Réglementation des Données en Afrique : Libre Circulation des Données, Régimes des Données Ouvertes et Cyber Sécurité

Hanani Hlomani
et
Caroline B. Ncube

Documents de travail DG-004

AFRICAN ECONOMIC RESEARCH CONSORTIUM
CONSORTIUM POUR LA RECHERCHE ÉCONOMIQUE EN AFRIQUE

Apporter de la rigueur et des éléments de preuve à
l'élaboration des politiques économiques en Afrique

Réglementation des Données en Afrique : Libre Circulation des Données, Régimes des Données Ouvertes et Cyber Sécurité

Par

Hanani Hlomani
Université de Cape Town

et

Caroline B. Ncube
Université de Cape Town[1]

CREA Document de Travail DG-004
Consortium pour la Recherche Economique en Afrique, Nairobi
Février 2023

CETTE ÉTUDE DE RECHERCHE a été rendue possible grâce à une subvention du Consortium pour la Recherche Economique en Afrique. Toutefois, les conclusions, opinions et recommandations sont celles de l'auteur et ne reflètent pas nécessairement les points de vue du Consortium, de ses membres individuels ou du Secrétariat du CREA.

Publié par : Le Consortium pour la Recherche Economique en Afrique
B.P. 62882 - City Square
Nairobi 00200, Kenya

Table des matières

Résumé

Globalement, cette étude vise à répondre aux préoccupations relatives à la réglementation des données sur le continent africain. En particulier, le document se concentre sur trois aspects majeurs de la réglementation des données qui tiennent les ficelles du développement potentiel du continent. Il s'agit de la libre circulation des données, de l'adoption de régimes de données ouvertes et de la cyber sécurité. Cela se fera dans le contexte général de l'Afrique, en mettant l'accent sur les instruments réglementaires des différents organismes au niveau continental et sous régional, et sur certaines législations nationales des pays qui ont développé des instruments législatifs répondant aux mêmes préoccupations. L'accent sera également mis sur les progrès réalisés par l'Union européenne, premier organisme continental à avoir adopté une approche géographiquement concertée en matière de réglementation globale des données. L'objectif est de tirer les leçons de ces efforts dans le but de déterminer une approche centrée sur l'Afrique de la réglementation des données, en particulier dans le contexte de l'accroissement du commerce interafricain envisagé par l'accord sur la zone de libre-échange continentale africaine, et d'une économie numérique renforcée, comme le préconise la stratégie de transformation numérique pour l'Afrique (2020-2030).

Mots-clés : *Données ; Gouvernance des données ; Protection des données ; Données personnelles ; Données non personnelles ; Données ouvertes ; Cyber-sécurité ; Développement ; Afrique ; Malabo ; ZLECAf*

1. Introduction

En raison des progrès technologiques rapides, il est difficile pour les juristes, les décideurs et les législateurs de rester au fait de toutes les considérations et de tous les débats politiques importants qui sont nécessaires pour s'assurer que la loi n'est pas dépassée et finalement invalidée par la technologie. La période 2019-2020 a démontré qu'il est possible pour le monde de passer à un écosystème partiellement ou entièrement numérisé. Il a déjà été dit que plusieurs entreprises mondiales envisagent de revenir à l'ancienne façon de travailler dans la période post-pandémie de COVID-19, étant donné l'efficacité avec laquelle le monde a pu s'adapter, collaborer et produire des résultats dans un écosystème numérique. Au centre de tout cela se trouve la nécessité de déplacer les données d'un appareil à l'autre, d'un lieu à l'autre et d'une personne à l'autre. Cela crée un casse-tête juridique pour les responsables de la législation et de l'élaboration des politiques, qui doivent formuler des politiques et des instruments législatifs solides garantissant que ces données peuvent circuler librement, légalement et sans porter atteinte aux intérêts personnels ou commerciaux dans un environnement numérique sûr et protégé contre les cyberattaques.

Les données peuvent être définies comme des éléments d'information qui peuvent être qualitatifs ou quantitatifs.[2] Ces informations peuvent être de nature abstraite ou concerner une ou plusieurs personnes.[3] Les données peuvent également être définies comme un ensemble de faits tels que des mots, des chiffres ou des observations, ou comme une manière de décrire les choses.[4] Le terme « données » ne doit pas être confondu ou utilisé de manière interchangeable avec le terme « information ». En effet, les données sont un ensemble de faits non structurés et non organisés, tandis que l'information fait référence à la manière dont on comprend ces faits non organisés dans leur contexte.[5] Vu la nature de l'écosystème numérique, qui dépend fortement de la décentralisation, les données ont été désignées comme la « nouvelle frontière de l'économie » après l'or (Manzo, 2019). Cela s'explique principalement par le fait que les données sont le moyen par lequel les appareils communiquent entre eux et le principal actif sur lequel les marchés, la recherche, les gouvernements et les entreprises s'appuient quotidiennement.[6] Compte tenu de la décentralisation des modes de communication et de l'explosion de la connectivité Internet, de nombreuses données sont échangées entre les utilisateurs de l'Internet et peuvent inclure des informations allant des détails personnels des personnes à tout ce qui n'est pas de nature personnelle.[7] À mesure que les données deviennent disponibles et accessibles, la pratique de l'analyse des

données prend de plus en plus d'importance. L'analyse de données est un processus qui utilise des techniques analytiques avancées telles que l'analyse prédictive, l'analyse statistique et l'exploration de données sur des ensembles de données pour découvrir de nouveaux faits, prédire des événements ou des comportements futurs ou expliquer des phénomènes passés qui n'avaient auparavant aucune explication logique (Russom, 2013). Ces techniques analytiques ont le potentiel d'avoir un impact positif sur un certain nombre de secteurs économiques à travers le continent africain, principalement en équipant les différentes parties prenantes d'informations qu'elles n'avaient pas auparavant et d'une richesse de ressources qui étaient auparavant bloquées par la législation ou en raison de barrières géographiques.

Actuellement, les débats sur la réglementation des données s'articulent autour de la question de savoir si les données en question sont de nature personnelle ou non personnelle, en raison du fait qu'à partir d'une approche réglementaire, les données personnelles et non personnelles ne devraient pas faire l'objet du même examen. Les données personnelles peuvent être définies comme toute information relative à une personne physique identifiée ou identifiable.[8] Cela signifie qu'une personne concernée est identifiable s'il est possible de l'identifier directement/indirectement au moyen d'identifiants tels que le nom, le numéro d'identification, les données de localisation, les données physiques, génétiques, culturelles, etc.[9] En pratique, cela peut également inclure toutes les données qui sont ou peuvent être attribuées à une personne, comme les numéros de téléphone, de carte de crédit ou les numéros personnels d'une personne.[10] Le contraire, et donc la définition des données non personnelles, sont des données électroniques qui ne contiennent aucune information pouvant être utilisée pour identifier une personne physique. Il peut s'agir, par exemple, de données non personnelles à l'origine, comme les données météorologiques, les cours des marchés boursiers, etc. ou de données qui étaient auparavant de nature personnelle mais qui ont été rendues anonymes (dépourvues de toute donnée personnelle).[11]

Comme cela a été dit, le taux de progression de la technologie rend de plus en plus difficile de suivre la meilleure façon de réglementer les données. Le continent africain a semblé se préoccuper davantage de la protection des données personnelles de ses citoyens. On estime qu'environ 24 des 55 pays d'Afrique ont adopté ou adopté une forme de réglementation, dans le but de protéger les données personnelles.[12] Cela a été largement attribué à la promulgation du règlement général européen sur la protection des données (RGPD),[13] qui a été adoptée en 2016 et qui est très influente en raison de sa réglementation des flux de données transfrontaliers, et qui a eu un impact sur un certain nombre de pays modèles de protection des données à l'échelle mondiale. Cependant, la plupart des pays axés sur l'innovation ont compris l'intérêt de formuler des régimes réglementaires qui protègent les données personnelles tout en veillant, dans le même temps, à ce que les données non personnelles puissent être extraites des données personnelles afin de favoriser l'innovation. En d'autres termes, au-delà de la valeur des données naturellement non personnelles, il y a également de la valeur dans les données qui ont été enfermées dans des ensembles de données contenant des informations personnellement identifiables.

Approches actuelles des États Africains et importance pour la zone de libre-échange continentale Africaine

L'Union africaine (UA) a adopté en 2014 la Convention sur la cyber sécurité et la protection des données personnelles lors de la vingt-troisième session ordinaire de l'Assemblée, qui s'est tenue à Malabo, en Guinée équatoriale (connue sous le nom de Convention de Malabo), qui n'est pas encore entrée en vigueur car le nombre requis de ratifications n'a pas été atteint. Cette convention, tout comme le GDPR, était focalisée sur les données personnelles et la cyber sécurité.[14] Au moment de la rédaction du présent document (octobre 2021), la Commission de l'UA élabore le cadre de la politique africaine en matière de données, qui s'inspire en partie de la Convention de Malabo.[15] Plusieurs communautés économiques régionales (CER) ont également adopté des instruments réglementaires, qui seront résumés dans la section 3 ci-dessous. En dehors de cet effort concerté, très peu a été fait en termes d'instrument législatif collectif continental/régional sur la protection des données, la plupart des pays ayant choisi de tenter une protection individuelle.

Alors que le continent s'apprête à réaliser les promesses de la Zone de libre-échange continentale africaine (ZLECAf), il sera important d'avoir une certaine harmonisation des cadres réglementaires afin de renforcer le commerce interafricain. Les entreprises et les entrepreneurs individuels qui font du commerce dans différents pays d'Afrique auraient tout à gagner s'ils avaient l'assurance que des principes similaires de protection des données et des modèles de gouvernance des données sont alignés sur tout le continent. Le commerce électronique et le commerce numérique ont connu une croissance exponentielle au cours des deux dernières années suite aux restrictions imposées aux interactions physiques entre les personnes pour enrayer la propagation de la pandémie de COVID-19. L'UA est le fer de lance de la croissance du commerce numérique grâce à la stratégie de transformation numérique pour l'Afrique 2020-2030.[16] Et dans ce contexte, un protocole de commerce électronique est en cours de négociation dans le cadre de la ZLECAf.[17] Il est prévu que la ZLECAf et la Stratégie de transformation numérique pour l'Afrique propulse l'économie numérique de l'Afrique (Chaytor, 2020). Comme nous l'expliquons dans la section 3 ci-dessous, la libre circulation des données est un élément important de la promotion du commerce interafricain et des flux de données transfrontaliers pour apporter des avantages significatifs. Au-delà des négociations du protocole de commerce électronique de la ZLECAf, il existe un élan mondial pour des négociations similaires. Plus précisément, l'Organisation mondiale du commerce (OMC) a entamé en janvier 2019 des négociations sur les aspects du commerce électronique liés au commerce, qui se poursuivent.[18] L'élaboration d'approches africaines communes contribuera donc à façonner l'agenda mondial de l'OMC (Okonjo-Iweala, 2021).

Définir les données personnelles

La délimitation de ce qui relève des données à caractère personnel a laissé les spécialistes perplexes pendant un certain temps. Alors que les données évidentes telles que les noms, les numéros d'identification, etc. sont indéniablement des données personnelles, la définition de l'UE des données personnelles à l'article 4.1 du GDPR définit les données personnelles comme toute information relative à une personne physique identifiée ou identifiable. Puisque la définition inclut "toute information", on doit supposer que le terme "données personnelles" doit être interprété aussi largement que possible. C'est pour cette raison que les limites de ce qui est personnel ou non sont constamment débattues.

Dans le cas de l'affaire Breyer,[19] la Cour de justice de l'Union européenne (CJUE), en tentant de définir ce qu'est une "donnée à caractère personnel", a estimé que tout élément d'information, qui, lorsqu'un complément d'information est demandé à un tiers, permet d'identifier une personne concernée, constitue une donnée à caractère personnel.[20] En tant que tel, si l'on devait appliquer les principes de Breyer de manière pratique, la probabilité que des données, qui se présentaient initialement comme des données non personnelles, puissent finalement tomber dans le champ de la définition des données personnelles du GDPR.[21] Dans ce cas, le fait de ne pas tenir compte des données non personnelles peut signifier qu'elles sont soumises aux mêmes restrictions que les données personnelles ou à d'autres exigences de localisation des données.

Outre les lignes floues sur ce qui constitue des données personnelles, les exigences de localisation des données constituent également une menace pour la transformation économique radicale du continent africain sur le dos de la révolution des données. Les exigences de localisation des données sont généralement des restrictions sur le flux de données d'un pays à l'autre. Par exemple, la loi peut exiger que tout traitement de données relatives aux citoyens d'un pays donné soit effectué à l'aide de serveurs situés à l'intérieur des frontières de ce pays, ce qui rend illégal le traitement de ces données ailleurs que sur ce territoire.[22] Ces restrictions augmentent le coût des activités transfrontalières et, dans un écosystème numérique, la menace pour l'efficacité est réelle. Par ailleurs, elles étouffent l'accès des entreprises et des organismes du secteur public à des services moins chers et plus innovants, ou obligent les entreprises opérant dans plusieurs pays à recourir à des capacités excédentaires de stockage et de traitement des données.[23] Pour les jeunes entreprises et les petites et moyennes entreprises (PME), cela constitue un sérieux obstacle à la croissance, à l'entrée sur de nouveaux marchés et au développement de nouveaux produits et services.[24] L'UE a adopté un cadre réglementaire pour la libre circulation des données à caractère non personnel dans l'UE,[25] qui énumère certaines des données non personnelles comme étant des données générées par l'intelligence artificielle, l'internet des objets et l'apprentissage automatique comme sources potentielles de données non personnelles, ainsi que quelques exemples très précis.[26]

Vue d'ensemble du document

Compte tenu de ce qui précède, le présent document tentera d'aborder les questions suivantes. Tout d'abord, il s'interrogera sur la manière dont les données (personnelles et non personnelles) ont été traitées par l'UE en tant que référence, dans le but d'imaginer comment un système harmonisé de réglementation des données qui englobe les données personnelles et non personnelles pourrait se présenter à l'échelle continentale ou régionale en Afrique. L'accent sera mis sur la détermination de la manière dont les instruments juridiques orientent ou rendent obligatoire l'identification des données non personnelles. En effet, outre les efforts déjà déployés pour protéger les données personnelles, il est nécessaire de réglementer la manière dont les données non personnelles sont utilisées afin de garantir que les données personnelles et non personnelles puissent circuler librement sur le continent et dans le monde entier, en s'appuyant sur une réglementation et des politiques solides. Cette libre circulation est nécessaire pour tirer parti des avantages économiques potentiels et peut contribuer à la réalisation du programme de développement de l'Afrique et des objectifs de développement durable (ODD). Le thème central étant celui de la libre circulation des données, le document approfondira ensuite des aspects tels que l'utilisation et la libéralisation des politiques de données ouvertes (la notion selon laquelle des données spécifiques devraient être librement disponibles pour être utilisées et réutilisées, notamment les informations du secteur public). Le document abordera ensuite, au-delà des problèmes juridiques potentiels liés à la libéralisation des données et à leur circulation, les préoccupations en matière de cyber sécurité qui accompagnent un tel régime réglementaire. Pour ce faire, nous examinerons la manière dont la Convention de Malabo protège les données personnelles, les communautés économiques régionales (CER) et les approches individuelles des États membres de l'UA en matière de cyber sécurité.[27]

2. L'approche de l'Union Européenne en matière de données

L'Union européenne (UE) a été à l'avant-garde de la mise en place d'un cadre réglementaire complet sur les données de nature personnelle et non personnelle. Depuis 2014, la Commission européenne a élaboré un certain nombre de directives et de lois visant à faciliter le développement d'une économie agile en matière de données. Citons par exemple le règlement sur la libre circulation des données non personnelles[28], la directive sur les données ouvertes[29], le GDPR[30] et la loi sur la cyber sécurité.[31] La stratégie européenne en matière de données récemment adoptée[32] adopte une approche interdisciplinaire de la réglementation de l'économie des données. La stratégie est ancrée dans la nécessité d'étendre l'utilisation, la demande et le développement responsables des produits et services numériques au sein du marché unique européen pour la période 2020 à 2025 et est soutenue par l'intention de faire de l'UE un leader dans une société axée sur les données. Par conséquent, la création d'un marché unique des données permettra à celles-ci de circuler librement au sein de l'UE et entre les secteurs, au profit des entreprises, des chercheurs et des administrations publiques.[33]

Comme il a été dit précédemment, le GDPR s'applique principalement au traitement des données à caractère personnel.[34] Cela s'applique à la fois à une personne identifiée et à une personne physique identifiable.[35] Si cela est appliqué concrètement, cela signifie donc que le GDPR et, par extension, la protection des données ne s'applique pas aux informations anonymes ou aux informations qui ne se rapportent pas à une personne physique identifiée ou identifiable. Il en va de même pour les données à caractère personnel qui ont été tellement diluées ou cryptées qu'elles sont rendues anonymes parce que la personne concernée n'est plus identifiable. C'est dans ce contexte que l'Union européenne a adopté le règlement relatif à un cadre pour le flux libre des données à caractère non personnel dans l'UE[36], également connu sous le nom de règlement FFD. Le règlement indique clairement qu'il "s'applique au traitement des données électroniques autres que les données personnelles"[37]

La formulation de ce règlement est née du constat que l'expansion de l'Internet des objets (IoT), de l'intelligence artificielle et de l'apprentissage automatique, qui sont des sources importantes de données non personnelles, posait continuellement des problèmes juridiques aux législateurs et aux tribunaux, car il n'existait aucun précédent sur la manière de traiter ces données. Dans un environnement concurrentiel où des pratiques telles que l'analyse des données peuvent créer un avantage concurrentiel,

les données non personnelles telles que la navigation en temps réel pour éviter le trafic peuvent permettre aux entreprises d'économiser jusqu'à 730 millions d'heures de temps de transit et jusqu'à 20 milliards d'euros en coûts de main-d'œuvre, entre autres exemples.[38]

Ayant pris conscience de la valeur et de l'utilité des données non personnelles, le règlement FFD vise à garantir quatre objectifs principaux :

(i) Le flux libre de données non personnelles à travers les frontières au sein de l'UE. Dans le même ordre d'idées, il s'agit de faire en sorte que toute organisation intéressée qui a la capacité et les moyens de le faire puisse stocker et traiter des données partout dans l'UE.

(ii) La disponibilité des données pour le contrôle réglementaire. En ce sens, elle vise à garantir que les autorités publiques conservent l'accès aux données, même lorsqu'elles sont situées dans un autre pays de l'UE ou lorsqu'elles sont stockées ou traitées dans le nuage.

(iii) La possibilité de changer efficacement et facilement de fournisseur de services en nuage pour les utilisateurs professionnels. La Commission a commencé à faciliter l'autorégulation dans ce domaine, en encourageant les fournisseurs à élaborer des codes de conduite concernant les conditions dans lesquelles les utilisateurs peuvent déplacer les données entre les fournisseurs de services en nuage et les réintégrer dans leurs propres environnements informatiques.

(iv) Cohérence et synergies totales avec le paquet sur la cyber sécurité, et clarification du fait que toutes les exigences de sécurité qui s'appliquent déjà aux entreprises stockant et traitant des données continueront de s'appliquer lorsqu'elles stockent ou traitent des données au-delà des frontières de l'UE ou dans l'informatique en nuage.

Le GDPR prévoit déjà le flux libre des données personnelles au sein de l'UE[39] sous réserve du respect/de la fourniture de certaines garanties.[40] Ainsi, la fusion de toutes les lois relatives à la réglementation des données dans l'UE garantit une approche globale et cohérente vis-à-vis du libre flux de toutes les données dans l'UE.

Leçons tirées de l'approche de l'UE

Les principaux enseignements à tirer de l'approche européenne sont les suivants : premièrement, l'UE a compris qu'il existe différents types de données et que les données personnelles ne sont pas les seules à avoir de la valeur ou à mériter une protection/réglementation. Deuxièmement, ces données n'ont pas de valeur lorsqu'elles sont statiques. Au contraire, toute valeur à tirer des données n'apparaît que lorsque celles-ci sont autorisées à circuler/se déplacer librement dans l'UE.

Troisièmement, l'approche de l'UE en matière de réglementation des données prend la forme d'une approche à multiples facettes. En plus d'avoir adopté une stratégie en matière de données qui sert de guide par rapport auquel tous les efforts législatifs doivent aspirer, on a pris conscience que pour atteindre les objectifs de la stratégie, différentes législations devraient être adoptées, bien qu'ayant le même objectif en tête. Étant donné que la réglementation des données comporte de nombreux aspects et que la technologie est en constante évolution, l'approche à facettes multiples offre non seulement une plus grande clarté et une plus grande certitude juridiques sur les différentes questions réglementaires, mais elle facilite également la modification et le développement de parties distinctes de la loi sans perturber les textes législatifs connexes. L'efficacité de cette stratégie, bien qu'elle soit toujours en cours d'élaboration, a jusqu'à présent donné des résultats positifs et suscité l'admiration du reste du monde, comme en témoigne le nombre de pays qui ont « emprunté » diverses dispositions des différents textes législatifs de l'UE pour les mettre en œuvre dans le cadre de leurs efforts réglementaires nationaux et régionaux.

3. Approches réglementaires africaines de la libéralisation des données et de leur circulation

La libre circulation des données

L'avènement de l'Internet a offert au monde un moyen d'envoyer de grandes quantités de données à presque n'importe quel endroit de la planète à un coût minimal. En fait, on peut dire que l'envoi de données au-delà des frontières ne coûte pas plus cher que l'envoi de données à l'intérieur de ces mêmes frontières. La pandémie de COVID-19 a mis en évidence l'importance des flux de données pour l'économie mondiale. Il a été démontré que les flux de données ont une influence dans des domaines tels que les soins de santé (traçage des contacts/recherche médicale/production de vaccins), les affaires/le commerce (achats en ligne, services de diffusion en continu, réunions/conférences virtuelles) et la vie sociale (appels vidéo familiaux, concerts en ligne). La mesure dans laquelle ces domaines ont été influencés (positivement) est un indicateur qu'à l'avenir, les flux de données ne feront qu'augmenter à mesure que davantage de pays et de secteurs adopteront la transformation numérique. Il a déjà été établi qu'entre 2007 et 2017, les flux de données mondiaux ont été multipliés par plus de vingt et on s'attend à ce que d'ici 2022, la situation de 2017 ait quadruplé (Banque mondiale, 2021).

Dans le contexte africain, les cadres internationaux et régionaux qui facilitent les flux de données transfrontaliers seront indispensables pour faciliter la mise en place d'un marché commun et, par extension, la réalisation des objectifs de développement du continent, comme la mise en place de la Zone de libre-échange continentale africaine (ZLECAf)[41] et de l'Agenda 2063 de l'Union africaine.[42] Alors que certains pays permettent aux données de circuler librement à l'intérieur et à l'extérieur de leurs frontières, de nombreux autres ont adopté des cadres législatifs qui parlent de la protection des données personnelles et qui contiennent, dans la plupart des cas, des clauses de localisation des données. En général, les lois sur la localisation des données exigent que les données personnelles relatives aux citoyens ou aux résidents d'une nation soient collectées, traitées et stockées à l'intérieur des frontières du pays (Bowman, 2017). Lorsqu'il est demandé que ces données soient transférées à l'international, plusieurs approbations et beaucoup de bureaucratie doivent être respectées.[43] Les lois sur la localisation des données sont souvent rendues nécessaires par des préoccupations liées à la sécurité des données. Ces lois visent à garantir, grâce à la surveillance et à d'autres méthodes de contrôle, que lorsque des données doivent être échangées, ces données sont obtenues légalement (à travers un consentement librement donné),

que les données sont utilisées/échangées dans un but spécifique, et que les données ne sont pas utilisées pour des activités non autorisées telles que le profilage ou la surveillance par les gouvernements ou tout autre tiers sans consentement (sauf si la loi l'exige).[44] Bien qu'il soit entendu qu'il est impératif que les transactions numériques soient soutenues par de formidables cadres réglementaires en matière de protection de la confidentialité, de sécurité et de protection des consommateurs, ces cadres peuvent entraver le transfert et l'utilisation transfrontaliers des données en imposant des efforts et des coûts substantiels aux entreprises, notamment aux micro, petites et moyennes entreprises (MPME), ce qui empêche les échanges internationaux.[45]

Dans les économies numériques et physiques d'aujourd'hui, la liberté de transférer des données de nature personnelle et non personnelle sans restriction entre les pays produit des résultats positifs pour les organisations, les individus et les pays.

Avantages des flux de données transfrontaliers

Avantages pour les particuliers

Pour les particuliers, le niveau et l'influence d'Internet ont déjà permis une interaction transparente avec des personnes et des organisations du monde entier. De même, les particuliers ont été exposés à des biens et services provenant de marchés étrangers, disponibles en ligne et pouvant être livrés dans de brefs délais, là où ces produits sont physiques.[46] Comme cela a déjà été mentionné,[47] la pratique de l'analyse des données a permis aux organisations de desservir des marchés plus géographiques, donnant à ces clients l'accès à une gamme plus large de biens et de services en fonction de leurs intérêts, de leurs désirs et de leurs besoins, ce qui améliore encore la concurrence sur les marchés et la satisfaction globale des clients.[48] En outre, les flux transfrontaliers de données permettent également aux individus de travailler à distance, où qu'ils se trouvent dans le monde. L'essor du travail à distance est connu sous le nom de "nuage humain". Le "nuage humain" est défini comme un ensemble naissant de marchés du travail en ligne ou numériques où les professionnels compétents et ceux qui cherchent à embaucher des professionnels peuvent se localiser et s'engager mutuellement dans des accords d'emploi/de travail.[49] Fin 2018, on estimait que l'argent dépensé pour l'utilisation du nuage humain générait environ 82 milliards de dollars dans le monde, un chiffre qui devait croître de façon exponentielle.[50] La facilitation des flux transfrontaliers permettra non seulement au pays d'accueil d'exporter des talents, mais aussi de réduire le taux de chômage et de générer des devises étrangères.

Avantages pour le pays

Les flux transfrontaliers libres ont permis à un plus grand nombre d'entreprises et de consommateurs nationaux d'accéder à la sphère du commerce numérique, encourageant ainsi l'adoption de stratégies commerciales fondées sur les données et stimulant

l'économie nationale.[51] Les entités du secteur public et les services gouvernementaux bénéficient également des flux transfrontaliers de données, ce qui leur permet de fournir des services publics de meilleure qualité à moindre coût et de poursuivre des objectifs de politique publique qui ne seraient peut-être pas réalisables autrement.

Avantages pour les organisations

La libre circulation des données à caractère personnel apporte des avantages sociaux et économiques beaucoup plus rapidement que l'autre solution, qui obligerait les entreprises à construire activement leurs arrière-bureaux et à rationaliser leurs processus et leurs fonctions de stockage pour servir de multiples marchés individuels.[52] Les pays qui adoptent des régimes réglementaires favorisant le libre transfert international des données permettent aux petites organisations spécialisées d'établir une présence sur Internet qui soit à la fois nationale et internationale.[53] Ainsi, il est possible d'adopter avec succès des services sur un marché national, puis de les étendre à d'autres marchés, ce qui apporte des avantages rapides au deuxième pays et aux pays ultérieurs.[54]

L'un des principaux avantages de l'Internet est qu'il permet à toute organisation, aussi petite soit-elle, d'utiliser l'Internet pour commercialiser et fournir ses idées, ses biens et ses services, partout où les données sont autorisées à circuler. En ce sens, s'il existe des restrictions à la circulation des données, les organisations ne seraient pas en mesure de fournir des informations et des produits en réponse aux demandes des particuliers.[55] Les organisations multinationales sont également en mesure de gagner en efficacité en centralisant et en virtualisant leurs opérations internes. Parmi les exemples d'amélioration de l'efficacité, citons l'expansion rentable des activités en utilisant une infrastructure flexible basée sur le nuage et des fournisseurs de services d'applications spécialisés, et en minimisant les investissements dans des matériels informatiques supplémentaires.[56]

L'avantage non apparent de la pandémie de COVID-19 parmi tous les aspects négatifs est que de plus en plus d'entreprises internationales ont compris l'importance d'adopter des stratégies de transformation numérique axées sur les données pour assurer leur avenir. Ces stratégies ont tendance à dépendre de la capacité à collecter, analyser, traiter et stocker des données dans des opérations multi-pays. La pratique de l'analyse des données s'amplifie d'autant plus que les entreprises cherchent à générer de nouvelles connaissances sur les clients et sur la performance de leurs opérations et de leurs produits.[57]

Lois sur la localisation des données en Afrique

Cette section donne un aperçu des lois de localisation des données de certains États africains. En lieu et place des opinions exprimées dans la section 3.1 de ce document, selon lesquelles les lois sur la localisation des données ne favorisent pas la libre circulation des données, la promulgation et la mise en œuvre de ces lois, par exemple à travers de lourdes amendes pour l'utilisation du stockage de données à distance,

ont des effets néfastes. Cependant, chaque État a le droit de promulguer et de mettre en œuvre ses lois nationales. La contribution de cet article est que, dans les processus législatifs et d'élaboration des politiques, les États africains devraient tenir compte de l'impact de la localisation des données sur les flux de données.

La Côte-d'Ivoire

En 2013, la Côte d'Ivoire a adopté des lois sur la protection de la confidentialité,[58] qui exigeait que les entreprises obtiennent l'autorisation préalable du régulateur avant de traiter des données personnelles en dehors de la Communauté économique des États d'Afrique de l'Ouest (CEDEAO).

Le Ghana

En 2019, le Ghana a promulgué le projet de loi et les lignes directrices sur les systèmes de paiement du Ghana qui, entre autres, définissent les exigences pour obtenir une licence d'opérateur de systèmes de paiement, ce qui a trait à la propriété locale et à la nomination d'administrateurs ghanéens. Avant cela, en juillet 2018, le Ghana a publié un projet de réglementation qui exigeait que toutes les transactions nationales soient traitées par le système de paiement et de règlement interbancaire du Ghana (GhiPPS, qui est détenu à 100 % par la Banque centrale du Ghana).

Le Kenya

La Loi sur la protection des données de 2019 au Kenya[59] ne prévoit pas les dispositions explicites sur la localisation des données, qui figuraient dans les versions antérieures de la loi. Cependant, elle contient toujours des dispositions restrictives concernant les données personnelles, qui exigent un consentement explicite pour les transferts de "données personnelles sensibles"[60] et que les responsables du traitement des données garantissent et fournissent la preuve que les données à caractère personnel transférées à l'étranger bénéficient de la même protection que si elles étaient stockées à l'intérieur des frontières du Kenya.[61] Les règlements d'application de ces dispositions sont encore en cours d'élaboration.

Les mesures proposées (2021)

Suite à la promulgation de la loi sur la protection des données de 2019, le Kenya a publié trois projets de règlement sur la protection des données pour faciliter la mise en œuvre de la loi sur la protection des données.[62] Il s'agit du Règlement (général) sur la protection des données,[63] le règlement sur la protection des données (enregistrement des contrôleurs et des responsables du traitement des données)[64] et le Règlement sur la protection des données (conformité et application).[65] En vertu des mesures proposées,

le règlement général exige que, lorsque le traitement des données est effectué dans le but de produire un bien public, le traitement doit être réalisé à travers un serveur et un centre de données situés à l'intérieur des frontières du Kenya.[66] Et qu'au moins une copie de référence des données personnelles doit être stockée dans un centre de données situé au Kenya.[67] Le règlement comprend également des dispositions relatives au transfert transfrontalier de données à caractère personnel. En vertu du Règlement général, avant de transférer des données à caractère personnel en dehors du Kenya, le destinataire doit savoir qu'il est lié par des obligations juridiquement exécutoires visant à garantir le même niveau de protection aux données à caractère personnel transférées que celui prévu par la loi sur la protection des données au Kenya et le Règlement général;[68] que la personne concernée soit informée des garanties et des implications et risques liés au transfert transfrontalier;[69] que la personne concernée a consenti au transfert de ses données à ce destinataire;[70] que l'entité transférante a pris des mesures raisonnables pour garantir que les données personnelles transférées ne sont pas utilisées à des fins non prévues;[71] et que les droits de la personne concernée sont sauvegardés.[72] Le Règlement général prévoit également que le transfert transfrontalier de données peut être autorisé sans restrictions lorsque le transfert est "nécessaire", conformément à l'article 48(c) de la loi sur la protection des données;[73] lorsque les exigences constituent une discrimination arbitraire ou injustifiée à l'égard d'une personne;[74] lorsque les exigences imposent une restriction au commerce;[75] et lorsque les restrictions aux transferts de données personnelles sont plus importantes que ce qui est nécessaire pour atteindre les objectifs de la loi sur la protection des données.[76] Le règlement général prescrit également les termes qui doivent figurer dans les accords de transfert transfrontalier entre les entités transférantes et les destinataires des données à caractère personnel, sans toutefois prescrire de modèles de clauses types comme c'est le cas dans l'Union européenne.[77]

Le Nigeria

En 2015, le Nigeria a promulgué de vastes exigences en matière de localisation des données dans le cadre des lignes directrices pour le développement du contenu nigérian dans les TIC.[78] Dans les lignes directrices, il est demandé à toutes les entreprises de télécommunications souhaitant héberger des données sur les abonnés et les consommateurs au Nigeria d'héberger ces données dans le pays et conformément à la législation en vigueur.[79] Il en va de même pour les sociétés de services en réseau[80] et les sociétés de gestion des données et de l'information.[81]

En 2011, la Banque centrale du Nigeria a également introduit une exigence de stockage et de traitement local pour les entités qui offrent des services de cartes aux points de vente (POS).[82] En vertu de la ligne directrice 4.4.8, toutes les transactions nationales, y compris, mais sans s'y limiter, les transactions aux points de vente et aux guichets automatiques au Nigeria, doivent être connectées en utilisant les services d'un opérateur local et ne doivent en aucun cas être acheminées hors du Nigeria pour être connectées entre les émetteurs et les acquéreurs nigérians.[83]

Le Rwanda

En 2012, le Rwanda a promulgué une réglementation selon laquelle toutes les données d'information critiques du gouvernement doivent être hébergées dans son centre de données national.[84] En termes d'application indirecte des lois sur la localisation des données, en 2017, le régulateur des télécommunications du Rwanda a imposé à MTN une amende de 8,5 millions de dollars US pour avoir conservé des données de clients rwandais en Ouganda et pour avoir exploité ses services informatiques en dehors du pays en violation de sa licence (CNBC Africa, 2017). Des commentaires ont déjà été faits dans la section introductive 3.3. ci-dessus sur la promulgation et la mise en œuvre des lois sur la localisation des données. En outre, on pourrait faire valoir que l'imposition d'amendes aussi élevées pourrait freiner les investissements des entreprises qui souhaitent utiliser des installations de stockage de données à distance.

Le Sénégal

En 2021, et à la lumière du nouveau centre de données du gouvernement en cours de construction au Sénégal, le président Macky Sall a annoncé que toutes les données et applications du gouvernement seront hébergées dans ce centre et que toutes les données stockées sur des serveurs étrangers seront rapatriées dans l'espoir de renforcer la souveraineté numérique du Sénégal (Swinhoe, 2021).

L'Afrique du Sud

En 2018, après s'être rendu compte que les banques sud-africaines nationales avaient l'intention de transférer une plus grande partie de leurs transactions vers des réseaux de services de paiement mondiaux, la Banque de réserve sud-africaine a suspendu la migration de tous les volumes de transactions nationales de Bankserv (système de paiement national appartenant aux banques sud-africaines) vers des systèmes de paiement internationaux.[85] La suspension devait rester en vigueur jusqu'à ce qu'une nouvelle politique soit élaborée et promulguée. Cette politique n'a pas encore été élaborée et promulguée au moment de la rédaction du présent document.

En 2013, l'Afrique du Sud a promulgué la loi sur la protection des informations personnelles (la loi POPI)[86], mais qui n'est entrée pleinement en vigueur que le 1er juillet 2021, soumet le transfert d'informations personnelles en dehors de l'Afrique du Sud à certaines exceptions. Celles-ci comprennent l'exigence que le destinataire des données soit en mesure d'offrir une protection complémentaire des données,[87] que la personne concernée consente au transfert des données ,[88] que le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et la partie responsable[89] ou pour la conclusion/l'exécution d'un contrat dans l'intérêt de la

personne concernée[90] et si le transfert est au bénéfice de la personne concernée.[91] Bien qu'il ne s'agisse pas de lois explicites sur la localisation, on s'inquiète de la manière dont elles seront interprétées et appliquées, car elles pourraient devenir des outils de localisation des données de facto.[92]

Mesures proposées

Plus récemment, le "Projet de politique nationale sur les données et le nuage" de l'Afrique du Sud de 2021[93] préconise l'adoption de normes de localisation des données et de traitement local des données pour toutes les données relatives aux "infrastructures d'information critiques"[94] et la mise en miroir des données pour les données personnelles.[95] Elle stipule également que toutes les données générées en Afrique du Sud sont la propriété de l'Afrique du Sud, quelle que soit la nationalité de l'entreprise impliquée dans leur collecte.[96]

L'Égypte

En Égypte, le président Abdel Fattah el-Sisi a ratifié la loi sur la protection des données personnelles[97] le 13 juillet 2020. La loi vise à protéger et à réglementer la collecte et le traitement des données personnelles des citoyens et résidents égyptiens. En ce qui concerne la localisation des données, la loi interdit le transfert ou la conservation de données personnelles vers un pays ou un territoire étranger sans l'autorisation du Centre égyptien de protection des données et à moins que ce pays ou territoire ne dispose de niveaux adéquats de protection des données personnelles.[98] Le ministre égyptien des communications et des technologies de l'information, Amr Talaat, aurait également déclaré que la loi sur la protection des données a été formulée pour soutenir les efforts du ministère visant à localiser l'industrie des centres de données et à créer un environnement sûr pour la circulation des informations dans le cyberespace.[99] L'Égypte fait également partie de l'Union du Maghreb arabe, qui n'a pas encore tenté de réglementer les données collectivement en tant qu'union.

Angola

La loi de protection des données[100] s'inspire des dispositions que l'on trouve dans les régimes juridiques de l'UE et du Portugal en matière de protection des données personnelles. L'autorité chargée de l'application de la loi, connue sous le nom d'Agência de Proteção de Dados (APD), n'a été créée qu'en octobre 2019 alors que la loi a été créée en 2011, et il n'y a actuellement aucun niveau significatif d'application de la loi. La loi exige que l'APD soit notifiée avant tout transfert international de données personnelles vers des pays jugés disposer d'un niveau de protection adéquat[101] en plus des exigences spécifiques qui doivent être satisfaites, telles que le consentement de la personne concernée. .[102] L'Angola appartient également à la

Communauté économique des États d'Afrique centrale (CEEAC), qui a adopté en 2016 une loi type (avec le soutien de l'UIT et de l'UE). Cependant, la CEEAC ne disposant pas d'instruments de droit communautaire contraignants, seuls 3 États membres sur 10 ont adopté une loi nationale sur la confidentialité (Le Bihan, 2018).

Politiques/normes en matière de données ouvertes

Pour compléter l'appel à la libéralisation des flux de données transfrontaliers, les normes/politiques ouvertes pour les données peuvent également être des outils particulièrement utiles pour faciliter l'accès, l'utilisation, la publication et le partage de données de meilleure qualité par les individus et les organisations, tout en répondant simultanément aux préoccupations de cyber sécurité. Les normes ouvertes pour les données sont des accords réutilisables qui nécessitent l'accès, l'utilisation, la publication et le partage de données de meilleure qualité (Open Data Institute, 2021). Les normes de données ouvertes peuvent également être définies comme des ensembles de spécifications ou d'exigences sur la manière dont des ensembles spécifiques de données doivent être mis à la disposition du public.[103]

Ils sont particulièrement utiles car :

1. Ils augmentent l'interopérabilité : L'interopérabilité des données est une caractéristique des ensembles de données où les données peuvent être facilement récupérées, traitées, réutilisées et reconditionnées (« exploitées ») par d'autres systèmes avec peu ou pas d'effort.[104]

2. Elles améliorent la comparabilité des données : Comme les normes de données ouvertes permettent un accès facile aux ensembles de données, elles facilitent la comparaison des données provenant de différentes sources et permettent de tirer des conclusions plus concrètes en s'appuyant sur un ensemble d'ensembles de données similaires.

3. Elles permettent l'agrégation : En réduisant les obstacles à l'accès aux données, les normes ouvertes pour les données encouragent la publication de nouvelles données et de données de meilleure qualité structurées de manière similaire, ce qui facilite leur combinaison. Ce faisant, le coût et la complexité de la combinaison de données similaires provenant de sources multiples sont considérablement réduits (Open Data Institute, 2021).

4. Ils permettent d'établir des liens : Les normes ouvertes facilitent la combinaison de divers ensembles de données pour donner des informations utiles.

Utilisations courantes des normes ouvertes pour les données

Comme cela a été dit, les normes ouvertes sont importantes pour aider à la création d'un écosystème de données solide. Au sein de cet écosystème, il y a les actifs de données, les organisations responsables de l'exploitation et de la maintenance des actifs de données, et les guides qui définissent comment utiliser, stocker et gérer les données.[105] Une infrastructure de données solide est fondamentale pour favoriser l'innovation des entreprises, améliorer les services publics et créer des communautés saines et durables.[106]

Promouvoir une compréhension commune

Il existe aujourd'hui de nombreuses normes ouvertes pour différents objectifs et dans différents secteurs. Le point commun de toutes les normes ouvertes réussies est qu'elles se concentrent sur la résolution de problèmes spécifiques avec des accords réutilisables qui favorisent une meilleure qualité des données. Par conséquent, lorsque des personnes et des organisations ont besoin de s'entendre sur des orientations communes, un langage partagé ou des modèles communs pour résoudre des problèmes, les normes ouvertes sont idéales.[107]

Soutenir la politique et la législation

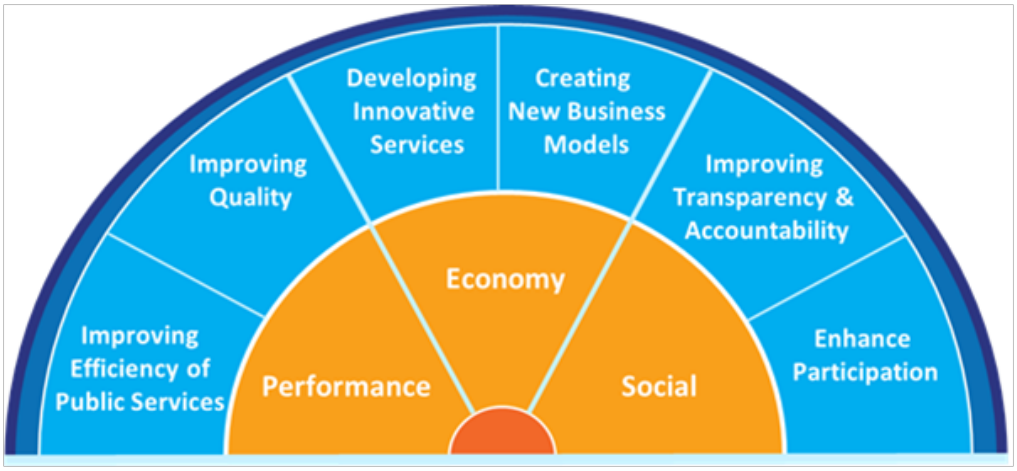
Lors de la mise en œuvre des politiques et de la justification de la législation adoptée ou élaborée par les gouvernements et autres organismes publics, les normes ouvertes pour les données peuvent constituer des outils de soutien utiles. En établissant des normes sur la manière de divulguer les données, d'automatiser les contrôles de conformité, d'agréger les données ou d'en rendre compte, on peut produire des données de meilleure qualité et renforcer les infrastructures de données.[108]

Pour combler les lacunes d'une infrastructure de données

Une solide infrastructure de données[109] est fondée sur des principes qui favorisent la redevabilité, la transparence, l'innovation commerciale, la société civile et les services publics. Au sein de l'infrastructure se trouvent les actifs de données, les organisations qui les exploitent et les entretiennent, ainsi que les règlements qui décrivent comment utiliser et gérer les données.[110] Il est donc important qu'une infrastructure de données solide soit soutenue par des normes de données ouvertes. L'identification des lacunes est rendue plus facile par la réduction des obstacles à l'entrée dans les ensembles de données et par la participation d'un plus grand nombre de parties prenantes.

Avantages des normes ouvertes de données

Les avantages des normes ouvertes de données peuvent être résumés à l'aide de l'image ci-dessous.



Source: Image issue des données europa.eu[111]

Avantages économiques

Les avantages économiques des normes de données ouvertes sont plus importants pour cette discussion. Le nœud des avantages présentés par les normes de données ouvertes est que les normes créent de nouvelles opportunités commerciales et des écosystèmes qui encouragent la concurrence. Premièrement, les normes contribuent à déconcentrer l'autorité. Les leaders du marché et les autorités bien établies sont découragés d'utiliser des formats personnalisés et propriétaires et choisissent plutôt d'utiliser des normes produites et partagées en coopération (Open Data Institute, 2021). Cela a pour effet d'uniformiser les règles du jeu pour la production et l'utilisation des données, permettant ainsi de nouvelles utilisations des données et de nouvelles entrées sur le marché.[112]

Par conséquent, en réduisant efficacement les obstacles à l'entrée et les coûts associés à la collecte et à l'agrégation des données dans un secteur particulier, les normes permettent également à un plus grand nombre d'organisations d'entrer dans l'écosystème afin de fournir des produits et des services plus diversifiés au sein de l'écosystème de données.[113] Parmi les exemples, citons la traduction, la conversion, la combinaison, l'établissement de rapports, la formation, l'analyse, les produits de consommation, les services interentreprises, etc. Les normes ouvertes pour les données signifient qu'une organisation peut se concentrer sur la fourniture de valeur à n'importe quel stade du cycle des données.

Avantages sociaux

Les normes de données ouvertes encouragent la collaboration entre plusieurs parties prenantes. Essentiellement, l'élaboration d'une norme utile à la communauté et utilisée par les parties prenantes nécessite une collaboration multipartite. La collaboration multipartite relie les personnes et les organisations travaillant dans un secteur. Les éditeurs de données souhaitent savoir qui d'autre publie des données en utilisant des normes, afin de comprendre comment les problèmes ont été résolus et d'améliorer leurs processus. Les utilisateurs de données souhaitent entrer en contact avec d'autres utilisateurs de données ayant des objectifs ou des problèmes similaires. Au cours de ce processus, une vision commune peut être développée (Open Data Institute, 2021). Lorsque des personnes et des organisations confrontées à un problème commun ou à un besoin non satisfait collaborent pour parvenir à un accord sur la production ou l'utilisation de données de meilleure qualité, les personnes et les organisations concernées ont besoin d'une vision commune des normes ouvertes, notamment d'une compréhension commune du problème qu'elles tentent de résoudre et d'un accord sur la manière dont elles vont le résoudre.[114]

Au cours du processus, une norme ouverte pour les données peut aider à coordonner les activités visant à comprendre le problème ou le besoin non satisfait ; à s'entendre sur l'écosystème actuel, les actifs de données, les concepts et le langage utilisés ; à s'entendre sur les données et les modèles nécessaires pour résoudre le problème ou répondre au besoin ; à mettre en commun les ressources pour travailler à la réalisation d'objectifs clairement définis pour la norme, ce qui mène à des activités se renforçant mutuellement ; établir des liens entre les secteurs pour soutenir les objectifs de la norme, ce qui peut contribuer à instaurer la confiance, l'apprentissage et le soutien par les pairs ; et produire et réutiliser des outils qui renforcent l'infrastructure des données, notamment en soutenant les éditeurs de données, en fournissant des informations aux utilisateurs de données et en facilitant la création d'outils et de services par les concepteurs.[115]

Impacts politiques

D'un point de vue politique, les normes ouvertes peuvent soutenir la mise en œuvre de la politique. Dans le passé, les décideurs politiques exigeant des organisations qu'elles publient des données se sont concentrés sur les données à publier, mais pas sur la manière de le faire. Cela conduit à des situations où la divulgation est généralisée, mais où les données sont difficiles à rassembler et à utiliser. En adoptant des normes ouvertes pour les données et en les reliant à la politique et à la réglementation, les décideurs politiques peuvent rendre les données plus utilisables, fournir des conseils clairs sur la façon de divulguer les données, automatiser les contrôles de conformité, l'agrégation des données et l'établissement de rapports. Les normes ouvertes pour les données apportent de la clarté aux éditeurs de données, la possibilité d'engager les parties prenantes et aident à garantir des résultats cohérents et comparables (Open Data Institute, 2021).

Avantages technologiques

Les principaux avantages technologiques des données ouvertes sont que les normes produisent des données de meilleure qualité.[116] Les normes ouvertes encouragent le développement d'outils et de services pour aider les éditeurs de données à produire des données de bonne qualité, notamment des outils pour valider, pré visualiser et comparer les données (Open Data Institute, 2021).

Les normes ouvertes peuvent conseiller les éditeurs de données sur la fréquence de publication des données. Certaines normes incluent des moyens de partager les calendriers de publication, les dates de publication, l'emplacement et les méthodes d'accès aux données. En partageant ces informations, il est plus facile de faire confiance aux données publiées.[117]

En outre, lorsque les données sont publiées de manière cohérente, le temps, le coût et les processus nécessaires à leur utilisation sont réduits. La publication cohérente encourage la création de nouveaux outils et services conçus pour tirer parti de données conformes à une norme.[118]

Exemple de normes de données ouvertes utilisées

La norme de données ouvertes la plus connue est probablement la General Transit Feed Specification (GTFS), qui est une norme développée par le géant technologique Google. La GTFS permet aux organismes de transport en commun de publier leurs données de transport dans un format qui peut être interprété et utilisé par une variété d'applications logicielles (GFTS, 2021). En raison de l'interopérabilité des normes de données ouvertes, les données GTFS peuvent être utilisées par de nombreuses autres applications logicielles tierces à des fins diverses. Citons par exemple la planification des trajets, la création d'horaires, les données mobiles, la visualisation des données, l'accessibilité, les outils d'analyse pour la planification et les systèmes d'information en temps réel (SMTG, 2021). Parmi les formats de données de transport public, le GTFS se distingue car il a été conçu pour répondre à des besoins spécifiques et pratiques de communication d'informations sur les services aux passagers. Il est conçu pour être relativement simple à créer et à lire, tant pour les personnes que pour les machines.[119] La valeur d'un système de transport efficace a des répercussions réelles sur l'économie d'un pays, mais comme il est si facile d'accéder aux données et de les partager de cette manière, l'efficacité est amplifiée même au-delà des frontières.

Préoccupations liées à la cyber sécurité

La circulation des données comporte des risques considérables en matière de sécurité, d'où la nécessité de la cyber sécurité et de la protection des données tant personnelles que non personnelles. Comme indiqué ci-dessus, la Convention de Malabo est le seul instrument juridique continental actuel qui se concentre sur la protection des données personnelles et la cyber sécurité. Elle est pertinente

pour la gouvernance des données dans la mesure où elle se rapporte à ces deux aspects, qui font partie intégrante de la gouvernance des données. En effet, comme indiqué ci-dessus, la CUA supervise le développement et la formulation du Cadre de politique des données pour l'Afrique, qui s'inspire, en partie, de la Convention de Malabo. Un cadre de gouvernance des données bien conçu doit inclure ces deux aspects car " la sécurité et la confidentialité sont devenues l'une des préoccupations majeures liées au stockage et à l'utilisation des données au sein des organisations " (Yang et al., 2019). Avant l'adoption de la Convention de Malabo en 2014, plusieurs CER ont adopté des instruments réglementaires sur la confidentialité et la cyber sécurité (Ncube, 2016). Il s'agit de : De la loi supplémentaire de la CEDEAO sur la protection des données personnelles au sein de la CEDEAO (2010) ; de la directive de la CEDEAO sur la lutte contre la cybercriminalité (2011) ; du projet de loi type sur la cybercriminalité du Marché commun de l'Afrique orientale et australe (COMESA) (2011) ; de la loi type sur la protection des données de la Communauté de développement de l'Afrique australe (SADC) et d'une loi type sur la criminalité informatique et la cybercriminalité (2012). Parmi ces textes, seul le modèle de la SADC couvre à la fois la confidentialité et la sécurité, mais comme il s'agit d'un instrument non contraignant, la Convention de Malabo est le seul instrument contraignant qui réglemente à la fois la confidentialité et la sécurité. En outre, selon son préambule, elle « incarne les engagements existants des États membres de l'UA aux niveaux sous régional, régional et international pour construire la société de l'information », ce qui en fait le modèle continental. En conséquence, cette section reprend les dispositions de la Convention de Malabo sur la cyber sécurité et la confidentialité. Comme indiqué ci-dessus, cette section est succincte, en raison de la couverture du même contenu, de manière plus détaillée, par un autre document qui fait partie du projet.

Confidentialité

Comme indiqué ci-dessus, la Convention de Malabo se concentre sur la protection des données personnelles (vie privée) plutôt que sur les données non personnelles. Sa disposition relative aux définitions énonce les définitions fondamentales suivantes:

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable par laquelle cette personne peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Fichier de données personnelles : tout ensemble structuré de données accessibles selon des critères déterminés, que ces données soient ou non centralisées, décentralisées ou réparties fonctionnellement ou géographiquement.

Données sensibles : toutes les données personnelles relatives aux opinions et activités religieuses, philosophiques, politiques et syndicales, ainsi qu'à la vie sexuelle ou à la race, à la santé, aux mesures sociales, aux procédures judiciaires et aux sanctions pénales ou administratives.

Elle aborde ensuite la réglementation du traitement des données à caractère personnel qui se définit comme suit :

> toute opération ou ensemble d'opérations effectuées ou non à l'aide de moyens automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison et le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel.

Le point central de cette réglementation est constitué par les principes de base régissant le traitement des données à caractère personnel, tels qu'énoncés à l'article 13. Ces principes sont les suivants

Principe 1 : Principe du consentement et de la légitimité du traitement des données à caractère personnel.

Principe 2 : Principe de légalité et de loyauté du traitement des données à caractère personnel

Principe 3 : principe de finalité, de pertinence et de conservation des données à caractère personnel traitées

Principe 4 : Principe d'exactitude des données à caractère personnel

Principe 5 : Principe de transparence du traitement des données à caractère personnel

Principe 6 : Principe de confidentialité et de sécurité du traitement des données à caractère personnel

Leur signification est la même que celle des principes du GDPR tels qu'énoncés à la section 2 ci-dessus. Ils sont complétés par l'article 14, qui énonce des principes spécifiques pour le traitement des données sensibles. Un autre élément essentiel de la protection de la vie privée dans la Convention de Malabo est sa section IV sur les droits suivants des personnes concernées : Droit à l'information (article 16) ; droit d'accès (article 17) ; droit d'opposition (article 18) et droit de rectification ou

d'effacement (article 19). Les Responsables du traitement des données personnelles ont les obligations suivantes : Devoirs de confidentialité (article 20) ; de sécurité (article 21) ; de stockage (article 22) et de pérennité (article 23).

Cyber sécurité

La Convention de Malabo ne dispose pas d'une définition de la cyber sécurité, qui aurait été utile pour étayer un aspect important qu'elle réglemente. Yang et al. (2019) définissent la cyber sécurité comme « la pratique consistant à protéger les infrastructures informatiques et de réseau, les systèmes d'exploitation, les programmes logiciels exécutés sur les infrastructures, et toutes les données stockées ou transmises par l'intermédiaire des infrastructures contre les attaques numériques et toute autre utilisation abusive » (Yang et al., 2019). Le chapitre trois de la Convention vise à promouvoir la cyber sécurité et à prévenir la cybercriminalité. L'article 24 traite des cadres nationaux de cyber sécurité, plus précisément des politiques et stratégies nationales relatives aux infrastructures d'information critiques (IIC). La Convention de Malabo définit la CII comme « la cyber infrastructure qui est fondamentale pour les services vitaux pour la sécurité publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la durabilité et la restauration du cyberespace critique ».

L'article 25 aborde ensuite les mesures juridiques, à savoir : (1) la législation nationale sur la cybercriminalité ; (2) les autorités de régulation ; (3) les droits des citoyens ; et (4) la protection des infrastructures critiques. Selon l'article 25.1, la législation nationale sur la cybercriminalité doit sanctionner efficacement « les actes criminels qui portent atteinte à la confidentialité, à l'intégrité, à la disponibilité et à la survie des systèmes de technologies de l'information et de la communication, aux données qu'ils traitent et à l'infrastructure de réseau sous-jacente ». Les données sont expressément mentionnées ici, de sorte que certaines mesures nationales de cyber sécurité relatives aux données sont obligatoires. En outre, l'article 25.2 exige "des mesures procédurales efficaces pour poursuivre les auteurs d'infractions".

L'article 26 exige ensuite des États parties qu'ils mettent en place un système national de cyber sécurité comprenant les institutions nécessaires, dotées du personnel adéquat, pour superviser la mise en œuvre des mesures juridiques par le biais d'actions, y compris la réponse aux incidents de cyber sécurité, la coordination et la coopération dans les enquêtes et les poursuites judiciaires, entre autres. Ces mesures juridiques et leur mise en œuvre doivent tenir dûment compte des droits de l'homme des citoyens.[120] Les États parties sont également tenus d'établir des mesures législatives ou réglementaires pour protéger les secteurs prioritaires qui sont importants pour la sécurité nationale, par exemple en introduisant des sanctions plus sévères pour les infractions dans ces secteurs.[121]

L'article 26 fournit quelques détails supplémentaires concernant le système national de cyber sécurité en donnant mandat à chaque État de "promouvoir la culture de la cyber sécurité" et suggère des mesures qui peuvent inclure des plans de

cyber sécurité et des campagnes de sensibilisation. L'article 27 traite des structures nationales de surveillance de la cyber sécurité, que les États parties sont tenus d'adopter pour la gouvernance de la cyber sécurité dans un cadre national. L'article 28 prévoit une coopération internationale grâce à l'harmonisation, en encourageant les États à s'offrir une assistance juridique mutuelle et l'échange d'informations, ainsi que l'utilisation des moyens existants pour la coopération internationale. L'article 29 prévoit ensuite des infractions spécifiques aux TIC. Il impose aux Etats parties de créer des infractions relatives aux attaques contre les systèmes informatiques, par exemple pour obtenir un accès non autorisé, et aux violations de données telles que l'interception ou la tentative d'interception de données informatisées. Il existe également des dispositions relatives aux infractions liées au contenu à l'article 29 et à l'adaptation des infractions et des sanctions en matière de propriété aux TIC aux articles 30-31, mais elles ne sont pas pertinentes pour le domaine d'intérêt du chapitre.

Les dispositions de la Convention de Malabo constituent une base de référence, mais il faut aller plus loin pour adopter une approche solide de la protection de la vie privée et de la sécurité des données non personnelles, car ses dispositions relatives à la protection de la vie privée concernent essentiellement les données personnelles et ses dispositions relatives à la cyber sécurité mettent l'accent sur l'infrastructure nationale ou la CII.

En résumé, cette section montre que la plupart des États africains doivent créer, améliorer ou renforcer leurs cadres de protection de la vie privée et de cyber sécurité. Étant donné que la ZLECAf et la stratégie de transformation numérique ont pour objectif de faciliter et de développer le commerce électronique et numérique en Afrique, il sera important d'aligner les cadres nationaux. Cela donne une certaine certitude aux entrepreneurs qui font du commerce dans plusieurs juridictions. Comme indiqué ci-dessus, et renforcé ci-dessous, les négociations du protocole de commerce électronique de la ZLECAf fourniront une plateforme pour convenir des principes fondamentaux de gouvernance des données.

4. Conclusion

Cette étude montre en partie qu'une ou deux choses se passent sur le continent. D'une part, les efforts continentaux concertés se déroulent lentement alors que la révolution des données se déroule à un rythme beaucoup plus rapide. Parce que c'est le cas, les nations progressistes, dans une tentative de concurrencer dans l'économie des données, ont choisi de tenter la gouvernance des données par elles-mêmes, offrant ainsi la situation actuelle de lois discordantes et éventuellement conflictuelles sur la réglementation des données. D'un autre côté, il se peut que nous soyons témoins d'un manque de confiance entre les États africains dans les efforts de réglementation unifiée. Dans certains cas, étant donné que les données qui ont la plus grande valeur sont personnelles, un tel manque de confiance peut être associé à la paranoïa et à la suspicion de la plupart des individus. Il est donc impératif de mettre en place le plus rapidement possible un environnement de données de confiance fondé sur l'État de droit, des dispositions institutionnelles et des réglementations complètes, ainsi que des institutions compétentes chargées de superviser l'utilisation des données publiques et privées.

Un tel environnement peut être créé à travers des efforts multipartites visant à améliorer l'accès aux données et leur utilisation. Cela peut signifier un dialogue actif entre les gouvernements, des consultations et des collaborations avec le secteur privé, et la mise en place d'autorités de protection des données (APD) compétentes pour les enquêtes et les poursuites en cas de violations transfrontalières. En tête de l'ordre du jour du dialogue intergouvernemental devrait figurer la négociation d'accords d'assistance mutuelle qui garantiront une protection similaire des données dans les États membres contractants et des engagements à enquêter et à poursuivre les cybercriminalités transfrontalières de manière exhaustive.[122] Cela contribuera largement à atténuer les préoccupations liées à la libre circulation des données. En outre, étant donné que la plupart des États africains sont encore en phase de développement, certains étant plus avancés que d'autres, le renforcement des capacités en matière de protection des données, de cyber sécurité et de gouvernance institutionnelle des données dans les organismes concernés doit être privilégié et réalisé par le biais de l'allocation des politiques et des ressources. En outre, lorsque des dispositions institutionnelles et des réglementations voient le jour à la suite de consultations et d'un dialogue, ces dispositions doivent être établies dans le cadre de processus inclusifs, consultatifs et transparents. La redevabilité et la transparence

répondent à la plupart des préoccupations qui suivent le passage à la libéralisation et à l'utilisation des données.

Comme indiqué au point 2 ci-dessus, il est important de souligner que les données personnelles et non personnelles ne doivent pas être traitées de la même manière, d'où l'existence d'approches distinctes dans d'autres parties du monde. Si les préoccupations relatives à la protection et à la réglementation des données personnelles sont légitimes, les données non personnelles, qui ont une grande valeur en soi, ne devraient pas faire l'objet du même examen. À cet égard, des leçons peuvent être tirées de l'approche adoptée par l'UE pour assurer la distinction entre les deux (voir les leçons clés décrites à la section 2.1 ci-dessus).

La situation actuelle, telle que résumée à la section 3 ci-dessus, confirme que la plupart des tentatives des pays africains pour réglementer les données se sont trop préoccupées des données personnelles, négligeant les données non personnelles. De même, les données personnelles ayant une valeur plus élevée, il n'est pas surprenant que les lois de protection à cet égard puissent être excessives. Si les formes actuelles de lois sur la localisation des données peuvent être considérées comme des tentatives des gouvernements nationaux d'affirmer leur souveraineté sur les données, un moyen de communication sans frontières, la réalité est qu'à mesure que de plus en plus de pays adoptent des cadres actualisés de protection des données, il est fort probable que certains décideurs proposeront des lois plus strictes sur la localisation des données, car ils estiment que la meilleure façon de protéger les données est de les stocker à l'intérieur des frontières d'un pays. Cependant, il est prouvé que la sécurité des données ne dépend pas de l'endroit où elles sont stockées. Au contraire, en autorisant la libre circulation des données à travers les frontières internationales, les problèmes de cyber sécurité sont moins susceptibles de se matérialiser. En permettant aux fournisseurs de services en nuage de s'appuyer sur des flux de données provenant de partout, ils seront en mesure d'établir les meilleures pratiques en matière de cyber sécurité. De même, si l'informatique dématérialisée ne garantit pas la sécurité, elle conduira à une meilleure sécurité, car la mise en œuvre d'un programme de sécurité solide nécessite des ressources et une expertise dont beaucoup d'organisations et de pays africains sont dépourvus. Mais les fournisseurs de l'informatique en nuage à grande échelle sont mieux placés pour offrir cette protection. En fait, la sécurité des données dépend principalement des contrôles logiques et physiques utilisés pour les protéger, tels qu'un cryptage fort sur les appareils et un périmètre de sécurité pour les centres de données. La nationalité de la personne qui possède ou contrôle les serveurs ou le pays dans lequel ces dispositifs sont situés n'a pas grand-chose à voir avec le niveau de sécurité. Par conséquent, étant donné les avantages potentiels que des flux transfrontaliers ouverts apporteraient, il serait prudent de commencer à aligner la politique sur la promotion de flux de données transfrontaliers ouverts. En outre, étant donné qu'un régime complet de données prévoit également la souveraineté des données, la spécificité des données devrait également être une priorité. Par spécificité des données, on entend la capacité des pays à préciser quels types de données peuvent ou ne peuvent pas circuler librement. La spécificité des

données doit être privilégiée afin d'éviter des restrictions involontaires au partage productif des données.

Alors que la ZLECAf et la stratégie de transformation numérique pour l'Afrique (2020-2030) cherchent à accroître le commerce électronique et le commerce numérique en Afrique, il est important d'examiner comment le soutien à la libre circulation des données en Afrique peut renforcer ces efforts. Il a été démontré que les flux de données transfrontaliers sont déterminants et ont le potentiel d'influencer grandement une nouvelle résurgence économique pour le continent, comme on peut le tirer des expériences des pays ou des organismes régionaux qui ont adopté une approche libérale de la réglementation des données. Leur expérience a démontré que la localisation des données ne sert pas l'objectif que beaucoup pensent qu'elle poursuit et qu'en fait, elle pourrait être considérée comme contre-productive en termes de sécurisation et de valorisation des données. La plupart des pays africains qui ont adopté des lois sur la localisation des données d'une manière ou d'une autre l'ont fait sous prétexte que la sécurité des données dépend de l'endroit où elles sont stockées ou collectées, ce qui est en fait une erreur. Il a été démontré que les politiques ouvertes en matière de flux de données transfrontaliers ont généré de meilleures mesures de sécurité et de meilleurs revenus pour les pays qui ont adopté ces systèmes. Le continent africain peut dès à présent s'inspirer de ces expériences pour soutenir de manière adéquate la libre circulation des données. Il est également nécessaire de souligner que l'adoption de normes ouvertes pour les données, qui compléteront les flux de données transfrontaliers, garantira que ces flux sont effectués de manière sûre et transparente et que les obstacles à l'accès à l'économie des données sont réduits, encourageant ainsi davantage d'acteurs à s'impliquer dans l'économie des données. En adoptant des normes de données ouvertes et en décentralisant le pouvoir de collecte, d'utilisation et d'agrégation des données, la participation à l'économie des données est encouragée et les risques d'utilisations illégitimes des données sont réduits. Dans ce processus, les gouvernements ont également la possibilité de travailler et de renforcer leur impact dans des domaines clés tels que la politique, la technologie et le développement et l'économie. Une telle approche reconnaît l'importance de la cyber sécurité et la soutient au sein d'un écosystème qui encourage la participation aux données ouvertes.

Finalement, il faudrait adopter une approche juridique cohérente, sans ambiguïté, qui offre une protection et des obligations sur tout le continent, tout en tenant compte de la valeur de la libéralisation des données. À l'avenir, les instruments juridiques existants devraient être révisés régulièrement, si nécessaire, afin d'éliminer les conflits de lois et de se tenir au courant des derniers niveaux de protection et d'obligations au sein des États membres.

Remarques

1. Ce travail est basé sur une recherche soutenue en partie par la Fondation nationale de recherche (NRF) d'Afrique du Sud (numéro de subvention : 115716). Toute opinion, observation, conclusion ou recommandation exprimée dans ce document est celle des auteurs et la NRF n'accepte aucune responsabilité à cet égard.

2. Glossaire de l'OCDE sur les termes statistiques "données" disponible sur https://stats.oecd.org/glossary/detail.asp?ID=532 consulté le 28/04/2021.

3. Ibid.

4. Math is fun what is data disponible sur https://www.mathsisfun.com/data/data.html consulté le 28/04/2021.

5. Diffen 'Données vs Information' disponible sur https://www.diffen.com/difference/Data_vs_Information consulté le 28/04/2021.

6. Ibid.

7. Ibid at 2.

8. Art 4(1) of the GDPR

9. "Données personnelles" (Règlement général sur la protection des données (RGPD) <https://gdpr-info.eu/issues/personal-data/> consulté le 17 janvier 2022.

10. ibid.

11. Expliqué : Qu'est-ce que les données non personnelles ? (The Indian Express, 27 juillet 202).0) <https://indianexpress.com/article/explained/non-personal-data-explained-6506613/> accessed 17 January 2022.

12. Privacy International 2020 est une année importante de lutte pour la protection des données en Afrique 3 mars 2020 disponible à l'adresse suivante : https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa consulté le 30/04/2021.

13. Le règlement général sur la protection des données 2016/679.

14. Ibid.

15. Research ICT Africa (RIA) Consultation en ligne : Appel à contributions sur le cadre stratégique pour les données en Afrique 17 Juillet 2021 https://researchictafrica.net/2021/07/17/online-consultation-call-for-submissions-africa-data-policy-framework/

16. Stratégie de transformation numérique de l'Union africaine pour l'Afrique 2020 - 2030 disponible à l'adresse suivante https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

17. Union africaine, 2020. Décision sur la zone de libre-échange continentale africaine (ZLECAf). Assembly /AU/Dec.751(XXXIII). https://www.tralac.org/documents/resources/cfta/3176-au-assembly-decision-on-the-afcfta-february-2020/file.html

18. Les négociations de l'OMC sur le commerce électronique progressent, en vue d'une déclaration à la 12e Conférence ministérielle. https://www.wto.org/english/news_e/news21_e/ecom_10nov21_e.htm

19. Patrick Breyer v Bundesrepublik Deutschland Case C-582/12.

20. Bird et Bird " Économie des données de l'UE : Questions juridiques, éthiques et sociales liées aux données", disponible à l'adresse suivante https://www.twobirds.com/~/media/pdfs/eu-data-economy-legal-ethical--social-issues.pdf. Consulté le 30/04/2021.

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid.

25. Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 concernant un cadre pour la libre circulation des données à caractère non personnel dans l'Union européenne, JO L 303..

26. Bird and Bird supra note 20.

27. Étant donné qu'un autre document de ce projet examine en détail la Convention de Malabo et les instruments réglementaires nationaux et communautaires en matière de protection des données, le présent document traite ces aspects de manière brève et succincte afin de minimiser les chevauchements et les répétitions..

28. Règlement (UE) 2018/1807 relatif à un cadre pour le flux libre des données non personnelles dans l'UE.

29. Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

30. Le règlement général sur la protection des données, supra note 13.

31. Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cyber sécurité) et à la certification en matière de cyber sécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (loi sur la cyber sécurité).

32. https://op.europa.eu/en/publication-detail/-/publication/ac9cd214-53c6-11ea-aece-01aa75ed71a1/language-en

33. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

34. Article 2.1. GDPR Supra note 13.

35. " [c'est-à-dire] celle qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques de l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique " (article 4.1 du RGPD) y compris les quasi-identifiants et les métadonnées (article4.1.).

36. Règlement FFD, supra note 28.

37. Article 2.1. du règlement FFD supra note 28..

38. https://medium.datadriveninvestor.com/digital-europe-200-billion-investment-strategies-for-artificial-intelligence-data-and-blockchain-f7f656e66603.

39. L'article 1(3) du GDPR indique que l'objectif primordial du GDPR est de garantir que "la libre circulation des données à caractère personnel au sein de l'Union n'est ni restreinte ni interdite pour des raisons liées à la protection des personnes physiques à l'égard du traitement des données à caractère personnel."

40. Voir chapitre 2 (Art 5 à 11) du GDPR .

41. https://openknowledge.worldbank.org/bitstream/handle/10986/34139/9781464815591.pdf

42. https://au.int/sites/default/files/documents/33126-doc-01_background_note.pdf

43. Ibid.

44. Lois sur la protection des données et la confidentialité | identification pour le développement https://id4d.worldbank.org/guide/data-protection-and-privacy-laws.

45. Banque mondiale "Créer de la valeur dans l'économie des données .

46. GSMA " Flux de données transfrontaliers : Concrétiser les avantages et supprimer les obstacles" disponible à l'adresse https://www.gsma.com/publicpolicy/resources/cross-border-data-flows-realising-benefits-and-removing-barriers

47. Voir note 9, Russom, Philip. " Gérer le big data ". (2013) Rapport sur les meilleures pratiques de TDWI, TDWI Research, à la page 5..

48. GSMA " Flux de données transfrontaliers

49. Analystes, secteur de la dotation en personnel. "Le cloud humain, la gig economy & la transformation du travail". (2017). Disponible à l'adresse suivante https://www2.staffingindustry.com/content/download/246507/9128496/HumanCloudSummary2017_170912.pdf

50. Ibid.

51. GSMA " Flux de données transfrontaliers

52. Ibid.

53. Ibid.

54. Ibid.

55. Ibid.

56. Ibid.

57. Ibid.

58. LOI n° 2013 450 du 19 juin 2013 sur la protection des données personnelles disponible à l'adresse suivante https://ictpolicyafrica.org/fr/document/4wo0y6uby6j

59. La loi sur la protection des données n° 24 de 2019..

60. Section 44 de la loi lue avec la section 25.

61. Article 25(h) de la loi .

62. Supra note 59.

63. Règlement (général) sur la protection des données, 2021, disponible à l'adresse suivante https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

64. Règlement sur la protection des données (enregistrement des contrôleurs et des responsables du traitement des données), 2021, disponible à l'adresse suivante https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/

65. Règlement sur la protection des données (conformité et application), 2021, disponible à l'adresse suivante https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021/

66. Règlement 25(1)(a) du Règlement général sur la protection des données .

67. Règlement 25(1)(b) du Règlement général sur la protection des données .

68. Règlement 38(1)(a) du Règlement général sur la protection des données .

69. Règlement 38(2) du Règlement général sur la protection des données .

70. Règlement 38(1)(b) du règlement général sur la protection des données .

71. Règlement 38(1)(c) du règlement général sur la protection des données .

72. Article 38(1)(d) du règlement général sur la protection des données.

73. Règlement 40(1)(a) du règlement général sur la protection des données. .

74. Règlement 40(1)(b) du règlement général sur la protection des données .

75. Règlement 40(1)(c) du règlement général sur la protection des données .

76. Règlement 40(1)(d) du règlement général sur la protection des données .

77. Règlement 39 du règlement général sur la protection des données

78. Lignes directrices pour le développement de contenu nigérian dans les technologies de l'information et de la communication (TIC) de 2015 et telles que modifiées en août 2019. Disponible sur https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf

79. Section 11.1.3 des lignes directrices pour le développement du contenu nigérian dans le domaine des TIC. .

80. Section 12.1.4 des lignes directrices pour le développement du contenu nigérian dans le domaine des TIC.

81. Section 13.1.2 et 13.2.3 des lignes directrices pour le développement du contenu nigérian dans le domaine des TIC.

82. Les directives obligatoires de 2011 de la Banque centrale du Nigeria sur les services d'acceptation des cartes aux points de vente (POS) sont disponibles à l'adresse suivante https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf

83. Directive 4.4.8 des directives obligatoires 2011 de la Banque centrale du Nigeria sur les services d'acceptation des cartes aux points de vente (POS).

84. Article 17 de l'arrêté ministériel N°001/MINICT/2012 disponible à l'adresse suivante https://www.rlrc.gov.rw/fileadmin/user_upload/LawsofRwanda/Laws%20of%20Rwanda/7._Administrative/5.9.%20State%20Finance/5.9.3.%20Procurement/5.9.3.3._M._Instructions_Procurement_of_ICT_goods_and_services_by_public_institutions.pdf

85. Cory N, Dascoli L " Comment les barrières aux flux de données transfrontaliers se répandent dans le monde, ce qu'elles coûtent, et comment les résoudre " Fondation pour la technologie de l'information et l'innovation Disponible sur le site https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

86. La loi sur la protection des informations personnelles n° 4 de 2013 disponible à l'adresse suivante https://popia.co.za/

87. Article 72(1)(a) de la loi POPI .

88. Article 72(1)(b) de la loi POPI .

89. Article 72(1)(c) de la loi POPI .

90. Article 72(1)(d) de la loi POPI .

91. Article 72(1)(e) de la loi POPI .

92. Cory N, Dascoli L Supra Note 85.

93. Le projet de politique nationale sur les données et le nuage est disponible à l'adresse suivante https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

94. "Infrastructure nationale d'information critique", telle que définie dans la section 9 de la politique, désigne tous les systèmes de TIC, les systèmes de données, les bases de données, les réseaux (y compris les personnes, les bâtiments, les installations et les processus), qui sont fondamentaux pour le fonctionnement efficace de la République d'Afrique du Sud.

95. Intervention politique 10.4.1.

96. Intervention politique 10.4.4. du projet de politique nationale sur les données et le cloud.

97. La loi sur la protection des données personnelles (loi n° 151 de 2020).

98. Article 14 de la loi sur la protection des données de 2020

99. La nouvelle loi égyptienne sur les données favorise la localisation des centres de données (/ Journal quotidien..., 5 août 2020) <https://www.datacenterplanet.com/data-center/egypt-new-data-law-supports-data-center-localization/> consulté le 11 novembre 2021.

100. La loi sur la protection des données (loi 22/11)

101. Section VI de la loi sur la protection des données

102. Article 34 de la loi sur la protection des données

103. La définition des normes de données ouvertes (Open Data Standards Directory) est disponible sur le site https://datastandards.directory/ consulté le 28/08/2021.

104. https://aims.gitbook.io/open-data-mooc/unit-4-sharing-open-data/lesson-4.2-introduction-to-data-interoperability

105 "Quand utiliser les normes ouvertes pour les données" Open Data Institute, 2021.

106. Ibid.

107. Ibid.

108. Ibid.

109. L'infrastructure de données consiste en des actifs de données soutenus par des personnes, des processus et des technologies .

110. Quand utiliser les normes ouvertes pour les données" Open Data Institute, 2021.

111. Les avantages économiques des données ouvertes. Disponible sur https://data.europa.eu/en/highlights/economic-benefits-open-data consulté le 09/10/2021.

112. Ibid.

113. Ibid

114. Ibid.

115. Ibid.

116. Dans son livre "Executing Data Quality Projects", Danette McGilvray définit la qualité des données comme "le degré de fiabilité des données pour toute utilisation requise".

117. Ibid.

118. Ibid.

119. Ibid.

120. Article 25.3.

121. Article 25.4.

122. Chapitre 7 du GDPR

Références

Bowman, C. 2017. “Data localization laws: An emerging global trend”. *Jurist*, 6 January 2017. Available at https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/.

Ncube, Caroline B. 2016. “Recent developments in African regulation of cybercrime: An overview of proposed changes to the South African framework”. *Journal of Internet Law*, 19(7): 3–20.

Chaytor, Batrice. 2020. AfCFTA: An enabler of digital trade and e-commerce. Available at https://resilient.digital-africa.co/en/blog/tech_voices/afcfta-an-enabler-of-digital-trade-and-e-commerce-1-4/.

CNBC Africa. 2017. “Rwanda utilities regulatory authority fines MTN US$ 8,5M‘ 17 May 2017. Available at https://www.cnbcafrica.com/2017/rwanda-utilities-regulatory-authority-fines-mtn-us-85m-non-compliance/.

GTFS. 2021. Making public transit data universally accessible. Available at https://gtfs.org/ accessed 10/10/2021 GTFS (2021): Making Public Transit Data Universally Accessible available at https://gtfs.org/ accessed 10/10/2021.

Jean-Francois Le Bihan. 2018. Regional regulatory capacity building. GSMA Africa Policy Day 16 July 2018. Available at https://www.gsma.com/publicpolicy/wp-content/uploads/2018/07/M360-Africa-Policy-Day-Presentation.pdf accessed on 11/11/2021.

Jeremy, Daniel. 2021. Data protection laws in Africa: What you need to know. CIO Africa 15 February 2021. Available at https://www.cio.com/article/3607734/data-protection-laws-in-africa-what-you-need-to-know.html?upd=1619734077195 accessed on 29/04/2021.

Manzo, Valentina. 2019. The internet of things and intellectual property rights: The protection of data 2019 WIPO Academy, University of Turin and ITC-ILO - Master of Laws in IP - Research Papers Collection - 2017–2018 Available at SSRN: https://ssrn.com/abstract=3387417 at 1.

Okonjo-Iweala, Ngozi. 2021. Remarks at the Centre for the Study of the Economies of Africa (CSEA)’s webinar on data governance in Africa: Pathways for strengthening confidence in the digital economy, 11 August 2021 https://www.youtube.com/watch?v=Vnvh2JZx8PA.

Open Data Institute. 2021. What are open standards for data? Available at https://standards.theodi.org/introduction/what-are-open-standards-for-data/ Accessed 28/08/2021.

Russom, Philip. 2013. Managing big data. TDWI best practices report, TDWI Research at 5.

Swinhoe, D. 2021. Senegal to migrate all government data and applications to new government data center. Data center dynamics, June 23 2021. Available at https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/.

World Bank. 2021. Creating value in the data economy: The role of competition, trade, and tax policy. World Development Report 2021: Data for better lives. March 24, 2021 available at https://www.worldbank.org/en/publication/wdr2021.

Yang, L., Li, J., Nko, N., Prickett, T.,Chao, F. 2019. "Towards big data governance in cybersecurity". *Data-Enabled Discovery*, Appl. 3, 10 (2019). https://doi.org/10.1007/s41688-019-0034-9 at 1.

Mission

Renforcer les capacités des chercheurs locaux pour qu'ils soient en mesure de mener des recherches indépendantes et rigoureuses sur les problèmes auxquels est confrontée la gestion des économies d'Afrique subsaharienne. Cette mission repose sur deux prémisses fondamentales.

Le développement est plus susceptible de se produire quand il y a une gestion saine et soutenue de l'économie.

Une telle gestion est plus susceptible de se réaliser lorsqu'il existe une équipe active d'économistes experts basés sur place pour mener des recherches pertinentes pour les politiques.

www.aercafrica.org/fr

Pour en savoir plus :

www.facebook.com/aercafrica

www.instagram.com/aercafrica_official/

twitter.com/aercafrica

www.linkedin.com/school/aercafrica/

Contactez-nous :
Consortium pour la Recherche Économique en Afrique
African Economic Research Consortium
Consortium pour la Recherche Économique en Afrique
Middle East Bank Towers,
3rd Floor, Jakaya Kikwete Road
Nairobi 00200, Kenya
Tel: +254 (0) 20 273 4150
communications@aercafrica.org