrôleurs de données et leurs partenaires

Rôle : créer et appliquer des pratiques responsables et durables en matière de traitement des données à caractère personnel, qui prend en compte les intérêts de la personne concernée ainsi que ceux du contrôleur de données et des partenaires.

Responsabilités :

- Maximiser la confiance portée par le citoyen/client/utilisateur, comme un avantage apporté par vos services et produits, et comme un atout économique de votre organisation. La confiance améliore la réputation, renforce le consentement et peut apporter un avantage concurrentiel dans un contexte commercial.
- S'attaquer aux problèmes pratiques de la protection des données à caractère personnel (consentement, périodes de conservation des données, sécurité des données, etc.), avec la bonne combinaison de mesures techniques et procédurales.
- Augmenter la prise en compte du respect de la vie privée dès la conception et renforcer la conception basée sur la valeur[3], en tant que partie intégrante du développement de produits/services.

3 La plupart des processus de conception de produits se concentrent principalement sur des aspects tels que la fonction, la forme, l'esthétique et le coût. La conception basée sur la valeur reconnaît que chaque choix de conception a une dimension éthique et intègre systématiquement des considérations éthiques dans le cycle de conception et de développement.

Citoyens et société civile

Rôle : créer des citoyens numériques efficaces ; devenir des parties prenantes actives de la protection individuelle de la vie privée et des données à caractère personnel.

Responsabilités :

- Comprendre les risques liés à la vie en ligne.
- Comprendre et exercer les droits relatifs aux données à caractère personnel, à la vie privée et à l'autonomie.
- Développer les capacités individuelles à protéger ses intérêts en ligne, que ce soit directement, ou en utilisant des outils et des services qui aident à améliorer la protection de la vie privée individuelle.
- Faire entendre une voix collective (avec les organisations de consommateurs et les organisations de la société civile) pour que le marché des consommateurs assure davantage la protection de la vie privée.

Tâches multipartites

Chaque partie prenante a un rôle à jouer dans la mise en place collective d'un écosystème en ligne fiable, profitable à tous.

La protection de la vie privée consiste à respecter les attentes des particuliers quant à la façon dont leurs informations personnelles sont traitées ; la protection de la vie privée dépend d'une relation de respect, entre les particuliers et les parties prenantes qui collectent et utilisent les données les concernant. La protection de la vie privée en ligne est renforcée lorsque tous ceux qui y ont un intérêt font partie de la solution.

De nombreux problèmes pratiques de protection des données nécessitent une action concentrée de plusieurs parties prenantes ; par exemple,

- Élaboration des meilleures pratiques en matière de codes de conduites (DPA, contrôleurs de données, organismes concernés) ;
- Création et exploitation de programmes de certification pour la protection des données (DPA, organisations de consommateurs, organismes de normalisation et de certification) ; et
- Consentement de l'utilisateur et respect de la vie privée (DPA, contrôleurs de données, organismes de consommateurs).[4]

Ce sont les actions recommandées sous la rubrique « Solutions multipartites ».

4 La protection de la confidentialité consiste souvent à respecter le contexte dans lequel l'information est divulguée et non à la partager ou à la réutiliser dans d'autres contextes (par exemple, ne pas prendre de données médicales privées et les publier dans un journal).

Remerciements

Nous prenons acte des précieuses contributions de Robin Wilton (Internet Society) qui a travaillé sur la première version des Lignes directrices et a révisé les versions successives en tenant compte des contributions des experts. Nous aimerions également remercier, pour leur contribution, toutes les personnes qui ont participé au colloque d'experts pour identifier, ont examiné les principaux thèmes des présentes Lignes directrices et les ont commentés sur le projet de document :

Souhila Amazouz (Commission de l'UA)
Yaovi Atohoun (ICANN)
Dawit Bekele (ISOC)
Alebachew Berhanu (Bahir Dar University)
Betel Hailu (ISOC)
Verengai Mabika (ISOC)
Evelyn Namara (ISOC)
Marsema Tariku (ISOC)
Wakabi Wairagala (CIPESA)
Auguste Yankey (Commission de l'UA)
Moctar Yedaly (Commission de l'UA)
Kinfe Yilma (Université de Melbourne)

Ont également apporté leurs contributions et/ou ont participé à la révision des différentes versions successives :

Jacques Bus (Digital Enlightenment Forum)
Jemal Hussien (Commission de l'UA)
Olaf Kolkman (ISOC)
Eve Maler (Forgerock Inc.)
Christine Runnegar (ISOC)
Colin Wallis (Kantara Initiative)
Pat Walshe (Privacy Matters Ltd.)
Sally Wentworth (ISOC)

Internet Society, avril 2018
Réf. Document : AUC-PDPG-Apr2018

Le contexte africain

Les présentes Lignes directrices prennent en compte les caractéristiques du contexte africain, telles qu'identifiées par le groupe d'experts :

- Diversité culturelle et juridique significative à travers le continent, avec différentes attentes en matière de respect de la vie privée.
- Différences d'accès aux technologies et aux services en ligne, entre les États membres.
- Sensibilités en ce qui concerne le profilage ethnique et le profilage sans consentement des citoyens, dans le contexte d'un État-nation.
- Disparité en termes de capacité dans des domaines tels que les technologies, le droit et la gouvernance liés à la technologie.
- Risques liés à une forte dépendance vis-à-vis des fabricants et prestataires de services non africains :
    - La capacité limitée des États membres de l'Union africaine à influencer le comportement des prestataires de services externes.
    - Risque potentiellement accru d'utilisation abusive des données lorsque le contenu et les services sont uniquement fournis par des sociétés étrangères (tels que les services « over the top » ou OTT) et, par conséquent, plus grande difficulté dans l'application des lois locales de protection des données.

Ces facteurs peuvent accroître la difficulté de formuler et d'appliquer des politiques cohérentes entre les États membres et parfois même à l'intérieur de ceux-ci.

Le contexte politique

Comme l'illustrent la Convention de l'Union africaine sur la cybersécurité et la protection des données (2014) et la Déclaration ministérielle d'Addis-Abeba (AU/CCICT-2, 2017), les Lignes directrices ont été élaborées dans le contexte de changements rapides de l'étendue et de la disponibilité des services en ligne en Afrique, et dans le cadre des objectifs politiques ambitieux de l'Agenda 2063 pour l'Afrique.

L'UA a consacré un intérêt politique considérable à l'harmonisation. Par exemple, l'Acte consultatif de l'Union africaine[5] (Article 3, Page 6) fait explicitement référence à la coordination et à l'harmonisation des politiques entre les Communautés économiques régionales existantes et futures, en appui, entre autres, aux objectifs suivants :

- Une Afrique unie et forte
- Une intégration politique et socio-économique accélérée du continent
- Mise en place des conditions permettant à l'Afrique de jouer son rôle légitime dans l'économie mondiale
- Développement durable au niveau économique, social, et culturel.

La Commission de l'UA établit également « l'Initiative de politique et de régulation pour l'Afrique numérique » (PRIDA), qui rendra possible l'examen des outils et des méthodologies permettant d'harmoniser et de coordonner les politiques et la réglementation.

Dans le cadre de l'objectif d'une plus grande intégration régionale, la Vingt-septième session ordinaire de la Conférence de l'Union (juillet 2016, Kigali, Rwanda) a décidé de mettre en œuvre un protocole pour la libre circulation des personnes sur tout le continent.

5 https://au.int/sites/default/files/pages/32020-file-constitutiveact_en.pdf

- Cette résolution a des implications dans l'échange transfrontalier standardisé, sûr et confidentiel des données d'identité des citoyens et l'échange transfrontalier des données à caractère personnel d'un citoyen qui travaille, réside ou effectue des transactions en dehors de son pays d'origine. La même séance a reconnu l'importance de la libre circulation des biens et des services en tant qu'élément profond d'intégration et d'unité continentales.
- Le principe de la libre circulation des personnes est également dans l'article 43 du Traité instituant la Communauté économique africaine (1991, Abuja, Nigeria).

L'UA a également pris des mesures importantes pour établir une zone de libre-échange continentale (ZLEC) en appui aux principes de la libre circulation des personnes, biens et services, comme en témoignent les Décisions, Déclarations, et Résolutions de sa Vingtième-cinquième session ordinaire (juin 2015, Johannesburg, Afrique du Sud). Cela a des implications pour le transfert transfrontalier correspondant de données à caractère personnel, dans le contexte de transactions en ligne (commerce), et de particuliers vivant et travaillant dans des États membres autres que leur pays d'origine.

Les États membres de l'UA ont également des obligations relatives aux libertés fondamentales et aux droits de l'homme, tel qu'elles sont énoncées dans les déclarations et les conventions de l'UA et des Nations Unies. Cela inclut l'engagement de respecter, protéger et promouvoir le droit à la vie privée et à la protection des données à caractère personnel. Dans un certain nombre de cas, le droit à la vie privée est déjà établi dans les constitutions des États membres (par exemple, Afrique du Sud, Botswana, République Démocratique du Congo, Égypte, Ghana, Kenya, Nigeria, Sierra Leone, Tanzanie, Ouganda, Zambie, et Zimbabwe reconnaissent le droit à la vie privée dans leurs constitutions nationales en tant que droit de l'homme fondamental).

Toutes ces politiques et obligations ont des implications en termes d'échange de données à caractère personnel qui soit sûr, transparent, robuste et confidentiel à travers les frontières et entre les juridictions. Ceci, par voie de conséquence, fait obligation aux États membres de l'UA de veiller à ce que les progrès vers l'intégration régionale, le libre-échange et le développement ne soient pas entravés ou soient plus risqués par l'impossibilité d'échanger des données à caractère personnel en toute sécurité et de manière sûre, fiable et avec le respect approprié des droits des particuliers.

Parallèlement, l'utilisation sûre, robuste et confidentielle des données à caractère personnel facilite les États membres de l'UA à faire ce qui suit :

- Maintenir leur propre autodétermination dans la société de l'information et se tenir au courant des changements rapides
- Tirer profit des innovations technologiques
- Créer et maintenir la confiance dans une économie axée sur les données

Pour maintenir la confiance dans l'économie fondée sur les données, les membres de l'UA doivent reconnaître le rôle joué par les données à caractère personnel et les forces économiques qu'elles génèrent. En cas de succès, l'économie fondée sur les données peut générer une croissance économique, fournir des services attractifs et innovants et améliorer la qualité de vie.

Cependant, l'économie fondée sur les données peut également avoir un côté sombre quand les données à caractère personnel sont exploitées de manière abusive et contre les intérêts de la personne concernée. Les coûts et risques inhérents à ces situations n'apparaissent parfois que lorsque les choses tournent mal, en cas de piratage des données ou de fraude. Cela peut avoir un effet profond sur la confiance dans les services en ligne et des répercussions aussi profondes sur l'économie fondée sur les données. Les Lignes directrices recommandent des mesures pour réduire le risque que présentent les résultats indésirables susmentionnés.

Le groupe d'experts était conscient que, pour certains États membres et décideurs politiques de l'UA, la protection des données à caractère personnel peut être un domaine relativement peu familier, ce qui peut constituer un obstacle à l'élaboration de politiques efficaces. Les Lignes directrices visent à aider les États membres à élaborer des politiques et des lois sur la protection des données à caractère personnel. Les recommandations sont donc accompagnées d'un certain nombre de mesures d'habilitation et de soutien, comme des programmes ciblés de sensibilisation et d'éducation à l'intention des décideurs et des particuliers.

Enfin, il y a un risque d'impacts considérables (sur leurs citoyens et leurs économies) si les États membres de l'UA ne font rien. En conséquence, les Lignes directrices proposent des actions visant à atténuer ce risque.

Vers une cohérence aux principes de protection de la vie privée qu'on retrouve dans d'autres régions

Principes dégagés par la Convention de Malabo

L'article 13 de la Convention dégage les six principes suivants relatifs à la protection des données :

- Consentement et légitimité
- Traitement loyal et équitable
- Objectif, pertinence et conservation des données
- Exactitude des données pendant leurs durées de vie
- Transparence du traitement
- Confidentialité et sécurité des données à caractère personnel

Ensembles de principes similaires provenant d'autres sources

Un certain nombre de cadres nationaux et internationaux de protection de la vie privée ont largement contribué à établir un ensemble de principes fondamentaux de protection des données de base. Ces principes sont mis en œuvre dans le cadre national de protection de la vie privée dans plus de 100 pays. Les trois textes les plus importants sont sans doute les Lignes directrices de l'Organisation de coopération et de développement économique (OCDE) sur la protection de la vie privée (non contraignantes et modifiées en 2013), la Convention 108 du Conseil de l'Europe qui a force obligatoire pour ses 51 signataires[6] et le Cadre de la coopération économique des pays du Pacifique (APEC) relatif à la protection de la vie privée, mis à jour en 2015. Ces documents expriment des principes similaires de protection de la vie privée et sont largement reconnus comme fournissant une base solide pour les politiques et les pratiques de protection de la vie privée en ligne.

À quelques variations mineures près, ils constituent la base des Lignes directrices adoptées par l'Assemblée générale des Nations Unies et le Commonwealth des Nations et sont largement alignés sur le Règlement général de l'Union européenne sur la protection des données de 2016.

Les domaines d'action des principes de protection de la vie privée susmentionnés sont les suivants :

- **Limitation de la collecte de données.** Les données à caractère personnel doivent être obtenues et traitées loyalement, équitablement, et dans la mesure du possible, de manière transparente.
- **Qualité des données.** Les données à caractère personnel doivent être exactes au moment de la collecte, et des mesures raisonnables doivent être prises pour s'assurer que leur exactitude est maintenue pendant la période de conservation.
- **Spécification de l'objectif.** Les données à caractère personnel doivent être collectées uniquement à des fins précises, explicites et légitimes. Les données à caractère personnel ne doivent être utilisées qu'à d'autres fins compatibles avec les lois applicables, telles que l'archivage de données d'intérêt public ou la recherche scientifique.
- **Limitation de l'utilisation.** Les données à caractère personnel ne doivent pas être divulguées, mises à disposition ou utilisées à d'autres fins, sauf avec le consentement de la personne concernée ou si la loi l'autorise.
- **Garanties de sécurité.** Les données à caractère personnel doivent être protégées par des mesures de sécurité raisonnables afin de préserver leur intégrité et leur confidentialité.
- **Ouverture.** Il devrait y avoir une politique générale d'ouverture sur les développements, les pratiques et les politiques en matière de données à caractère personnel.

6 À la date de publication des présentes lignes directrices.

- **Participation individuelle.** Les particuliers doivent avoir le droit d'obtenir des informations sur leurs données à caractère personnel détenues par des tiers. Les données doivent être fournies dans un délai raisonnable, sous une forme facilement lisible et à un coût non excessif. Les personnes concernées ont le droit de contester leurs données et de les faire modifier si elles sont inexactes, ou les supprimer si cela est inapproprié.
- **Sens de la responsabilité.** Les personnes responsables de la collecte et du traitement des données à caractère personnel doivent être en mesure de prouver qu'elles sont conformes à ces principes.

L'alignement sur les six principes énoncés à l'article 13 de la Convention n'est pas exact, mais il y a des nombreux points communs. Les deux points de divergence sont les suivants :

- L'article 13 de la Convention de Malabo considère le « consentement » comme un principe distinct, alors que dans les cadres de l'OCDE et du Conseil de l'Europe, le consentement est pris en compte comme critère de traitement loyal.
- Les articles 7 et 10 de la Convention 108 de la Convention de l'Europe, le Principe 14 des Lignes directrices de l'OCDE sur la protection de la vie privée et le paragraphe 32 du Cadre de l'APEC relatif à la protection de la vie privée expriment des exigences relatives à la responsabilité du contrôleur de données. La responsabilité n'est pas explicite dans les principes de la Convention de Malabo (Article 13) ni dans les Obligations du contrôleur de données à caractère personnel (Articles 20-30). Cependant, les articles 16 à 19 impliquent une responsabilité du contrôleur de données lorsqu'ils présentent certains droits de la personne concernée (exactitude des données, correction, suppression, etc.).

Ces variations sont relativement mineures, et elles ne devraient pas faire oublier le fait qu'il y a beaucoup plus de points communs et d'alignements que de divergences. Néanmoins, nous suggérons que les États membres de l'UA accordent une attention particulière aux mécanismes de responsabilité pour les contrôleurs de données dans les cadres respectifs de protection des données, de sorte que ce sujet important ne soit pas négligé.

Cadres régionaux et nationaux existants en Afrique

Le centre de collaboration CIPESA a mené des recherches sur ces lignes directrices et a identifié les cadres africains qui rappellent les principes de protection de la vie privée et de protection des données similaires à ceux énumérés ci-avant :

- Loi type de la SADC pour la protection des données (2010)
- Acte additionnel de la CEDEAO A/SA.1/01/10 relatif à la protection des données à caractère personnel (2010)
- Cadre de la CAE pour la cyberlégislation (2008)

Selon les mêmes travaux de recherche, les pays suivants ont une législation actuelle ou proposée (au moment de la rédaction des présentes Lignes directrices) qui intègre des principes similaires concernant les droits des personnes concernées et l'établissement d'une autorité de protection des données : Angola (2016), Guinée équatoriale (2016), Mauritanie (2017), Afrique du Sud (2013), Burkina Faso (2004), Mali (2013), Gabon (2011), Bénin (2009), Ghana (2012), Côte d'Ivoire (2013), Lesotho (2012), Madagascar (2014), Maroc (2009), Sénégal (2008), Tunisie (2004), Zimbabwe (2003). Les lois sur la protection de la vie privée et la protection des données du Kenya, Niger, Nigéria, Tanzanie, et Ouganda contiennent également des dispositions similaires.

Thèmes par groupe de parties prenantes

Cette partie des Lignes directrices fait état des sujets et des questions soulevés au cours du processus de consultation et du colloque d'experts.

Ils sont regroupés par type de parties prenantes, et au sein de chaque section de parties prenantes, les thèmes sont classés en fonction des articles correspondants de la Convention. L'objectif de cette partie est de fournir le contexte et les informations de base relatifs aux Recommandations présentées dans la partie suivante.

Gouvernements et décideurs

Thème	Observations
Flux transfrontaliers des données et cadres	Une réglementation à la mesure de celles d'autres juridictions concourt à la confiance mutuelle et jette les bases d'un échange fiable de données, y compris (mais sans y limiter) les données à caractère personnel. La protection des données à caractère personnel est donc un facteur d'amélioration de la confiance au niveau de la circulation des personnes, des biens et des services.
Harmonisation (Convention de Malabo, Préambule, Paragr. 20)	Le préambule de la Convention mentionne l'opportunité d'une cyberlégislation harmonisée. Sur le même principe, les mesures permettant d'améliorer la cohérence entre les États membres de l'UA en matière de législation sur la protection des données aideront à réduire ou à atténuer l'asymétrie dans la protection de la vie privée. Les stratégies, les politiques et les lois de protection des données à caractère personnel devraient viser à intégrer les domaines suivants : • Sensibilisation accrue aux obligations et aux droits en matière de protection des données à caractère personnel • Objectifs politiques et cadres • Les lois et les autorités de protection des données ; application des lois et sanctions Les États membres de l'UA devront collaborer pour parvenir à une telle cohérence. L'Initiative PRIDA de la Commission de l'UA devrait être un catalyseur important de ces efforts.
Droits des citoyens et prérogatives de l'état (Convention de Malabo, Préambule et art. 8)	La Convention réaffirme l'engagement des États membres de l'UA de respecter les libertés fondamentales et les droits de l'homme, ainsi que la Charte africaine des droits de l'homme et des peuples. Un principe important est de faire en sorte que les particuliers jouissent les mêmes droits tant en ligne que hors ligne. De plus, la Convention se réfère également aux prérogatives de l'État, par lesquelles il est compris que le droit à la vie privée est un droit qualifié qui peut être légitimement dérogé dans certain cas dans l'intérêt de la sécurité nationale, du maintien de l'ordre et de la sécurité publique. Cela pose un défi de gouvernance quant : • à la définition des conditions cohérentes et réalisables sous lesquelles de telles exceptions à la loi relative à la protection des données peuvent être autorisées ; • Mise en place d'un régime de surveillance solide et fiable pour surveiller le recours aux exceptions, en particulier dans des situations où la sécurité nationale est menacée et l'accès aux informations sur la gouvernance peut être limité (pour des raisons compréhensibles).

Asymétrie et réciprocité entre les niveaux de protection fournis par les États membres de l'UA et entre les membres de l'Union africaine et d'autres entités (Convention de Malabo, Art. 10.6.k)	Il est probable que des asymétries existent au niveau de la protection des données fournie par les États membres de l'UA, mais leurs effets peuvent être atténués et/ou réduits en accordant une attention appropriée à la gouvernance, aux mesures réglementaires et d'application, et aux facteurs économiques. L'article 10.6.k de la Convention mentionne des arrangements de réciprocité pour les transferts de données à l'extérieur de l'UA. La réciprocité est un facteur clé pour réduire l'asymétrie dans la protection des données à caractère personnel. Les critères cohérents d'adéquation (entre les États membres) pour le traitement des données à caractère personnel sont un mécanisme important pour assurer la réciprocité pratique dans les mesures juridiques et d'exécution. (Cependant, ce n'est qu'une approche. Dans la région des pays d'Asie-Pacifique, par exemple, plutôt que de prendre des décisions adéquates comme base pour les transferts transfrontaliers, l'APEC a développé un mécanisme volontaire basé sur la responsabilité, connu sous le nom de système de règles transfrontalières de protection de la vie privée de l'APEC (système CBRP) et le système de reconnaissance du droit à la vie privée pour les responsables du traitement des données (système PRP).

Contrôleurs de données

Thème	**Observations**
Rôles et obligations	Le comportement des contrôleurs de données est motivé par divers facteurs (tels que la rentabilité, l'efficacité, les avantages sociaux ou communautaires) qui souvent dépendent du secteur d'activités (secteur commercial, public ou à but non lucratif) où le contrôleur de données opère. Leur comportement sera également limité, en principe, par la loi applicable, mais seulement si cette loi est effectivement appliquée. Dans ce contexte, la loi ne peut généralement définir qu'un seuil minimum pour un comportement acceptable du contrôleur de données. Une protection réellement efficace de la vie privée exigera probablement que les contrôleurs des données dépassent le seuil légal et adoptent les meilleures pratiques de traitement des données, telles que la participation à un système de certification pour la protection des données à caractère personnel. Cela pourrait être considéré comme une disposition de protection des données équivalente à l'alinéa de l'article 32 de la Convention qui exige l'adoption de codes de conduite harmonisés dans le domaine de la cybersécurité.
Relation entre les contrôleurs de données et les responsables du traitement des données	En ce qui concerne les données à caractère personnel : • Le contrôleur de données est chargé de déterminer les finalités et la manière dont les données à caractère personnel sont, ou doivent être, traitées. • Le responsable du traitement de données désigne toute personne (autre qu'un employé assurant le contrôle du traitement des données) qui assure le traitement des données au nom du contrôleur de données. En règle générale, le contrôleur de données ne perd aucune de ses responsabilités lorsqu'il transmet les données à caractère personnel à un responsable du traitement des données pour qu'il traite en son nom. Le responsable du traitement des données « hérite » également les responsabilités du contrôleur de données en ce qui concerne la protection des données qui lui sont transmises, et la protection de la vie privée de la personne concernée. Cependant, par exemple, le responsable du traitement de données n'est pas en charge de la réponse à apporter aux demandes d'accès aux données (SAR) relatives aux données à caractère personnel qui lui sont transmises : le responsable du traitement des données peut légitimement renvoyer une telle demande au contrôleur de données. (Les SAR seront présentées plus en détail ci-après, du point de vue du contrôleur de données et de l'autorité de protection de données).

Consentement (Article 13, Principe 1)	L'obtention d'un consentement pour le traitement des données à caractère personnel présente des défis éthiques, juridiques et pratiques. Une législation bien intentionnée peut donner aux contrôleurs de données une mesure incitative à effet pervers qui au final sape la confiance au lieu de la renforcer. Par exemple, l'Union européenne a introduit une « loi relative aux cookies » destinée à empêcher les sites Web de pister les utilisateurs à leur insu ou sans leur consentement, en utilisant des éléments d'information identifiables (cookies) stockés dans le navigateur de l'utilisateur. Certains sites Web ont réagi en présentant une option de consentement « à prendre ou à laisser » qui ne laisse pas de véritables choix aux utilisateurs. Ils respectent certainement la lettre de la loi, mais ils refusent d'appliquer l'esprit de la loi. Dans l'ensemble, ces utilisateurs n'ont pas eu de meilleurs retours en termes de protection de la vie privée. Pour résoudre le problème du consentement, il faudra certainement faire appel à une combinaison de mesures juridiques et de mesures techniques, et dans certains cas, des mesures dissuasives à l'encontre des puissants prestataires de services pour contrer les mesures incitatives économiques qui les poussent à « contourner » la loi. Les lois sur la protection des données à caractère personnel devraient être élaborées au moyen d'un processus qui concilie les exigences posées sur le plan juridique et les possibilités techniques tout en assurant l'intérêt supérieur de la personne à qui on demande le consentement. Dans certaines réglementations sur la protection des données, telles que la Convention 108 du Conseil de l'Europe, l'obligation de consentement est davantage limitée (par exemple, il est exigé que le consentement soit informé, spécifique, révocable, etc.), chacune de ces conditions a des implications qui peuvent exiger l'adoption de mesures juridiques, techniques et procédurales par le contrôleur de données. Ce problème, en grande partie, ne trouve pas encore de solutions définitives, et les États membres sont encouragés à faire des recherches multidisciplinaires pour arriver à de meilleures façons de l'aborder.
Flux de données à caractère personnel entre les contextes, et son impact sur la vie privée (Art. 13, Principe 2 - Licéité du traitement)	L'intégrité contextuelle est importante.[7] La collecte de données à caractère personnel dans un contexte, puis l'utilisation ultérieure dans un autre contexte sans la connaissance et le consentement de l'individu viole la vie privée de l'individu (par exemple, une situation où les données à caractère personnel partagées par un utilisateur pour compléter une transaction sont vendues à un annonceur à l'insu de l'utilisateur). Cette notion d'intégrité contextuelle implique que le contrôleur de données doit être conscient du contexte dans lequel les données ont été recueillies et doit respecter l'intégrité de ce contexte. Ceci est lié au principe de « finalité de la collecte » relatif au respect de la vie privée. Comme il existe souvent des incitations puissantes pour que les contrôleurs de données transfèrent des données d'un contexte à un autre (par exemple, prendre les données transactionnelles des clients et les vendre pour pouvoir les utiliser dans la publicité ciblée), les politiques de protection des données doivent veiller à ce que cela ne soit jamais fait au détriment de la personne concernée ou que la personne concernée ait la possibilité d'exprimer et d'appliquer ses préférences quant à savoir si, quand et comment cela devrait se produire. Le transfert de données entre différents contextes est surtout un problème lorsque les utilisateurs ignorent ce qui se passe. Par exemple, un enfant qui reçoit un ours en peluche « connecté » ne comprend pas que l'ours relie le contexte privé de « la maison » avec un contexte commercial d'une tierce partie. Les utilisateurs de l'application de fitness Strava semblent ne pas savoir que l'appareil récupère les données de localisation d'un contexte (comme une base militaire active) et le rend public dans un autre contexte (carte consultable en ligne). Étant donné que les utilisateurs n'exercent aucun contrôle sur l'utilisation ultérieure des données qu'ils divulguent, une part importante de la responsabilité en ce qui concerne l'utilisation appropriée des données incombe au contrôleur de données. Les gouvernements devraient encourager une culture de conception éthique et fondée sur des valeurs[8]. Ils devraient également veiller à ce que les prestataires de services soient informés des choix de conception intégrant les principes relatifs au respect de la vie privée et d'autres principes éthiques dans les produits et services qui traitent des données à caractère personnel.
Demandes d'accès aux données formulées par les personnes concernées (Convention de Malabo, Article 16 à 19), et leur relation avec la responsabilité et la transparence	La plupart des lois actuelles sur la protection des données intègrent également un principe de responsabilité, par exemple les Lignes directrices de l'OCDE sur la protection de la vie privée. Les principes directeurs de l'OCDE citent également la transparence comme principal élément de responsabilité. Pour les contrôleurs de données, cela implique, entre autres, une obligation de répondre aux demandes de la personne concernée sur les données stockées à son sujet. Ceci implique en retour que les décideurs politiques s'assurent que les demandes d'accès des personnes concernées soient traitées dans un cadre juridique qui garantit qu'elles sont gérées dans l'intérêt légitime de la personne concernée, et n'imposent pas d'obstacles à la personne concernée ni de charges excessives sur le contrôleur de données.

7 « Privacy As Contextual Integrity » (Helen Nissenbaum, Washington Law Review, 2004)
8 Voir, par exemple, « Ethical IT Innovation » (Sarah Spiekermann, 2016)

La confidentialité du traitement des données et les mesures appropriées pour sécuriser les données (Articles 20 à 21, et Article 15 concernant la connectivité)	La Convention oblige les contrôleurs de données à prendre des mesures appropriées pour protéger les données à caractère personnel, en garantissant leur confidentialité et leur intégrité. Les « mesures appropriées » comprennent un certain nombre d'options techniques, procédurales et physiques. Par exemple, les documents papier rangés dans un classeur sont protégés par une forme de contrôle d'accès ; les documents numériques ont une autre forme de protection avec des moyens d'authentification et d'autorisation fortes[9] ; les fichiers cryptés offrent une autre forme de protection, etc. Les contrôleurs de données doivent être encouragés à appliquer les meilleures pratiques reconnues par l'industrie pour la sécurité des données. À cet égard, de nombreux pays ont adopté une approche fondée sur les risques. Ces pays évaluent les mesures jugées appropriées en termes de risque, de probabilité et d'impact potentiel de non-protection des données à caractère personnel en question. Les trois facteurs « classiques » de la sécurité sont tous pertinents dans ce contexte : la confidentialité, l'intégrité et la disponibilité. Les données doivent être protégées contre les divulgations non souhaitées, les modifications non souhaitées et les destructions/inaccessibilités non souhaitées. Les États membres devraient consulter les Lignes directrices sur la cybersécurité portant sur ces sujets. Toujours dans le domaine de la cybersécurité, les contrôleurs de données et, le cas échéant, les autorités de protection des données devraient rechercher des mécanismes de sécurité fiables (algorithme, longueur de clé et discipline de gestion clé) aux niveaux national et international. Les exemples de sources de conseil sur ces sujets provenant d'autres régions sont : • ENISA (Agence de l'Union européenne pour la sécurité des réseaux et de l'information) • NIST (Institut national des normes et de la technologie, États-Unis, mais largement mentionné par d'autres pays) • CESG (Lignes directrices spécifiques au Royaume-Uni, par exemple l'industrie britannique s'en réfère) Ces indications aideront les autorités nationales à évaluer, par exemple, la période pendant laquelle une forme particulière de cryptage pourrait être considérée comme un mécanisme de protection fiable aux fins des articles 20 à 21. De même, lorsque des techniques de pseudonymisation et/ou d'anonymisation sont utilisées pour protéger des données à caractère personnel contre une divulgation ou un usage non souhaité, leur efficacité doit être surveillée à la lumière des progrès réalisés dans les techniques de « ré-identification » de données prétendument anonymisées ou pseudonymisées. En plus de la ré-identification, deux autres menaces au respect de la vie privée devraient être considérées dans ce contexte : les inférences et les recoupements de données. • L'inférence fait référence à la possibilité de prendre des données non personnelles et les utiliser pour établir des hypothèses ou des prédictions personnelles, ou de prendre des données à caractère personnel et les utiliser pour établir des données à caractère personnel sensibles sur une personne. En d'autres termes, les données qui peuvent sembler être à caractère personnel peuvent en fait l'être, ou peuvent être utilisées pour déduire des données à caractère personnel. De même, les données à caractère personnel « normales » pourraient être le point de départ pour établir des données à caractère personnel sensibles. Les États membres doivent revoir leur législation en matière de protection des données afin de vérifier que les personnes physiques ou les groupes sont protégés contre le ciblage ou la discrimination qui découle de l'utilisation de ces données dérivées ou inférées. • Le recoupement des données fait référence à la capacité des contrôleurs de données ou des tiers à établir des données à caractère personnel à partir de différentes sources qui concernent le même individu. Par exemple, les relevés d'appel pour ce numéro de téléphone et les messages publiés sur un certain site de médias sociaux sont associés à la même personne. Ce type de couplage de données peut sérieusement porter atteinte à la vie privée et à l'autonomie de l'individu, en l'empêchant de mener une vie discrète en ligne. Ce sont des domaines où il est difficile de légiférer avec succès, en particulier lorsque les technologies relatives à l'inférence (intelligence artificielle, prise de décision algorithmique et apprentissage automatique) évoluent si rapidement et qu'il est si facile d'extraire des données pour les types de liaison décrite ci-avant. En conséquence, nous recommandons une approche multipartite du problème et une recherche de solution basées sur la capacité à combiner des mesures réglementaires, procédurales, techniques et éducatives selon les besoins. Une approche basée sur les risques est susceptible de donner des résultats meilleurs.

9 L'authentification est le processus qui consiste à valider l'identité d'une personne lorsqu'elle tente d'accéder à un service ou une ressource. L'autorisation est le processus permettant d'établir le droit d'accès d'un utilisateur authentifié au service ou à la ressource en question. Le contrôle d'accès est le processus d'application de ce droit.

Période de conservation (Convention de Malabo, Art. 22)	La plupart des lois actuelles sur la protection des données intègrent le principe de la limitation de la conservation des données. Cependant, peu de contrôleurs de données mettent ce principe en pratique, et par conséquent beaucoup de données sont conservées plus longtemps que nécessaires (parfois indéfiniment), ce qui expose les contrôleurs de données à un plus grand risque de violation des données à caractère personnel et peut également mener à une violation de la vie privée des personnes concernées. Le régime de réglementation et de surveillance ne devrait pas être fondé sur l'hypothèse que les données seront supprimées par défaut, il devrait inclure des mesures pour encourager la réduction et la suppression des données, et assurer le respect de ce principe.
Durabilité de l'accès aux données (Convention de Malabo, Art. 23)	Le contrôleur de données est tenu, en vertu de la Convention, de veiller à ce que les données à caractère personnel restent techniquement accessibles. Sur le plan de la vie privée, cela aura une incidence sur la capacité du contrôleur de données à respecter les diverses exigences des articles 16 à 19 de la Convention (droit à l'information, d'accès, de rectification, de suppression, etc.) Il peut également être un facteur dans le respect des demandes d'accès des personnes concernées (Article 17) : L'article 17 ne parviendra pas à servir les intérêts de la personne concernée si les contrôleurs de données répondent aux demandes d'accès des personnes concernées dans un format ou d'une manière que la personne concernée ne peut pas utiliser.

Autorités de protection des données

Thème	Observations
Éléments d'un régime de gouvernance (Article 10 à 12)	Lorsque les parties prenantes ont un rôle statutaire en vertu des lois de protection de la vie privée et des données à caractère personnel, le respect des exigences statutaires doit être soumis à la surveillance et à l'application de la loi ; ceci est directement lié au principe de la responsabilité relatif à la protection des données. Lorsque les parties prenantes ont des obligations contractuelles ou nominatives, il doit être possible de vérifier leur conformité, ce qui implique la présence d'évaluateurs et de vérificateurs compétents et qualifiés. Ces entités devraient donc être ajoutées à la liste des parties prenantes, comme suit : • Personnes concernées, • Différentes catégories de contrôleurs de données (fournisseur d'identité, fournisseur d'attribut, prestataire de service), • Autorités de protection des données, • Évaluateurs de conformité, • Auditeurs de conformité, et • Organismes d'accréditation pour les évaluateurs et les auditeurs. Cela implique également que les autorités de protection des données ont le pouvoir d'enquêter sur les processus d'accréditation, d'évaluation et de vérification, et de sanctionner les échecs. Un tel régime peut constituer la base d'un système de certification, pour normaliser et mettre en œuvre les principes de protection des données. Un système de certification pourrait également couvrir des fonctions connexes dans les domaines de la sécurité de l'information, qui sont vitales pour établir ce qui constitue des « mesures appropriées » au titre des articles 20 et 21 (et pertinente pour les articles 15 et 23). La mise en place par chaque État membre d'un système de certification pour ces disciplines permettrait d'élaborer des règlements et des lignes directrices pour : • Services de confidentialité, d'intégrité et de disponibilité pour le traitement des données. • Évaluation et sélection des algorithmes cryptographiques, des longueurs de clé et des procédures de gestion importantes. • Évaluation des forces relatives des différents mécanismes d'authentification. • Protection des données à caractère personnel grâce à l'anonymisation et à la pseudonymisation. • Critères d'évaluation des risques pour la ré-identification des données anonymisées/pseudonymisées. • Critère d'évaluation des risques relatifs aux données d'inférence et de recoupement. La certification peut ensuite constituer la base de l'attribution d'une marque de confiance aux parties prenantes qui répondent aux critères spécifiés, ce qui, à son tour, peut aider à informer et à guider les particuliers sur les décisions de confiance qu'ils font en ligne.

Rôle et indépendance des DPA (Article 11)	Une autorité de protection des données (DPA) peut ne pas atteindre son objectif si elle peut être soumise à des pressions politiques, administratives ou commerciales indues. Par exemple, si son personnel est soumis à des nominations ou licenciements arbitraires, s'il ne dispose pas des pouvoirs d'exécution ou des ressources appropriés, ou s'il est soumis au lobbying commercial ou à des contentieux vexatoires.
Décisions d'adéquation (Article 12.2.k)	Les DPA efficaces sont un élément clé pour assurer que les transferts de données transfrontaliers se fassent dans un cadre de confiance mutuelle et de normes cohérentes (voir aussi les observations ci-après, dans la partie Gouvernement et décideurs, en ce qui concerne la réciprocité).
Droit des personnes concernées (Article 13, 16-19)	Les DPA auront un rôle clé à jouer pour clarifier, communiquer, surveiller et appliquer les droits des personnes concernées, comme indiqué dans plusieurs articles/dispositions de la Convention. Article 18 : le droit d'opposition au traitement. Les DPA seront tenues en partie responsables pour avoir accepté une demande d'opposition sur des motifs légitimes et assumeront des responsabilités importantes lorsqu'il s'agit de déterminer quand il est pratique et raisonnable d'exercer ce droit (par exemple, à quel moment peut-on supposer qu'une personne concernée a implicitement accepté le traitement de ses données, et dans quelles circonstances une demande explicite de consentement est demandée ?). Article 19 : le droit de rectification/suppression. Les DPA peuvent être tenues de donner des conseils, par exemple, sur les circonstances dans lesquelles les données à caractère personnel peuvent ou doivent être supprimées à la demande de la personne concernée, même si les données en question sont vraies et précises. Par exemple, à quel moment une personne concernée peut-elle demander à ce que les données à caractère personnel soient supprimées au motif que le contrôleur de données n'a plus besoin de les conserver ? Dans le cas où se produirait sur ce point un désaccord entre la personne concernée et le contrôleur de données, qui pourrait résoudre ce différend ? Le droit à la suppression devrait être distingué du droit à la désindexation (parfois appelé de manière trompeuse « le droit à l'oubli »[10]). Désindexer le contenu Web, dans le contexte de la vie privée, est un moyen de rendre certaines données moins facilement accessibles en ligne. La loi EU[11] été utilisée pour obliger le moteur de recherche à supprimer les résultats de certaines recherches indexées sur le nom de la personne concernée. Cela n'empêche pas la publication d'informations sur le Web, ni ne garantit que l'information ne peut pas être trouvée. Entre autres, la loi additionnelle du CEDEAO sur la protection des données[12] contient des dispositions générales qui pourraient être utilisées pour introduire un droit similaire.

10 « Hiding In Plain Sight » (Garstka, Erdos, University of Cambridge 2017) donne une explication complète de la désindexation par opposition au « droit à l'oubli » : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043870

11 The « Google v Spain » Judgment, 2014 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

12 Acte additionnel A/SA. 1/01/10 sur la protection des données à caractère personnel dans la CEDEAO (2010)

Citoyens et société civile (article 8.1, 8.2)

Thème	Observations
Droits et responsabilités correspondantes d'apprendre et de s'informer	La majeure partie de la responsabilité pratique pour protéger la vie privée peut être considérée comme relevant des contrôleurs de données et des autorités de protection des données. Cela reflète l'asymétrie inhérente dans la relation entre la personne concernée et les sociétés, et les organismes du secteur public qui traitent ses données. Les personnes concernées ont très peu de capacité pratique ou technique à protéger leurs données à caractère personnel une fois que leurs données ont été collectées. Cependant, les individus sont aussi des parties prenantes, et pas seulement en tant qu'acteurs qui subissent ou en tant que propriétaire des données à caractère personnel qui font l'objet de traitement. Les individus ne pourront pas exercer les droits qu'ils ne connaissent pas, et les consommateurs ne peuvent pas influencer le marché par leur comportement s'ils ne sont pas suffisamment informés des choix de consommation qu'ils font. Les individus doivent être habilités à être des citoyens/consommateurs numériques informés et connaître, par exemple, l'affaire qu'ils concluent lorsqu'ils s'inscrivent pour des services « gratuits », ou participent à des plateformes de médias sociaux qui monétisent leurs données. En outre, les citoyens ont des attentes légitimes sur la possibilité d'exercer leurs activités en ligne en toute sécurité. Les législateurs et les autorités de contrôle ont donc le devoir de veiller à ce que les citoyens ne soient pas exposés à des risques indus par l'utilisation des TIC et l'économie numérique. Les asymétries de pouvoir et d'information peuvent représenter un obstacle important à cet égard, car ils peuvent : • Empêcher le comportement du consommateur à exercer une influence sur le marché. • Masquer les effets des modèles commerciaux exploiteurs ou prédateurs. • Diminuer la confiance dans le commerce électronique et d'autres services en ligne. • Empêcher l'Afrique de tirer parti des avantages de la transformation numérique. Les mêmes types d'asymétrie peuvent également saper la confiance dans la relation entre le citoyen et les services publics. Quand de telles érosions de confiance deviennent systématiques, que ce soit dans les secteurs commerciaux ou publics, les avantages escomptés de l'économie numérique ne peuvent pas être réalisés. Les labels de confiance et les certifications décrits ci-avant, dans la partie « Éléments d'un régime de gouvernance » participent considérablement à la création et au maintien de la relation de confiance entre les particuliers et les services en ligne.
Conseils indépendants et renforcement des capacités	Les particuliers ont besoin d'aide et d'encouragement dans leurs efforts pour être mieux informés sur la protection des données à caractère personnel et sa pertinence pour le respect de la vie privée. La société civile a un rôle à jouer pour assurer que la recherche, l'analyse, les rapports et les activités de plaidoyer soient disponibles, et que les particuliers soient motivés à apprendre ce qu'est la vie privée en ligne et à la protéger.
Représenter les intérêts des parties prenantes	Les organisations de la société civile (OSC) et la communauté universitaire ont un rôle important à jouer, dans le contexte africain, pour aider à garantir que les efforts de protection de la vie privée et des données ne sont pas entravés par la taille et la diversité du continent. À cet égard, nous encourageons les organisations de la société civile à se réunir aux niveaux national et régional, en tirant parti des groupements régionaux existants au sein de l'UA. D'autres groupements peuvent également être utiles pour défendre plus efficacement les intérêts de certains groupes de parties prenantes tels que les femmes et les enfants, les personnes handicapées, les personnes particulièrement exposées à la cyberintimidation, etc.

Plaidoyer indépendant	Les OSC peuvent fournir un service précieux en fournissant des évaluations indépendantes de l'état actuel des lois sur la protection de la vie privée et des données, y compris des analyses comparatives avec d'autres États membres et d'autres régions/continents. Ils peuvent également contribuer aux processus établis tels que le Mécanisme universel d'examen par les pairs organisé par les Nations Unies. Pour que la société civile joue efficacement son rôle, les gouvernements doivent également faire leur part pour que les OSC disposent d'un environnement de travail sûr et constructif, avec une protection appropriée contre le harcèlement et l'ingérence.

Recommandations

Fondations : Respect de la vie privée, confiance et utilisation responsable

Respect de la vie privée comme la base de la confiance dans l'environnement numérique

Recommandation : Nous encourageons les États membres de l'UA à prendre des actions politiques pour la ratification et l'application des dispositions de la Convention de Malabo et à déclarer de manière explicite que la protection de la vie privée et des données à caractère personnel en ligne est non seulement un droit fondamental, mais aussi un processus vital à long terme visant à cultiver et maintenir la confiance dans l'utilisation des TIC, condition préalable au développement continu de la société de l'information en Afrique. Ceci est particulièrement important en ce qui concerne les facteurs sociaux tels que l'ethnicité, la vulnérabilité, le handicap et le désavantage.

Utilisation durable et responsable des données à caractère personnel dans l'économie guidée par les données

Recommandation : Les gouvernements et les autorités de la protection des données devraient surveiller l'économie guidée par les données en ce qui concerne les pratiques potentiellement dommageables en matière de données à caractère personnel, comme les suivantes :

- Les pratiques de collecte et de monétisation des données qui faussent le marché et entraînent un manque de choix du consommateur.
- Les pratiques d'utilisation des données qui génèrent des risques non maîtrisés (par exemple, une petite entreprise qui accumule beaucoup plus de données que ce dont elle est capable de gérer par manque de ressources ou de compétences) ou une grande entreprise qui regroupe des quantités massives de données pour en faire une cible unique et irrésistible.
- Des modèles commerciaux prédateurs ou exploiteurs qui manquent de transparence et de responsabilité en ce qui concerne la collecte et l'utilisation des données à caractère personnel.

Dans la mesure du possible, les gouvernements et les autorités de protection de données devraient agir pour corriger les pratiques telles que celles décrites, tout en tenant dûment compte des avantages, des innovations durables, de la concurrence et des modèles commerciaux. L'application efficace des mesures préventives exigera probablement un ensemble de principes et de règles définis d'un commun accord pour régir les transferts transfrontaliers de données à caractère personnel.

Parties prenantes : Gouvernements et décideurs

Une plus grande cohérence dans la protection des données à caractère personnel en Afrique

Recommandation :

- Développer une approche cohérente en matière de : politique et loi sur la protection des données à caractère personnel ; la création d'autorités de régulation ; et des mesures d'exécutions (tel que décrit ci-après dans la partie AUTORITÉS DE PROTECTION DES DONNÉES).
- Élaborer des critères communs et cohérents pour évaluer l'adéquation du niveau de protection des données à caractère personnel afin de permettre les transferts transfrontaliers au sein de l'UA.

Ce sont des facteurs importants qui permettent d'assurer la réciprocité entre les États membres :

- Les termes et conditions dans lesquels les contrôleurs de données opèrent.
- Les droits et conditions dont jouissent les particuliers en ce qui concerne la collecte et l'utilisation des données à caractère personnel.
- Les mesures d'exécution et les recours juridiques disponibles pour les personnes concernées.

Les États membres devraient également accorder une attention particulière à l'Initiative PRIDA de la Commission de l'UA à mesure qu'elle évolue, en veillant à ce qu'ils soient bien placés pour tirer parti des opportunités de travail collaboratif pour harmoniser les politiques et réglementations dans ce domaine. [MC - Préambule, page 3 et article 10.6]

Respect de la vie privée en ligne et hors ligne

Recommandation : Les États membres doivent respecter et protéger les droits des particuliers à la vie privée en ligne et hors ligne. Ils doivent réviser leurs lois, procédures et pratiques, y compris ceux qui ont trait à la surveillance ou à l'interception des communications, afin d'assurer le respect effectif de ces obligations.

Exceptions aux lois sur la protection des données et de la vie privée

Recommandation : Les États membres ne doivent admettre des exceptions à l'application des lois sur la vie privée et la protection des données à caractère personnel que pour des questions de souveraineté nationale, de sécurité nationale ou de sécurité publique, lorsque ces exceptions répondent à un but légitime, sont nécessaires, proportionnées et non arbitraires. Les membres doivent s'assurer que tous les pouvoirs qui sont exemptés de l'application des lois relatives à la vie privée et à la protection des données à caractère personnel sont soumis à un régime de contrôle judiciaire robuste, fiable et indépendant qui assure la transparence et la responsabilité. [MC - Préambule page 2 et 3]

Parties prenantes : Contrôleurs de données et responsables du traitement des données

Demandes d'accès des personnes concernées (SAR) - Perspective du contrôleur de données

Recommandation : Les responsables du traitement des données doivent être tenus de répondre aux demandes d'accès des personnes concernées d'une manière ou dans un format permettant à la personne concernée de le traiter. Sinon, l'article 17 risque de ne pas servir les intérêts de la personne concernée.

Contribuer aux solutions multipartites

Recommandation : Lorsque les problèmes de protection des données nécessitent des solutions multipartites ou coordonnées, les contrôleurs de données doivent jouer leur rôle dans le processus de définition des problèmes, de consensus sur les options disponibles et de mise en œuvre des solutions. Cela s'applique particulièrement aux domaines décrits plus en détail dans la section ci-après, sur les solutions multipartites :

- Meilleures pratiques, codes de conduite et certification,
- Consentement,
- Respect de l'intégrité contextuelle,
- Réponses aux SAR,
- Confidentialité et intégrité des données à caractère personnel, et
- Période de conservation.

Les contrôleurs de données doivent accorder une attention particulière aux progrès dans les meilleures pratiques, telles que le respect de la vie privée dès la conception et le respect de la vie privée par défaut. Ce sont, entre autres, des facteurs importants pour déterminer quand ne pas collecter ou conserver des données.

Les décisions de collecte, de traitement ou de conservation des données découlent généralement d'une série d'autres choix de conception et de mise en œuvre qui ont été faits tout au long du processus de développement du produit. Les contrôleurs de données doivent tirer parti de la quantité croissante de conseils sur la conception de systèmes éthiques ou de systèmes basés sur des valeurs afin d'intégrer depuis les premières étapes de la conception du produit les principes qui renforcent le respect de la vie privée. Cela permet de réduire les coûts ultérieurs de conformité aux exigences de protection des données, et améliore la confiance des utilisateurs.

Parties prenantes : Autorités de protection des données

Rôle et indépendance des autorités de protection des données

Une autorité nationale de protection des données (DPA) indépendante est un élément essentiel du cadre juridique et institutionnel pour construire la confiance en ligne, comme l'envisage la Convention de Malabo (Article 10 à 12).

Recommandations : Le poste de Commissaire de la DPA doit être pourvu par nomination, avec une durée de mandat limitée et sous la supervision d'un conseil consultatif représentant les parties prenantes, notamment les représentants des citoyens (société civile), les consommateurs (organisations de consommateurs), les contrôleurs des données commerciales (chambres de commerce), communauté universitaire et gouvernement, et si possible, les opérateurs de systèmes de certification de la protection des données à caractère personnel (voir la Recommandation 9 ci-après).

Les États membres doivent établir une DPA indépendante pour s'assurer que leurs lois nationales sur la protection de la vie privée et des données à caractère personnel soient respectées. La DPA doit avoir un mandat clair, des pouvoirs et des ressources nécessaires pour pouvoir :

- Surveiller et imposer la conformité aux lois applicables en matière de protection de la vie privée et des données.
- Faciliter l'élaboration de code de conduite volontaire pour l'industrie.
- Recevoir et traiter les réclamations, pétitions et plaintes concernant le traitement des données à caractère personnel, et informer les requérants des résultats.
- Imposer des sanctions et des recours en cas de violation de la loi.
- Fournir une interprétation, et si nécessaire, des décisions administratives faisant autorité sur l'application des lois.
- Évaluer l'adéquation de la protection pour les transferts des données transfrontalières.
- Collaborer et échanger des informations, des conseils et des meilleures pratiques avec les DPA homologues.
- S'engager avec d'autres parties prenantes (telles que le gouvernement, les contrôleurs de données, la société civile) pour élaborer des orientations réglementaires, des cadres de confiance et des mesures habilitantes telles que l'éducation des parties prenantes.
- Informer les personnes et les contrôleurs de données de leurs droits et obligations.
- Élaborer des propositions pour améliorer le cadre législatif et réglementaire du traitement des données à caractère personnel.

Dans l'intérêt de la confiance et de la transparence, les États membres doivent encourager ou exiger que les autorités chargées de la protection de la vie privée et des données à caractère personnel fassent rapport publiquement de leurs activités, le cas échéant.

Demandes d'accès des personnes concernées (SAR) - Perspective de la DPA

Recommandation : Les États membres doivent veiller à ce que les autorités de protection des données disposent des pouvoirs appropriés en matière de demandes d'accès, afin de compléter les obligations décrites à l'article 12(2) de la Convention.

- Si les personnes concernées ont le droit de demander des copies de donnée à caractère personnel à un contrôleur de données, les autorités de la protection des données (DPA) doivent être en mesure de contrôler les résultats de la législation correspondante. Les DPA doivent être habilitées à veiller à ce que les réponses aux SAR servent les intérêts légitimes de la personne concernée, n'imposent pas d'obstacles à la personne concernée (frais excessifs, procédures lourdes, etc.) et n'entraînent pas de charges excessives sur le contrôleur de données.

Thème : Solutions multipartites

Cette section donne des recommandations dans plusieurs domaines où les résultats positifs dépendront de l'effort coordonné entre les parties.

Meilleures pratiques, codes de conduite et systèmes de certification

Recommandations :

- En vue de la réalisation des objectifs multipartites décrits dans cette partie, les États membres doivent convoquer des forums multipartites, avec les autorités de protection des données, les contrôleurs de données et d'autres parties prenantes, pour compléter les bases juridiques par des codes de conduite volontaires mettant en œuvre les meilleures pratiques en matière de protection de la vie privée et des données à caractère personnel.
- Les gouvernements, les industries et les associations de consommateurs doivent envisager la création de systèmes de certification pour certifier qu'un produit ou un service répond à des critères spécifiques de protection des données. Par exemple, la certification peut constituer un signal indiquant qu'un contrôleur de données a été audité par rapport aux critères des meilleures pratiques telles que le respect de la vie privée dès la conception, la sécurité des données ou la transparence de ses termes et conditions.

Création d'un comité de protection des données à caractère personnel à l'échelle de l'Afrique

Recommandation : Créer un comité panafricain axé spécifiquement sur la protection de la vie privée et des données à caractère personnel, faciliter la coordination et le partage d'informations entre parties prenantes, aider à identifier les domaines où les ressources sont nécessaires et conseiller les décideurs politiques africains sur les stratégies régionales et le renforcement des capacités.

Le Comité est un réseau d'expert évolutif, compact et fiable créé par la Commission de l'UA en collaboration avec la communauté Internet africaine. Le leadership du Comité doit être multipartite. Il s'appuie sur l'expertise d'organisations africaines et nationales, et d'institutions telles que les communautés économiques régionales (CER). Il comprend des DPA, des entreprises, des représentants du milieu universitaire, de la communauté technique et de la société civile. En se structurant comme un réseau flexible et multipartite, le Comité s'assure de relever les défis émergents et futurs en matière de la protection de la vie privée auxquels l'Afrique est confrontée.

Le Comité pourrait être chargé de conseiller et de soutenir la AUC dans ces activités de protection de confidentialité en :

- Conseillant la Commission de l'UA sur les questions et politiques de protection de la vie privée et des données à caractère personnel, telles que les initiatives de renforcement des capacités ;
- Étant le référentiel à long terme des meilleures pratiques en matière de protection de la vie privée et des données à caractère personnel ;
- Identifiant les domaines de recherche nécessaires à la formulation de politiques et de directives générales ou sectorielles, à mesure que de nouvelles circonstances et exigences émergent ;
- Identifiant des moyens de soutenir les DPA pour renforcer les capacités et partager les informations au niveau régional et au sein de l'Union africaine ;
- Organisant un forum de parties prenantes de confiance pour une divulgation responsable et coordonnée des violations de données ;
- Proposant des moyens de renforcer les compétences des professionnels de la protection de la vie privée en Afrique (par exemple, dans le cadre d'un programme de certification) ; et
- Aidant la Commission de l'UA à élaborer des stratégies de coopération transfrontalière en matière de respect de la vie privée et de renforcement des capacités.

Le travail du Comité doit être coordonné avec le Comité technique spécialisé de la communication et des technologies de l'information et de la communication (CICT) de l'UA, sous les auspices de la Commission de l'UA. Les détails concernant son nom, sa mission, sa vision, ses objectifs et ses activités détaillées peuvent être élaborés par la Commission de l'UA en collaboration avec la communauté Internet africaine.

En particulier, nous présentons ces recommandations comme un moyen de renforcer la confiance grâce à un système de certification pour la protection des données à caractère personnel sur la base des concepts décrits ci-avant, dans la partie « Éléments de régime de

gouvernance ». Ce Comité peut avoir pour objectif concret la création d'un cadre de confiance pour mettre en place un tel régime de gouvernance. Le cadre définit le rôle des évaluateurs de la conformité, des auditeurs de la conformité et des organismes d'accréditation. À leur tour, ces organismes sont chargés de codifier les critères correspondant à chaque rôle dans le régime de gouvernance.

- En ce qui concerne les contrôleurs de données et les autorités de protection des données, une grande partie de la codification sera déjà dans la législation applicable.
- En ce qui concerne les organismes d'accréditation, ou des orientations concernant les mécanismes de sécurité de l'information, il peut être nécessaire d'identifier ou de développer les critères d'évaluation pertinents.
- En ce qui concerne les domaines de la sécurité de l'information, les États membres doivent rechercher des sources d'orientation, au niveau national, régional et international si nécessaire.

Consentement

Recommandations :

- Les autorités chargées de la protection des données devraient collaborer avec les responsables du traitement des données (par exemple, par le biais des organismes concernés) pour une approche collaborative et multipartite du problème de consentement afin de trouver un équilibre entre les mesures techniques (telles que les reçus de consentement), les mesures réglementaires (telles que les avis relatifs aux cookies) et les mesures de conception de produits (telles que l'expérience utilisateur et les contrôles).
- Lorsque le consentement est juridiquement qualifié (par exemple, des contraintes judiciaires spécifiant que le consentement doit être informé, spécifique, donné librement, révocable, etc.), les autorités de protection des données doivent convoquer un groupe multipartite avec des prestataires de services, des avocats, des représentants de la société civile, des concepteurs et des universitaires pour décider si les exigences juridiques sont mieux satisfaites par des mesures techniques, par des mesures réglementaires ou par des mesures axées sur l'utilisateur ou par une combinaison de ces mesures.

Objectif de la collecte

Recommandations :

- Les autorités chargées de la protection des données doivent disposer des pouvoirs et des ressources nécessaires pour faire respecter le principe de la vie privée sur « les fins de la collecte » tel que prévu à l'article 13 de la Convention. Cependant, la mise en œuvre efficace du principe nécessite une solution collaborative et donc une approche multipartite. Cette approche multipartite peut et doit s'appuyer sur les principes établis de la vie privée dès la conception et de la vie privée par défaut, notamment dans des domaines tels que l'équité des décisions de conception, la minimisation des données et le respect de l'intégrité contextuelle.
- Les gouvernements doivent veiller à ce que les autorités de la protection des données disposent des ressources nécessaires pour surveiller et faire appliquer le principe de « l'objectif de collecte ». Les autorités chargées de la protection des données devraient donner des orientations aux fournisseurs et aux prestataires de services sur la nécessité de la transparence et de la responsabilité en ce qui concerne ce principe, en tant que fondement de la confiance des consommateurs. Si nécessaire, une législation de protection des consommateurs doit être adoptée pour renforcer les droits de la personne concernée dans l'environnement numérique.

Période de conservation des données

Recommandations :

- Les autorités chargées de la protection des données devraient collaborer avec les responsables du traitement des données (par exemple, par l'intermédiaire des organismes concernés) pour convenir de la mise en pratique du principe des périodes de conservation. Cela nécessite probablement une combinaison de mesures techniques (telles que la définition de métadonnées pour enregistrer la date de la collecte des données à caractère personnel et la date de suppression) et des mesures réglementaires, telles qu'un audit de la pratique des contrôleurs de données. [MC - Article 22]
- Pour effectuer de telles activités d'audit, l'organisme doit être doté des ressources et des capacités nécessaires. La Convention appelle à ce que ce soit l'autorité de protection des données. Les gouvernements doivent décider, dans le contexte de l'État-nation, si ces audits sont effectués sur une base statutaire, avec une approche fondée sur la gestion des risques ou dans le respect de codes de conduites applicables dans des secteurs spécifiques réglementés (comme les soins de santé, les services financiers, etc.). [MC - Article 12(2)(g)] [MC - Article 17]

Thème : Bien-être du citoyen numérique

Les attentes des citoyens et le devoir de diligence des gouvernements

Recommandations :

- Comme indiqué ci-après, dans la partie « Citoyen et société civile », les particuliers renoncent le contrôle d'une grande partie de leurs données à caractère personnel une fois qu'elles ont été divulguées. Les contrôleurs de données sont donc les principaux responsables de la mise en place de bonnes pratiques et de la protection de la vie privée.
- Cependant, les citoyens doivent tirer parti de l'Internet et d'autres sources d'orientation pour s'assurer qu'ils sont correctement informés des risques et des avantages de leurs activités dans l'économie numérique et l'environnement connecté, que ce soit à la maison, au travail ou dans les espaces publics.
- Les gouvernements ont un autre rôle, direct ou indirect, qui est d'habiliter les particuliers à exercer leur droit à la vie privée en aidant les citoyens à être informés et éduqués sur la manière d'exercer leur droit en vertu de la loi sur la protection des données à caractère personnel.
- Les autorités de surveillance et les gouvernements doivent prendre des mesures pour s'assurer que les prestataires de services et les fournisseurs de produit en ligne sont suffisamment transparents quant à leurs modèles commerciaux et leurs capacités de produits, que les particuliers sont à même de faire des choix informés par rapport aux implications relatives à la vie privée des produits et services qui leur sont offerts.

Organisation de la société civile (OSC)

Recommandations :

- Les États membres doivent reconnaître et soutenir le rôle des OSC en :
  - Développant des recherches informatives, des analyses, des rapports, des tutoriels et du matériel de plaidoyer sur la protection de la vie privée et des données à caractère personnel pour aider les citoyens à comprendre et à exercer leurs droits ;
  - Recherchant les caractéristiques relatives à la vie privée et à la sécurité des données des applications et services en ligne pour identifier les bonnes et les mauvaises pratiques ; et
  - Produisant des examens indépendants, objectifs et factuels de « l'état de la protection de la vie privée et des donnés », en tant qu'un outil de surveillance pour protéger et représenter les intérêts des particuliers.
- Les États membres sont encouragés à considérer les OSC comme des partenaires dans la sensibilisation de la population pour former des « citoyens numériques », informée, capable et à l'abri du danger. Ils doivent également s'assurer que les OSC disposent d'un cadre et des protections juridiques appropriés pour contribuer à ce partenariat.

Thème : Mesures d'habilitation et de soutien

L'article 31 de la Déclaration ministérielle (Addis-Abeba, novembre 2017) appelle la Commission de l'UA « à assurer le suivi de la signature de la ratification par les États membres » de la Convention de Malabo.

En conséquence, nous encourageons les États membres à adopter l'approche suivante, en vue d'accroître la rapidité et la confiance avec lesquelles les États membres sont en mesure d'adopter et de mettre en œuvre les mesures demandées par la Convention.

Recommandations : Les décideurs doivent s'engager en collaboration avec la société civile, les défenseurs de la vie privée, les entreprises, les universités et d'autres parties prenantes, afin de produire une gamme de documents explicatifs et de formations accessibles sur les sujets suivants. L'objectif de ces documents est de surmonter les obstacles représentés par le manque de sensibilisation, de connaissance et de compréhension.

- Principes fondamentaux de la vie privée numérique, et ses risques et avantages
- Modèles commerciaux courants et/ou dominants pour les services en ligne
- Publicité et monétisation des données dans l'économie guidée par les données

- Sensibilisation aux différentes cultures et aux attentes en matière de vie privée, dans et au-delà du contexte africain
- Protection de la vie privée dès la conception et les perspectives des technologies favorisant la protection de la vie privée
- Inclusion/exclusion numérique et parties prenantes marginalisées
- Risques et inconvénients découlant des activités en ligne et des modèles commerciaux guidés par les données
- Implications des technologies émergentes (exploration des données, apprentissage automatique et intelligence artificielle, systèmes autonomes, objets connectés, etc.)
- . . . Et d'autres sujets à mesure qu'ils deviennent pertinents

Ces documents doivent constituer la base d'un programme de nombreuses tables rondes avec les parties prenantes, y compris avec la participation des décideurs, dont le but est de tirer parti des connaissances et de la sensibilisation acquises et de les utiliser immédiatement sous la forme d'un engagement renouvelé des parties prenantes. Le programme doit avoir les objectifs suivants :

- Échanger des informations et renforcer la confiance entre les parties prenantes politiques, techniques, juridiques, commerciales, universitaires et des parties prenantes issues de la société civile ;
- Améliorer les connaissances, la compréhension et la confiance des décideurs sur de nouveaux sujets ;
- Veiller à ce que les décideurs aient la possibilité de mettre ces connaissances en pratique avec leurs communautés d'intervenants ; et
- Donner aux parties prenantes informées et intéressées une voix pour façonner l'avenir en ligne de leurs pays, régions et continents.

Les membres peuvent élaborer un tel programme sur l'approche de la cybersécurité préconisée à l'article 31 de la Déclaration d'Addis-Abeba (UA/CICT-2), qui prévoit une conférence annuelle sur la cybersécurité et un événement d'un mois sur la cybersécurité à l'échelle du continent.

Par exemple, il peut être intéressant d'établir un programme régulier de :

- Publication d'un des matériels de formation susmentionnés,
- Une période de lecture et de réflexion, et
- Un atelier et une table ronde des parties prenantes pour discuter du sujet et convenir des actions à mener.

Ces activités peuvent aboutir à une conférence annuelle et à un événement d'un mois sur le thème de la protection des données et de la vie privée en ligne.

À propos de l'Internet Society

L'Internet Society (ISOC) soutient et promeut le développement d'Internet en tant qu'infrastructure technique mondiale, une ressource pour enrichir la vie des individus et une force pour le bien dans la société. Opérant à travers une communauté mondiale de chapitres et de membres, l'Internet Society collabore avec une grande diversité de groupes dans le but de promouvoir les technologies destinées à sécuriser Internet, et défend les politiques garantissant l'accès universel.

Ensemble, nous mettons l'accent sur :

- La construction et le soutien des communautés qui font fonctionner Internet ;
- La promotion du développement et de l'application de l'infrastructure Internet, des technologies et des normes ouvertes ;
- Le plaidoyer en faveur d'une politique cohérente avec notre vision d'Internet.

À propos de la Commission de l'Union africaine

L'Union africaine (UA) a été officiellement lancée en juillet 2002, suite à la décision prise en septembre 1999 par son prédécesseur, l'Organisation de l'unité africaine (OUA), créée en 1963, de créer une nouvelle organisation continentale pour poursuivre ses travaux. Au total, 54 pays ont rejoint la nouvelle organisation, dont le siège est resté à Addis-Abeba (Éthiopie).

La Commission de l'Union africaine est le secrétariat de l'UA chargé des fonctions exécutives. Elle est composée de dix fonctionnaires, dont un président, un vice-président et huit commissaires. Cette structure représente l'UA et protège ses intérêts sous les auspices de la Conférence des chefs d'État et de gouvernement ainsi que du Conseil exécutif.

La Commission de l'UA est responsable des portefeuilles suivants : Paix et sécurité, Affaires politiques, Commerce et industrie, Infrastructures et énergie, Affaires sociales, Économie rurale et agriculture, Ressources humaines, science et technologie et Affaires économiques.

La vision directrice de l'Agenda 2063 est la vision de l'UA : 'Bâtir une Afrique intégrée, prospère et en paix, dirigée par ses citoyens et constituant une force dynamique sur la scène mondiale'. La Commission de l'UA a pour mission de 'devenir une institution efficace et créatrice de valeurs qui exerce un rôle moteur dans le processus d'intégration et de développement de l'Afrique, en étroite collaboration avec les États membres de l'Union africaine, les Communautés économiques régionales et les citoyens africains'.