Régime Juridique de Protection des Données et Gouvernance des Données en Afrique : Une Vue d'Ensemble

Olumide Babalola

Documents de travail DG-003

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

Régime Juridique de Protection des Données et Gouvernance des Données en Afrique : Une Vue d'Ensemble

Par

Olumide Babalola[1]
Université de Portsmouth,
Royaume-Uni

CREA Document de Travail DG-003
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

Dans sa définition la plus simple, la gouvernance des données fait référence à la gestion globale des données (personnelles et non personnelles) pour faciliter la réalisation des objectifs organisationnels. La protection des données, quant à elle, régit principalement la gestion des données personnelles pour la protection globale de la confidentialité des utilisateurs et d'autres droits et libertés fondamentaux. La quatrième révolution industrielle a considérablement augmenté le traitement des données personnelles à des fins commerciales et sociales en Afrique, d'où la nécessité imminente de réglementer le traitement de ces informations personnelles à des fins indésirables en mettant en place des cadres juridiques pertinents pour traiter les effets défavorables sur les humains, dont les informations personnelles sont utilisées à des fins diverses. Cette étude analyse le cadre juridique régional relatif à la protection des données en Afrique à la lumière de ses principales dispositions, de son adéquation, de son efficacité et de son applicabilité en matière de gouvernance des données sur le continent. Le document établit une juxtaposition avec le Règlement général sur la protection des données de l'Union européenne en ce qui concerne son impact distant ou immédiat sur la législation africaine en matière de protection des données. La recherche met en évidence les insuffisances du cadre juridique de la protection des données et l'absence de mécanisme pour les transferts transfrontaliers de données personnelles, qui devraient être réglementés par les autorités de protection des données (APD) existantes en Afrique. La recherche conclut ensuite avec quelques incitations à la protection des données dans le contexte de la gouvernance des données sur le continent.

Mots-clés : *protection des données, gouvernance des données, GDPR, Convention de Malabo, données personnelles.*

1. Introduction

Vue d'ensemble

La protection des données aurait fait son apparition en Europe en 1970, lorsque l'État fédéral allemand de Hesse (Mayer-Schonberger, 1997) a promulgué sa loi sur la protection des données, qui a été suivie par la loi suédoise sur les données nationales en 1973 (Oman, 2010). En Afrique, la République du Cap-Vert a ouvert la voie en 2001 en promulguant la première loi sur la protection des données en Afrique. La loi capverdienne sur la protection des données a été adoptée le 22 janvier 2001 afin de créer un cadre juridique pour la protection des données personnelles dans le pays (Makulilo, 2012).

Contrairement à l'Europe, où les États membres ont transposé les dispositions des instruments internationaux régionaux dans leurs diverses législations municipales sur la protection des données, le Cap-Vert s'est fortement appuyé sur la loi portugaise sur la protection des données, qui a elle-même transposé la directive européenne 95/46/CE sur la protection des données[2] avant qu'il ne soit remplacé par le règlement général sur la protection des données de l'UE -GDPR (Traca, et Embry, 2011). Entre 2001 et 2014, lorsque le premier et unique traité international panafricain sur la protection des données a été adopté en Guinée équatoriale,[3] 14 pays africains[4] avaient déjà promulgué leurs lois respectives sur la protection des données sans pouvoir s'inspirer de la convention, car la plupart de ces lois étaient calquées sur le cadre juridique européen en matière de protection des données (Greenleaf et Cottier, 2018).

Dans une approche descriptive, cet article examine les principaux instruments internationaux qui réglementent la protection des données en Afrique en décrivant brièvement les événements qui ont abouti à leur adoption, ainsi que leurs buts et objectifs. Il analyse également les principales dispositions de ces instruments à la lumière de leur applicabilité et de la mesure dans laquelle elles ont permis de mieux faire respecter la protection des données sur le continent. Ce document analyse ensuite la corrélation entre la protection des données et la gouvernance des données en Afrique dans le contexte des instruments régionaux, et il conclut sur la nécessité d'un cadre juridique pour la protection des données dans le cadre de la gouvernance des données en Afrique, avec quelques recommandations qui pourraient être adoptées pour développer de nouveaux cadres de protection des données ou renforcer les cadres existants, en particulier dans le cadre de la gouvernance des données.

Questions de recherche

Cette étude, de manière descriptive et normative, pose et analyse un certain nombre de questions, ainsi :

(i) Quelles sont les lois ou les directives quasi-juridiques (cadre juridique) qui réglementent ou soutiennent la protection des données en Afrique ?

(ii) Comment ce cadre juridique se mesure-t-il aux normes internationales ?

(iii) Dans quelle mesure ce cadre est-il appliqué ou mis en œuvre sur le continent ?

(iv) De quelle manière ce cadre influence-t-il ou devrait-il influencer la gouvernance des données en Afrique ?

(v) Quelles sont les incitations à la protection des données et à la gouvernance des données sur le continent ?

2. Cadre juridique sur la protection des données en Afrique

Unlike what is obtainable in the European Union (EU) where the General Data Protection Regulation (GDPR) provides some sort of formidable harmonization of the erstwhile irregular data protection laws across the Union, its African counterpart does not have a Pan-African legislation that is immediately enforceable across board without domestication. This is not, however, to say that Africa does not have an existing legal framework on data protection; the elephant in the room remains the institutional capacity and political will to enforce the available instruments. This paper discusses the extant legal framework for data protection on the continent.

Convention de l'Union Africaine sur la cyber sécurité et la protection des données personnelles 2014 (Convention de Malabo)

Les conversations autour de la réglementation du cyberespace ont effectivement commencé à la fin des années 1990, lorsque le comité de l'Assemblée générale des Nations unies a envisagé un instrument sur " le désarmement et la sécurité internationale ", dont les délibérations ont été menées par un projet de résolution présenté par la Russie en 1998 (Kavanagh, 2017). Sur la proposition de la Russie, les Nations unies ont ensuite constitué un groupe d'experts gouvernementaux (GGE) impliqué dans les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale.

Dans l'un de ses rapports,[5] le GGE note que : " L'utilisation des TIC dans les conflits futurs entre États devient plus probable, le risque d'attaques nuisibles des TIC contre les infrastructures critiques est à la fois réel et sérieux, et les États s'inquiètent à juste titre du danger de déstabilisation des perceptions erronées, du potentiel et de l'économie découlant de la difficulté d'attribuer la source d'un incident lié aux TIC " (Tikk et Schia, 2020). Cependant, les activités de l'ONU autour de la cybersécurité n'ont pas incité de nombreux pays africains à adopter la réglementation prévue en matière de protection des données, puisque seuls 11 États membres[6] avaient institué des cadres de protection des données en 2011 (Ball, 2017).[7]

En 2011, l'Union africaine (UA) a pris une mesure audacieuse pour réglementer la protection des données en publiant un projet de convention de l'UA sur l'établissement d'un cadre juridique crédible pour la cybersécurité en Afrique,[8] qui visait, entre autres

objectifs, à harmoniser les lois des États membres sur la protection des données et diverses questions (Orji, 2012). En 2013, le projet a été révisé et rebaptisé Convention de l'Union africaine sur la confiance et la sécurité dans le cyberespace,[9] mais elle a été réexaminée et a subi un autre changement de nom qui a abouti à la Convention de l'UA sur la cybersécurité et la protection des données personnelles en 2014, qui fut précédée d'une conférence d'experts des ministères de la justice des États membres de l'UA où le contenu de la convention a été examiné en profondeur, Abdulrauf, 2021).[10]

En définitive, le 27 juin 2014, lors de la 23e session ordinaire du sommet de l'UA à Malabo, en Guinée équatoriale, le projet de convention sur la cybersécurité et la protection des données personnelles[11] a été adopté par les chefs d'État afin d'établir un cadre crédible pour la cybersécurité en Afrique à travers la protection des données personnelles.[12]

La Convention de Malabo comporte un total de 38 articles, précédés d'un préambule de 20 paragraphes. La Convention vise à encourager les États membres à créer des cadres et des mécanismes pour protéger les données personnelles et les droits fondamentaux, et à faciliter la libre circulation des données sur le continent. Le premier article définit les termes principaux de la protection des données tels que le consentement, le contrôleur de données, la personne concernée, le marketing direct, le cryptage, les données de santé, le traitement des données personnelles, le destinataire, les données sensibles, le tiers, etc. mais, de manière surprenante, il omet de définir des concepts tout aussi importants tels que la pseudonymisation, le responsable du traitement des données, la violation des données, l'autorité de protection des données ou l'autorité de contrôle et le traitement transfrontalier. Bien que l'on puisse dire que l'omission de ces termes ne semble pas, à première vue, avoir une grande portée, la Convention est censée être une boussole pour les lois de protection des données sur le continent, comme le montrent ses articles 8(1) et (2), qui cherchent à établir un cadre pour la protection des données "physiques" et un mécanisme pour s'assurer que le traitement des données garantit la protection des droits fondamentaux. Cependant, même cette disposition n'atteint pas le statut de modèle législatif à cet égard. Il est donc souhaitable que la Convention soit complétée par des instruments pertinents afin de définir de manière exhaustive les clauses de protection des données régulières et fondamentales omises, faute de quoi son application pourrait engendrer une confusion conceptuelle inimaginable.

La Convention s'applique au traitement automatisé ou non automatisé[13] de données à caractère personnel sur le territoire d'un État membre.[14] Comme le GDPR, la Convention ne fournit pas de définition ou de description de ce qui constitue un traitement "automatisé" ou non automatisé, mais le droit européen définit le "profilage".'[15] Le traitement automatisé a toutefois été défini comme "une opération de traitement effectuée sans aucune intervention humaine ; à l'inverse, le traitement non automatisé est tel qu'il est effectué en partie ou en totalité avec une intervention humaine".[16] Le profilage et la prise de décision automatisée dans le contexte africain sont en pleine expansion dans le secteur bancaire, notamment avec le développement croissant des FinTechs et la prolifération des guichets automatiques de banque (GAB) ; cependant, il n'existe aucune législation panafricaine à ce sujet.

La Convention exige que les États membres mettent en place des autorités nationales indépendantes chargées de la responsabilité légale de veiller à ce que les données personnelles sur leurs territoires respectifs soient traitées conformément aux dispositions de la Convention, tout en respectant le rôle universel des autorités de protection des données (Giugiu et Larsen, 2016).[17] La Convention s'attend à ce que les autorités nationales chargées de la protection des données informent le public de ses droits en matière de protection des données sur leur territoire respectif,[18] tandis que ses membres sont isolés de toute influence gouvernementale, ce qui renforce leur indépendance et leur impartialité.[19] En juin 2021, sur les 30 pays d'Afrique disposant d'une législation adéquate en matière de protection des données, seuls 20 ont des autorités de protection des données (APD).[20] D'autres doivent encore en créer une ou en constituer les membres. La Convention prévoit clairement que les fonctions et les pouvoirs des APD comprennent le fait d'informer le public de ses droits, d'émettre des avis, de recevoir et de résoudre les plaintes, d'effectuer des audits sur le traitement des données, d'imposer des décisions administratives, de tenir un répertoire du traitement des données, de réglementer les transferts transfrontaliers, d'établir des mécanismes de coopération avec d'autres APD nationales,[21] l'autorisation de certaines activités de traitement,[22] les données impliquant des informations génétiques, des informations sur les infractions, le numéro d'identification national, les données biométriques, les données historiques et statistiques, entre autres.

Dans ce qui semble être un changement de nom et un réarrangement des principes universellement reconnus de la protection des données, la Convention regroupe le consentement et le traitement légitime,[23] distinct du principe de légalité et d'équité. Il fusionne ensuite la finalité avec les limites de stockage[24], l'exactitude et la transparence sont indépendantes, tandis que la confidentialité est regroupée avec la sécurité des données à caractère personnel.[25] Au total, la Convention reconnaît six principes redésignés, dont aucun n'envisage le principe de minimisation des données ou de responsabilité tel que reconnu par le droit européen, même si elle prévoit des principes spécifiques en cas de traitement de données personnelles sensibles.[26] L'application d'un tel regroupement et d'un tel embrouillage des principes ne serait pas seulement évidente dans l'application du concept groupé, mais elle pourrait aussi créer une confusion dans l'esprit des responsables du traitement des données quant à leurs obligations.

La Convention, comme la plupart des autres lois sur la protection des données, reconnaît le droit de la personne concernée à l'information, le droit d'accès, le droit d'opposition, la rectification ou l'effacement, mais elle omet également le droit de déposer une plainte auprès de l'autorité de contrôle, le droit à la portabilité des données, la restriction des traitements ultérieurs, etc.[27] Elle impose également aux responsables du traitement des données de garantir la confidentialité et la sécurité des données personnelles dont ils ont la garde.[28]

Bien que la Convention ait été adoptée en 2014, elle n'est pas encore entrée en vigueur en raison de l'article 36, qui ne la rend exécutoire que 30 jours après sa ratification par 15 États membres. Au 20 juin 2021, seuls l'Angola, le Ghana, la Guinée,

le Mozambique, Maurice, la Namibie, le Rwanda, le Sénégal et la Zambie ont ratifié la Convention.[29] En dépit de ses limites, Abdulrauf (2021) plaide toutefois en faveur de la disposition élargie et de la position autoritaire de la Convention, en particulier dans la mesure où elles influencent la législation ultérieure sur la protection des données sur le continent.

Loi additionnel relatif à la protection des données personnelles au sein de la CEDEAO (Loi de la CEDEAO)

La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a été créée pour promouvoir la coopération régionale entre les États membres, notamment pour la croissance économique, entre autres objectifs (Terwase et al., 2015). Le traité de la CEDEAO qui en découle prévoit l'harmonisation et la coordination des politiques nationales et la promotion de programmes d'intégration dans les domaines de la science, de la technologie, des questions juridiques, etc.[30]

Le 16 février 2010, 12 chefs de gouvernement de la CEDEAO réunis à Abuja, au Nigeria, ont adopté la Loi additionnel A/SA.1/01/10 relatif à la protection des données personnelles au sein de la CEDEAO[31] (la Loi), qui vise principalement à réglementer la protection des données au sein des États membres.

La loi définit des termes relatifs à la protection des données tels que le consentement, l'autorité de protection des données, les données personnelles, les données sensibles, les données relatives à la santé, la personne concernée, le responsable du traitement, le sous-traitant, le tiers et le destinataire[32] mais omet des terminologies importantes telles que traitement, profilage, pseudonymisation, anonymisation, profilage, violation de données personnelles, transfrontalier, etc. Le résultat de cette omission peut toutefois se faire sentir lorsque la loi est invoquée pour régler des questions relatives au traitement transfrontalier des données, en particulier devant les tribunaux régionaux lorsqu'ils sont confrontés à des questions de conflit de lois et de décision sur les principales APD nationales, etc.[33] La loi s'applique aux traitements de données à caractère personnel effectués par des entités publiques ou privées, par des moyens automatisés ou non, au sein de la CEDEAO, avec des exceptions.[34]

La loi donne mandat à chaque État membre d'établir son propre APD national indépendant, avec des paramètres garantissant son impartialité, son secret professionnel[35] et met en évidence les responsabilités et les pouvoirs des APD le secret avec le pouvoir d'imposer des sanctions aux parties fautives.[36] Dans sa propre version des sept principes de la protection des données, la loi stipule que le traitement est légitime lorsqu'il est effectué avec le consentement de la personne concernée, mais prévoit des exceptions lorsque l'exigence du consentement peut être omise.[37]

Le deuxième principe de légalité et de loyauté exige que le traitement soit effectué de manière légale, loyale et non frauduleuse.[38] Dans ce qui semble être une sorte de division, la loi sépare le consentement, qui est un motif de traitement légale, du

principe de légalité et de loyauté, qui est fusionné avec le principe de légalité, de loyauté et de transparence de l'UE (Kosta, 2013). En tant que troisième principe, la loi fusionne la limitation de la finalité, la minimisation des données et la limitation du stockage en un seul principe appelé "principe de finalité, de pertinence et de préservation"[39] qui exige que les données soient obtenues dans un but précis, qu'elles soient conservées de manière adéquate et qu'elles ne soient pas conservées au-delà de la période requise. Ce principe comporte également un élément du principe de légalité.[40] Les autres principes sont l'exactitude, la pertinence de la finalité et la préservation, la transparence, la confidentialité et la sécurité et le choix du responsable du traitement des données.[41]

S'inspirant du modèle européen de transfert transfrontalier de données vers des pays tiers, la loi limite le transfert de données personnelles en dehors de la sous-région de la CEDEAO aux seuls pays où il existe un niveau de protection adéquat[42] pour les droits et libertés fondamentaux. Bien que la loi ne prévoie pas de mécanismes élaborés pour réglementer ces transferts, elle oblige simplement les responsables du traitement des données à informer les APD avant le transfert.[43] Quant aux droits de la personne concernée, la loi reconnaît le droit d'être informé,[44] right to access,[45] droit d'opposition,[46] droit de correction et de destruction.[47] Là encore, la loi omet les droits fondamentaux de la personne concernée, tels que le droit à la restriction du traitement ultérieur, le droit à la portabilité des données, le droit relatif à la prise de décision automatisée, etc. La loi conclut essentiellement sur les obligations du responsable du traitement des données en matière de confidentialité, de sécurité, de conservation et de durabilité,[48] lesquelles obligations semblent toutefois similaires aux principes de protection des données dans leurs objectifs.

Communauté de développement de l'Afrique australe (SADC) - Loi type sur la protection des données

En 2009, l'impératif de créer un ensemble harmonisé et uniforme de politiques pour l'industrie des technologies de l'information et de la communication dans les pays subsahariens du groupe des États d'Afrique, des Caraïbes et du Pacifique a nécessité la promulgation et l'adoption de la loi type sur la protection des données de la Communauté de développement de l'Afrique australe (SADC),[49] qui a été adoptée en 2013. Comme de nombreuses lois sur la protection des données, la loi type définit des terminologies telles que le consentement, le contrôleur de données, le processeur, la personne concernée, les données génétiques, les données personnelles des enfants, le traitement, l'autorité de protection, le destinataire, le tiers de données sensibles et le flux transfrontalier. En revanche, la loi ne définit pas l'anonymisation, la pseudonymisation, le profilage, la violation de données personnelles, la demande d'accès des personnes concernées, etc.

D'après le libellé de l'article 2, il apparaît que le champ d'application de la loi n'est pas limité à la sous-région de la SADC puisqu'il ne fait référence qu'à "un pays ou un

territoire donné", termes qui n'y sont même pas définis. Même dans le préambule, il apparaît que la loi type n'est pas limitée à une quelconque région, notamment dans le paragraphe de conclusion qui dit que:

> "C'est en tenant compte de ce qui précède qu'il est reconnu que la protection des données à caractère personnel implique la mise en place d'un régime spécifique et adapté aux participants de chaque région, tel qu'énoncé dans la présente loi type."

Malgré sa portée panafricaine, la loi type est une loi souple sans effet juridiquement contraignant sur les États membres, mais comme les Lignes directrices de l'OCDE en Europe, elles ne font que guider les États membres sur l'approche de l'élaboration des lois sur la protection des données et une tentative d'harmonisation des lois dans la région (Shumba, 2015).

La loi prévoit la mise en place d'un régulateur indépendant pour les États membres, qui sera constitué par des juges nommés par l'exécutif et des organisations non gouvernementales ayant des connaissances compétentes et requises en matière de protection des données et bénéficiant d'une immunité.[50] Contrairement à d'autres instruments régionaux en Afrique, la loi type fournit les dispositions les plus complètes sur la nature, les devoirs d'indépendance et les pouvoirs des APD nationales, mais elle prévoit malheureusement que l'APD rende compte à une institution non définie au lieu du Parlement,[51] et érode ainsi son indépendance (Greenleaf, 2012). La loi type reconnaît le principe de la qualité des données, de la légalité et de la limitation de la finalité et elle contient de nombreuses dispositions sur le traitement des données sensibles et non sensibles, des données relatives aux enfants, des données relatives aux litiges, etc.,[52] mais elle omet toutefois des principes tels que la minimisation des données, l'exactitude de la limite de stockage, la redevabilité, l'intégrité et la confidentialité, etc. La loi décrit les obligations des responsables du traitement dans les cas où les données personnelles sont collectées directement auprès des personnes concernées et dans d'autres cas, l'obligation de garantir la sécurité des données et la responsabilité des tiers qui accèdent aux données par leur intermédiaire, la notification des violations de données ou des incidents.[53]

La loi reconnaît également aux personnes concernées les droits suivants : accès, opposition, décision automatisée, droit de représentation et droit de recours judiciaire.[54] En vertu de la loi, les membres des APD sont tenus de prêter serment de garder le secret.[55] car ils sont habilités à imposer des amendes aux contrôleurs en cas d'infraction et à poursuivre les contrevenants devant le tribunal.[56] La loi soumet le transfert transfrontalier de données aux dispositions pertinentes de la loi nationale adoptée pour la mise en œuvre de la loi type, et il s'agit là de la seule disposition qui concerne les États membres de la SADC, car elle exige un niveau de protection adéquat avant le transfert de données à caractère personnel vers des États non membres.[57] Bien que la loi fasse référence au niveau d'adéquation, contrairement au GDPR de l'UE, elle ne fournit pas les paramètres pour la détermination de ce niveau de protection.[58]

Malgré les dispositions remarquables de la loi type, celle-ci ne constitue qu'un cadre consultatif pour l'adoption de lois nationales, et non un instrument juridiquement contraignant pouvant être ratifié.[59]

Cadre juridique de la Communauté d'Afrique de l'Est (CAE) pour les lois sur le cyberespace 2008

Dans le cadre de ses efforts visant à renforcer l'intégration régionale de l'Afrique de l'Est grâce à l'interconnectivité numérique pour une prestation de services sans faille, la Communauté d'Afrique de l'Est a constitué un groupe de travail qui a recommandé un cadre juridique pour les lois relatives au cyberespace[60] avec pour objectif principal d'élaborer des politiques favorisant la coopération entre les États membres (Mwiburi, 2019).

Le Cadre définit la " protection des données " comme les obligations assignées aux entités traitant des données personnelles. Il reconnaît également qu'un régime de protection des données doit garantir certains droits des personnes concernées.[61] En vertu de ces dispositions, les responsables du traitement des données sont tenus de respecter les principes complexes de redevabilité, de transparence, de loyauté, de légalité, d'exactitude des données, de sécurité des données et de limite du traitement.[62] Le Cadre omet la minimisation des données, les limites de la finalité et la redevabilité, mais suggère un système d'autorégulation pour minimiser les coûts associés à l'approche conventionnelle de mise en conformité.[63]

Sans préjudice de ses dispositions progressives mais brèves sur la protection des données, elle constitue un simple cadre pour les États membres mais n'est pas juridiquement contraignante pour eux tant qu'ils n'ont pas transposé les dispositions dans leurs lois nationales respectives (Greenleaf et al., 2014). Il convient de noter que le cadre juridique a influencé à distance ou de quelque manière que ce soit la législation sur la protection des données au Kenya, en Ouganda et au Rwanda, qui ont adopté la législation par la suite.

3. Interaction entre la gouvernance des données et la protection des données en Afrique

La gouvernance des données est " l'exercice de l'autorité et du contrôle sur la gestion des données " (Abraham, et al., 2019). Elle implique également la confiance accordée aux données et leur redevabilité pour tout résultat négatif occasionné par leur mauvaise qualité. L'ensemble de la gouvernance des données en tant que concept renvoie au principe de redevabilité du traitement des données (Weber et al., 2009). Otto et al. (2007) définissent le concept comme un "cadre à l'échelle de l'entreprise pour l'attribution de droits et de devoirs liés à la prise de décision afin de pouvoir traiter les données de manière adéquate en tant qu'actif de l'entreprise". Il s'agit de " la mise en place d'une structure formelle de personnes, de processus et de technologies permettant à une organisation d'exploiter les données en tant qu'actif de l'entreprise " (Zornes, 2006).

La gouvernance des données s'intéresse à la répartition des responsabilités et des obligations entre les différents acteurs d'un système de gestion des données en ce qui concerne les droits des décideurs et l'obligation de rendre des comptes sur les actifs de données d'une entité. Alors que la gouvernance des données se rapporte principalement à la collecte et à la gestion des données qui garantissent une utilisation efficace et efficiente pour la productivité globale d'une entité (Cheong, et al., 2007), la protection des données permet de sauvegarder les données personnelles collectées[64] contre l'utilisation abusive, le compromis et/ou la corruption dans les limites de certains principes. Il est instructif de constater que la gouvernance des données ne se limite pas aux données personnelles, mais que la protection des données dans ce contexte ne vise qu'à protéger les données personnelles gérées parallèlement au big data[65] dans le cadre de la gouvernance des données. Par conséquent, certains principes de traitement des données ont un impact important sur la gouvernance des données en ce qui concerne les données à caractère personnel traitées par l'entité juridique.[66] Contrairement à l'Europe où les principes du traitement des données sont uniformément prévus par le GDPR,[67] le seul instrument régional facilement contraignant et applicable en Afrique est la Loi complémentaire de la CEDEAO sur la protection des données (Greenleaf, 2020). La Convention de l'UA sur la cybersécurité n'est pas encore en vigueur car sa disposition d'entrée en vigueur n'a pas été activée, moins de 15 membres l'ayant signée.[68]

Malgré son état comateux, la Convention prévoit des principes d'exactitude et de limitation de stockage[69] mais il ne prévoit pas explicitement la redevabilité.[70]

Cependant, ce principe est une ramification du principe de transparence (Alhadeff, et al. 2021), donc puisque la Convention prévoit ce dernier, la redevabilité peut être discutée dans le cadre de la gouvernance des données. Puisque la Convention de Malabo a une portée panafricaine, je vais examiner certains de ses principes qui interagissent avec la gouvernance des données en Afrique, même si elle est actuellement inapplicable.

Principe de precision

La précision est l'une des composantes de la qualité des données (Cong et al., 2017). Le principe de précision implique l'exactitude, l'exhaustivité et la cohérence des données et il va sans dire que les organisations ont besoin de données de la plus haute qualité pour fonctionner de manière optimale (Joshi, 2021). Dans le cadre de l'utilisation des données (personnelles) par une entité, les questions relatives à la confidentialité telles que la transparence, la sécurité, le compromis des (données personnelles) sont toujours soulevées et parfois les questions pertinentes restent sans réponse. Bair (2004) note que la qualité des données est définie par "le type et le domaine des données, l'exhaustivité, le caractère unique et l'intégrité référentielle, la cohérence entre toutes les bases de données, la nouveauté, l'actualité et la conformité aux règles de gestion".

Pour ce qui est de la relation entre le principe de précision et la gouvernance des données, Cohn (2015) affirme que " la gouvernance des données est un catalyseur de la qualité et la valeur provient de données de qualité bien gouvernées. Des données pertinentes, opportunes, cohérentes, fiables et exactes sont une attente et ne sont pas obtenues par hasard. Dans le jargon de la protection des données, le principe de la qualité des données[71] exige que les données à caractère personnel soient efficaces, adaptées, pertinentes et complètes pour la finalité de leur traitement.[72] Ce principe stipule que, lorsque les organisations utilisent les données de leurs clients pour prendre des décisions, elles doivent s'assurer que ces informations personnelles sont non seulement utilisées d'une manière pertinente par rapport à l'objectif de la collecte, mais qu'elles sont également exactes, saines et régulièrement mises à jour. Cela permettra de s'assurer que les informations personnelles utilisées pour les décisions importantes de l'organisation sont exactes afin d'éviter toute violation indue des droits et libertés fondamentaux des personnes concernées (Lee, 2002).

En vertu de ce principe, les organisations (privées et publiques) sont tenues de garantir l'exactitude des informations qu'elles conservent et des opinions qu'elles expriment à l'égard des personnes concernées, en particulier lorsque des décisions ayant une incidence sur ces dernières sont prises (Hallinan et Borbesius, 2020). Il impose aux responsables du traitement des données de prendre des mesures raisonnables pour s'assurer de l'aptitude des informations personnelles traitées dans le cadre de leurs activités organisationnelles. En guise de représentation de ce principe, l'article 13, principe 3 de la Convention de Malabo exige que la collecte des données soit adéquate, pertinente et non excessive au regard des finalités

pour lesquelles elles sont collectées.[73] En définitive, les personnes morales doivent mettre en place des mécanismes pour garantir la validité et la qualité des données à caractère personnel dont elles ont la garde, en s'imprégnant d'une culture d'entreprise consistant à effectuer des mises à jour périodiques et à supprimer en temps utile les données périmées ou non pertinentes.

Limitation du stockage

Le stockage des données est l'une des principales composantes de la gouvernance des données. Parfois, elles sont stockées indéfiniment dans des bases de données non réglementées et non surveillées pour les analyses fantaisistes et/ou l'utilité des contrôleurs, souvent sans le consentement des personnes concernées (Pike, 2020). L'adoption d'une législation sur la protection des données en Europe, par exemple, a fait paniquer de nombreuses organisations, surtout lorsqu'il s'est agi de vérifier les bases juridiques de la collecte et/ou du stockage des données des visiteurs en ligne sur leurs plateformes numériques, sans nécessairement fixer les mécanismes d'obtention du consentement éclairé (Francesco et al., 2021). S'il n'est pas interdit aux entreprises de stocker les données personnelles des clients, ce stockage doit se faire dans les limites des lois applicables en matière de protection des données et de ses exceptions (Duceto, 2020). Par exemple, le traitement des données à des fins de recherche constitue l'une des exceptions au principe de limitation du stockage, puisque les données peuvent être conservées plus longtemps que nécessaire notamment pour la vérification des résultats de la recherche (Pormeister, 2017).

Le stockage sans discrimination et indéfini des données personnelles des clients et des autres personnes concernées par les organisations pose des risques inimaginables pour la confidentialité, attribuables à des mesures de sécurité techniques et organisationnelles non réglementées et, la plupart du temps, insuffisantes et inadéquates (le cas échéant) par les responsables du traitement des données (Biega et Finick, 2021). Fondamentalement, les données personnelles ne doivent pas être conservées sous une forme permettant d'identifier les personnes concernées pendant une durée supérieure à celle justifiée par la loi. Lorsque les données personnelles ne sont plus nécessaires ou qu'elles sont devenues non pertinentes ou obsolètes, les responsables du traitement peuvent soit les supprimer purement et simplement, soit les anonymiser ou les pseudonymiser dans certains cas (Mourby et al., 2018).

En vertu de la Convention de Malabo de l'UA, la limitation de la conservation n'est cependant pas un principe mais une obligation pour les responsables du traitement des données. L'article 22 interdit catégoriquement la conservation des données à caractère personnel pendant une durée supérieure à celle nécessaire à la réalisation de l'objectif de leur collecte, mais la disposition est dépourvue d'exceptions ou de paramètres pour la période de conservation applicable. Le principe s'articule avec le droit de la personne concernée à l'oubli ou à la suppression ou à l'effacement des données à caractère personnel, qui ne sont plus pertinentes ou à jour. Sans préjudice des circonstances entourant la collecte de données personnelles par une organisation,

ce principe fonctionne toujours pour lui permettre de ne pas conserver et/ou stocker les données pendant une période plus longue que celle raisonnablement nécessaire. Par conséquent, une fois que les données ont été utilisées aux fins de la collecte, il incombe à l'organisation de supprimer ou d'anonymiser immédiatement ces données personnelles afin de réduire le risque de violation des principes de minimisation et de précision des données lorsqu'elles deviennent non pertinentes, excédentaires, inexactes ou périmées. Les instruments régionaux ne prévoient pas de périodes de conservation spécifiques ; toutefois, les lois nationales pertinentes devraient être consultées sur les limites de conservation des données mais, en fin de compte, une formidable politique de gouvernance des données devrait être élaborée pour combler les lacunes législatives à cet égard.

La participation des législateurs et des parties prenantes à la gouvernance des données devient toutefois très importante si l'on considère que sur 55 pays africains, au moins 49 ont (ou sont sur le point) de promulguer des lois ou des règlements exigeant des abonnés potentiels qu'ils fournissent des données personnelles comme condition d'obtention d'une ligne téléphonique (Donovan et Martyin, 2013), mais malheureusement, seuls 19 de ces pays ont établi des autorités de protection des données[74] pour faire respecter les lois pertinentes en matière de protection des données.

Redevabilité

Ce principe est issu des lignes directrices de l'OCDE[75] de 1980 et est repris dans sa version révisée de 2013. Le principe exige principalement que les entités juridiques reconnaissent et assument la responsabilité de leurs opérations sur les données personnelles dans le cadre des activités organisationnelles. Les responsables du traitement des données ont le devoir impératif de faire preuve de mesures techniques et organisationnelles adéquates pour sécuriser les données conformément à la législation pertinente en matière de protection des données pour la protection ultime des droits des personnes concernées (De Hert et al., 2012). Conformément à ce principe, les entités juridiques sont tenues de documenter le respect de leurs obligations en vertu de la législation pertinente en matière de protection des données (Becker, 2019).

La redevabilité n'est pas explicitement prévue par la Convention de Malabo, mais ce principe est étroitement lié au principe de transparence et a été considéré comme un principe renforçant la protection de la confidentialité et des données.[76] En démontrant leur redevabilité, les organisations doivent adopter une approche pratique des questions de protection des données et de la confidentialité en adoptant des mesures efficaces et contemporaines qui ne sont pas seulement discernables au premier coup d'œil, mais qui peuvent être démontrées de manière transparente en cas de demande ou d'audit réglementaire (Falk, 2016).

Les responsables du traitement des données doivent assumer l'entière responsabilité de la manière dont ils traitent directement ou indirectement les

données et mettre en œuvre des mesures et une documentation appropriées pour prouver leur conformité aux lois applicables (Bennet, 2021). Ils sont responsables et doivent démontrer la qualité des données.

Confidentialité et intégrité

Ceci est reconnu par le principe 6 de la Convention de Malabo. Ce principe impose simplement aux organisations qui traitent des données personnelles de prendre des mesures organisationnelles et techniques appropriées pour protéger ces informations personnelles contre le mauvais usage, la corruption, le vol et/ou la destruction. En ce sens, la confidentialité renvoie au devoir de l'organisation qui traite les données de s'assurer que ces informations ne sont pas partagées ou exposées à des personnes non souhaitées, tout en les gardant aussi sûres et secrètes que techniquement possible.

4. Incitations du cadre juridique pour la protection des données/ gouvernance des données en Afrique

Les avantages de la protection des données pour la gouvernance des données sont nombreux. Toutefois, aux fins du présent document, j'aborderai brièvement les incitations provenant de la protection des droits et des gains économiques pour les organisations et les gouvernements.

Garanties du droit à la confidentialité

Même si la Charte africaine ne reconnaît pas expressément la confidentialité comme un droit fondamental, elle n'exclut pas le droit des Africains de jouir d'une vie familiale privée.[77] Cette idée d'un droit à la vie privée pour les individus est également à la base de la notion de protection des données. En fait, la protection des données trouve son origine dans le droit au respect de la vie privée, de sorte qu'un cadre juridique adéquat et formidable pour la protection des données garantirait non seulement certains droits des personnes concernées, mais aussi un contrôle considérable sur leurs informations personnelles et, en fin de compte, la confiance des consommateurs dans les activités de traitement.

Une démocratie saine

Un État démocratique sain est un État dans lequel ses citoyens peuvent faire des choix informés et autonomes (Forde, 2016). Or, traiter des données sans tenir compte de l'impact qu'elles peuvent avoir sur les individus peut avoir pour effet de limiter la capacité des individus à faire des choix ou de limiter les choix disponibles pour ces individus d'une manière qui limite leur autonomie (Feldman, 1994). Ce point est encore plus crucial dans le monde actuel de la dépendance technologique, où le traitement automatisé et les identités numériques deviennent progressivement des déterminants plus importants des choix de la vie réelle d'un individu. Les lois sur la protection des données s'y opposent. L'idée que lorsque le consentement est invoqué comme base juridique du traitement, il doit être éclairé et ne doit pas être obtenu par des tactiques coercitives fait écho à ces préoccupations d'autonomie démocratique. En outre, même dans les cas où les données sont traitées sans consentement, la notion de droits des personnes concernées et les obligations en matière de transparence, d'équité et de redevabilité offrent les contrôles indispensables dont les individus ont

besoin pour conserver leur capacité à faire des choix véritablement libres. On peut donc conclure sans risque de se tromper qu'un monde où la protection des données est respectée est un monde dans lequel les semences du totalitarisme d'entreprise ou gouvernemental ne peuvent pas prospérer.

Les gains économiques de la libre circulation des données

Le concept de libre circulation n'est pas simplement celui où il n'y a pas d'obstacles juridiques aux transferts de données entre juridictions. Il implique plutôt que lorsque ces barrières juridiques existent, elles n'imposent pas d'exigences de localisation des données. Les exigences en matière de localisation des données ont pour effet direct d'augmenter les coûts des activités commerciales entre les juridictions. En particulier, pour les entreprises axées sur les données, telles que les fournisseurs de services en nuage, ces coûts ont pour effet supplémentaire de poser des obstacles importants à l'entrée sur de nouveaux marchés sur le continent. Cela décourage la création de telles entreprises et crée un environnement qui limite la croissance des start-ups et des petites et moyennes entreprises (PME) africaines. En outre, la libre circulation des données personnelles faciliterait la diffusion des informations et la collaboration bénéfique des entreprises et des sociétés de la région. Toutefois, ces avantages s'étendent aux possibilités de collaboration en dehors de la région. Le cadre européen de protection des données définit la tendance globale pour les collaborations technologiques à travers le monde. La mise en œuvre et le lancement d'un cadre africain de protection des données peuvent créer une opportunité pour la reconnaissance des pays africains comme ayant un niveau adéquat de protection des données. Cela pourrait faciliter la collaboration transfrontalière, même pour les entreprises non axées sur les données qui cherchent à s'associer à des entreprises africaines.

5. Conclusion

La gouvernance des données se rapporte principalement à la gestion des données pour la croissance de l'organisation. L'expérience a montré que la gestion du big data impliquerait toujours le traitement de données personnelles, d'où l'activation des principes de protection des données.

L'Afrique ne dispose actuellement que d'un seul instrument régional contraignant - la Loi complémentaire de la CEDEAO sur la protection des données - parmi d'autres instruments internationaux comportant des dispositions sur divers principes qui confèrent de manière convaincante la gouvernance des données sur le continent. Sur 55 pays africains, seuls 30 ont des lois de protection des données entièrement dédiées, et 19 d'entre eux ont établi des APD pour faire respecter les lois, il est donc clair que la gouvernance des données sur le continent reste largement non soutenue par un cadre législatif et d'application.

Avec l'ampleur des données personnelles échangées, stockées ou transmises au sein du système de gouvernance des données en Afrique, un cadre juridique formidable et approprié de protection des données devient très important pour garantir aux utilisateurs le contrôle de leurs informations personnelles, et pour réglementer le traitement/gestion de ces informations par les contrôleurs de données contre l'utilisation abusive, le compromis, le vol ou d'autres opérations malveillantes avec les données personnelles.

Pour une gouvernance des données correctement réglementée, il est à espérer que les pays africains ratifieront la Convention de Malabo et renforceront leurs cadres juridiques municipaux respectifs en matière de protection des données afin de compléter la gestion des données personnelles par les organisations publiques et privées, non seulement sur leurs territoires respectifs mais aussi sur l'ensemble du continent.

La coopération transfrontalière des autorités nationales de protection des données, envisagée par les traités régionaux, devrait être encouragée et renforcée afin de stimuler l'application des lois régionales et municipales sur la protection des données, dans le but d'améliorer le flux transfrontalier de données et la gouvernance internationale des données dans le cadre de règles transfrontalières uniformes de protection des données.

Remarques

1. LLM ("Lecture") ; avocat à la Cour suprême du Nigeria ; associé directeur, Olumide Babalola LP ; membre de l'Association internationale des professionnels de la protection de la confidentialité (IAPP) ; membre du Réseau international des professionnels du droit de la confidentialité (INPLP) ; auteur, Droit de la confidentialité et de la protection des données au Nigeria.

2. La directive a été promulguée par l'Union européenne en 1995, afin d'harmoniser toutes les lois sur la protection des données au sein de l'union et de réglementer le traitement des données personnelles stockées dans des bases de données numériques. Voir Rebecca Wong, " La Directive 95/46/CE sur la protection des données : idéalismes et réalismes " (2012) Revue internationale de droit, informatique et technologie, 1.

3. La Convention de l'UA sur la cybersécurité et la protection des données personnelles a été adoptée à Malabo le 27 juin 2014.

4. Cap-Vert (2001), Maurice (2004), Seychelles (2004), Tunisie (2004), Burkina Faso (2004), Sénégal (2008), Maroc (2009), Bénin (2009), Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Mali (2013) et Côte d'voire (2013).

5. Les rapports qui remontent à 2014 ont été récemment mis à jour en mars 2021, lorsque les États participants ont décidé de renforcer leurs capacités en matière d'infrastructures d'information critiques, notamment en ce qui concerne le partage et la coordination de l'information aux niveaux national, régional et international." Voir Assemblée générale des Nations unies, " Rapport final substantiel " < https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> consulté le 26 octobre 2021.

6. Cap-Vert (2001), Maurice (2004), Seychelles (2004), Tunisie (2004), Burkina Faso (2004), Sénégal (2008), Maroc (2009), Bénin (2009), Angola (2011), Gabon (2011) et Lesotho (2011).

7. Bautlin M. Ball, " Note introductive à la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles " (2017) The American Society of International Law, 165.

8. Trouvé sur le site: https://au.int/en/cyberlegislation.

9. Trouvé sur le site https://ccdcoe.org/uploads/2018/11/AU-130101-DraftCSConvention.pdf.

10. Lukman Adebisi Abdulrauf et Charles Manga Fombad, " La Convention de l'Union africaine sur la protection des données 2014 : A Possible Cause for Celebration of Human Rights in Africa " (2016) 8(1) Journal of Media Law, 1, 8.

11. Trouvé sur le sitet https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

12. La 23e session ordinaire de l'Union africaine se termine à Malabo. Voir https://au.int/fr/newsevents/29258/23rd-ordinary-session-african-union-ends-malabo#:~:text=Malabo%2C%20Equatorial%20Guinea%2030%20June,from%2026%2D27%20June%202014.> accessed 26 May 2021.

13. Article 9(1), Convention de Malabo.

14. Les 55 membres de l'UA sont les suivants: Le Burundi, le Cameroun, la République centrafricaine, le Tchad, le Congo, la République démocratique du Congo, la Guinée équatoriale, le Gabon, Sao Tomé-et-Principe, les Comores, Djibouti, l'Érythrée, l'Éthiopie, le Kenya, Madagascar, Maurice, le Rwanda, les Seychelles, la Somalie, le Sud-Soudan, la République du Soudan, la Tanzanie, l'Ouganda, l'Algérie, l'Égypte, la Libye, la Mauritanie, Maroc, République arabe sahraouie démocratique, Tunisie, Angola, Botswana, Royaume d'Eswatini, Lesotho, Malawi, Mozambique, Namibie, Afrique du Sud, Zambie, Zimbabwe, Bénin, Burkina Faso, Cap-Vert, Côte d'voire, Gambie, Ghana, Guinée, Guinée-Bissau, Liberia, Mali, Niger, Nigeria, Sénégal, Sierra Leone et Togo.

15. Voir l'article 4(4); Klaus Wiedemann, K. 2018.

16. IAPP https://iapp.org/resources/article/automated-processing/ accessed 29 May 2021.

17. Andra Giugiu and Tine A. Larsen, Rôle et pouvoir des autorités nationales de protection des données (2016) 3 EDPL, 342.

18. Art. 11(1)(a).

19. Art. 11(1)(b); Graham Greenleaf. 2012.

20. Angola, Bénin, Burkina Faso, Cap-Vert, Côte d'Ivoire, Égypte, Gabon, Ghana, Kenya, Lesotho, Mali, Maroc, Maurice, Niger, Nigeria, Sao Tomé-et-Principe, Sénégal, Afrique du Sud et Tunisie. Mali, Maroc, Maurice, Niger, Nigeria, Sao Tomé-et-Principe, Sénégal, Afrique du Sud et Tunisie. Voir Paradigm Initiative et Olumide Babalola, "Data Protection Authorities in Africa : Un rapport sur l'établissement, l'indépendance, l'impartialité et l'efficacité des autorités de contrôle de la protection des données au cours des deux décennies de leur existence sur le continent.

21. Article 12(2) (a)-(o).

22. Art. 10 (4).

23. Article 13 (1).

24. Article 22.

25. Article 13 (3) – (6).

26. Article 14.

27. Article 16 et 17.

28. Article 20 et 21.

29. La liste des statuts se trouve à l'adresse https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> consulté le 20 juin 2021.

30. Art. 32(a) Traité révisé de la CEDEAO de 1993 se trouve à < https://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf>; see also Abiodun Ashiru, 'Une analyse comparative du cadre juridique de la pénalisation du cyberterrorisme au Nigeria, en Angleterre et aux États-Unis". (2021) 12(1) NAUJILJ, 99, 107.

31. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf> consulté le 22 juin 2021.

32. Art. 1.

33. En Europe, les APD nationales tentent parfois d'usurper la compétence des tribunaux pour régler ces litiges transfrontaliers en recourant à d'autres mécanismes de règlement des litiges. Voir Olga Estadella-Yuste, "Transborder Data Flows and the Sources of Public International Law" (1991) 16(2) North Carolina Journal of International Law and Commercial Regulation,380, 412.

34. Art. 3 et 4.

35. Art.14 et 19.

36. Art. 20.

37. Art. 23 (1) et (2).

38. Art. 24.

39. Art. 24.

40. Art. 25.

41. Articles 25, 26, 27, 28 et 29.

42. Il s'agit d'un concept européen qui a été reconnu par les Lignes directrices de l'OCDE, mais qui a pris de l'importance avec l'abrogation de la directive 95/46/CE sur la protection des données, en réglementant le transfert international des données à caractère personnel. Voir Julian Wagner, "The Transfer of Personal Data to Third Countries under the GDPR : Quand un pays destinataire fournit-il un niveau de protection adéquat ? ". (2018) 8(4) International Data Privacy Law, 319.

43. Art. 36.

44. Art. 38.

45. Art. 39.

46. Art. 40.

47. Art. 41.

48. Art. 42 – 45.

49. Trouvé sur le site < https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf> consulté le 19 juin 2021.

50. Art. 3(2).

51. Art. 3(10).

52. Art. 11-17.

53. Art. 21-27.

54. Art. 31-38.

55. Art. 41(1)

56. Art. 42.

57. Art.44 (1)(a).

58. Art. 44 (1) (b). Voir aussi Wagner. 2018.

59. Parlement de la République sud-africaine. < https://pmg.org.za/files/RNW2764-150825.docx> consulté le 9 juin 2021.

60. Trouvé sur le site http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq> accessed 11 June 2021.

61. Clause 2.5.

62. Ibid.

63. Ibid.

64. Celle-ci est définie dans le cadre de la Convention de Malabo comme : " 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 ".

65. La définition est la suivante : "Le terme "big data" désigne des ensembles de données qui sont non seulement volumineux, mais aussi très variés et rapides, ce qui les rend difficiles à traiter à l'aide des outils et techniques traditionnels" Voir Elgendy et Elraga. 2014.

66. Les principes d'exactitude, de limites de stockage et de redevabilité seront examinés en détail plus loin dans cette étude.

67. Principes de légalité, d'équité et de transparence ; réduction des données ; limite de stockage ; restriction de la finalité ; exactitude ; intégrité et confidentialité et redevabilité. Voir art. 5(1) et (2). Ces principes sont similaires à ceux prévus par la directive européenne 15/46 CE sur la protection des données, qui a été abrogée. Voir Bygrave. 2014.

68. Liste des pays qui ont signé, ratifié ou adhéré à la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles <
< https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 22 June 2021.

69. Article 13 (3).

70. Le principe fait partie de la législation européenne sur la protection des données depuis 1980, date à laquelle il a été introduit dans les "Recommandations du Conseil portant sur les lignes directrices régissant la protection de la confidentialité et les flux transfrontières de données à caractère personnel" de l'Organisation de coopération et de développement économiques, le 23 septembre 1980.
<https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> consulté le 21 juin 2021.

71. Certains chercheurs ont toutefois fait valoir que, bien que ce principe soit prévu à l'article .... de la directive européenne 95/46/CE abrogée sur la protection des données, cette inclusion était mal conçue, car la qualité des données ne joue pas nécessairement un rôle autonome dans la législation sur la protection des données, contrairement à l'économie des données, c'est-à-dire l'industrie du traitement des données elle-même. Voir Thomas Hoeren, "Big Data and Data Quality" in Big Data in Context Legal, Social and Technological Insights Thomas Hoeren et Barbara Kolany-Raiser (eds) (Springer, 2018,) 2.

72. ‘Le "traitement" est un terme technique qui désigne la modification, l'utilisation, la transmission, la collecte, la conservation, la destruction, le transfert et toute opération ou ensemble d'opérations portant sur des données à caractère personnel, telles que définies à l'article 1er de la Convention de Malabo.

73. L'art. 13 (4) prévoit que les données collectées doivent être exactes et, si nécessaire, mises à jour.

74. Angola (Agência de Protecção de Dados); Benin (Personal Data Protection Authority); Burkina Faso (Commission de l'Informatique et des Libertés); Cape Verde (Agência de Protecção de Dados); Chad (Agence Nationale de Sécurité Informatique et de Certification Électronique); Côte d'Ivoire (Autorité de Régulation des Télécommunications de Côte d'Ivoire); Egypt (Personal Data Protection Centre); Gabon (Commission nationale pour la protection des données à caractère personnel); Ghana (Data Protection Commission); Kenya (Office of Data Protection Commissioner); Madagascar (Commission Malagasy de l'Informatique et des libertés); Mali (Autorité de Protection des Données à Caractère Personnelles); Mauritius (Data Protection Office); Morocco (Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel); Niger (High Authority for the Protection of Personal Data); Nigeria (National Information Technology Development Agency); Sao Tome and Principe (Agência Nacional de Protecção de Dados Pessoais); Senegal (Commission des Données Personnelles); South Africa (Information Regulator); and Tunisia (Instance nationale de protection des données personnelles).

75. L'article 14 prévoyait que : "Un responsable du traitement des données devrait être tenu de respecter les mesures qui donnent effet aux principes énoncés ci-dessus.’

76. Guagnin et Leon (2012), et aussi Zimnerman et Cabinakova (2015).

77. L'article 18 de la Charte africaine des droits de l'homme et des peuples exhorte les États membres à protéger la famille, "unité naturelle et base de la société".

Références

Abdulrauf, Lukman Adebisi and Fombad, Charles Manga. 2016. "The African Union Data Protection Convention 2014: A possible cause for celebration of human rights in Africa". *Journal of Media Law*, 1,8. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Abdulrauf, Lukman Adebisi. 2021. "Giving 'teeth' to the African Union towards advancing compliance with data privacy norm". *Information and Communication Technology Law*, 1, 30(2).

Abraham, Rene, Jan vom Brocke and Schneider, Johannes. 2019. "Data governance: A conceptual framework, structured review and research agenda". *International Journal of Information Management*, 1, 49.

Alhadeff, J., van Alsenoy, B. and Dumorhier, J. 2021. "The accountability principle in data protection regulation: Origin, development and future directions". In Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). *Managing privacy through accountability*. Palgrave Macmillan.

Ashiru, Abiodun. 2021. "A comparative analysis of the legal framework for the criminalization of cyberterrorism in Nigeria, England and the United States". Nnamdi Azikiwe University Journal of International Law and Jurisprudence 12(1) 99, 107. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf. Accessed 22 June 2021.

Bair, J. 2004. Practical data quality: Sophistication levels? http://www.knightsbridge.com/pdfs/in_the_news/. Accessed 21 June 2021.

Ball, Bautlin M. 2017. "Introductory note to African Union Convention on Cyber Security and Personal Data Protection". *The American Society of International Law*, 165. https://au.int/en/cyberlegislation.

Becker, Regina. 2019. "A data information system for accountability under the General Data Protection Regulation". *Giga Science*, 8(12): 122.

Bennet, C.J. 2021. "The accountability approach to privacy and data Protection: Assumptions and caveats". In Daniel Guagnin, Carla Iiten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). *Managing privacy through accountability*. Palgrave Macmillan.

Biega, A. and Finick, M. 2021. "Reviving purpose limitation and data minimization in personalization, profiling and decision-making system". Max Planck Institute for Innovation and Competition Research Paper No. 21.04, 1, 5.

Brendan, Joseph A., van Alsenoy and Dumorhier, J. 2021. "The accountability principle in data protection regulation: Origin, development and future directions in managing privacy through accountability. In Daniel Guagnin, Carla Iiten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). Palgrave Macmillan.

Bygrave, Lee A. 2002. *Data protection law: Approaching its rationale, logic and limits*. Kluwer International.

Bygrave, Lee A. 2014. *Data privacy law: An international perspective*. Oxford: Oxford University Press.

Cheong, Lai Kuan and Chang, Vanessa. 2007. The need for data governance: A case study. 18th Australasian Conference on Information system.

Cohn, Barbara L. 2015. "Data governance: A quality imperative in the era of big data, open data and beyond. *Journal of Law and Policy for the Information Society*, 10 (3): 812.

Cong, G., Fan, W., Geerts, F. and Ma, Shuai. 2017. "Improving data quality: Consistency and accuracy. Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23–27, 1.

De Hert, P., Papa, V.K., Wright, D. and Gutwirth, S. 2012. "The proposed regulation and the construction of a principles-driven system for individual data protection". *The European Journal of Social Science Research*, 26(1).

Donovan, Kevin P. and Martyin, Aaron K. 2013. "The rise of African SIM registration: The emerging dynamics of regulatory change". https://firstmonday.org/ojs/index.php/fm/article/view/4351/3820. Accessed 15 June 2021.

Duceto, R. 2020. "Data protection, scientific research and the role of information". *Computer and Security Review*, 37: 1, 5.

Elgendy, Nada and Elraga, Ahmed. 2014. "Big data analytics: A literature review paper. *Lecture Notes in Computer Science*, 8557, 214-227.

Estadella-Yuste, Olga. 1991. "Transborder data flows and the sources of public international law". *North Carolina Journal of International Law and Commercial Regulation*, 16(2): 380–412.

Falk, T.T. 2016. The concept of accountability as a privacy and data protection principle. https://www.cpomagazine.com/data-privacy/concept-accountability-privacy-data-protection-principle/. Aaccessed 17 June 2021.

Feldman, David. 1994. "Secrecy; dignity or autonomy? Views of privacy as a civil liberty". *Current Legal Problems*, 47(2): 42–54.

Forde, Aidan. 2016. "The conceptual relationship between privacy and data protection". *Cambridge Law Review*, 1: 135–137.

Francesco, G., Palazzani, L., Dimitiou, D., Domingo, J.D. Jiame Fons-Martinez, J., Jackson, S., Tozzi, P.V. and Caterina Rizzo, C. 2021. Digital tools in the informal consent process: A systematic view. https://www.researchsquare.com/article/rs-1273/v2. Accessed 13 June 2021.

Gao Cong, Gao, Wenfei Fan, Wenfei, Floris Geerts Floris and Ma S. 2017. "Improving data quality: Consistency and accuracy". Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23–27.

Giugiu, Andra and Tine A. Larsen. 2016. "Role and power of national data protection authorities". Eueopean Data Protection Law, 3: 342.

Greenleaf, Graham and Coltier, Bertil. 2020. "Comparing African data privacy laws: International, African and regional commitments". *University of New South Wales Law Research Series*, 1: 21.

Greenleaf, Graham and Cottier, Bertil. 2018. "Data privacy laws and bills: Growth in Africa, GDPR influence". *Privacy Laws and Business International Report*, 152: 11.

Greenleaf, Graham and Georges, Marie. 2014. "African regional privacy instruments: Their effect on harmonization". *Privacy Law and Business International Report,* 132: 19–21.

Greenleaf, Graham. 2012. "Independence of data privacy authorities international standards and Asia-Pacific experience". *Computer Law and Security Review*, 1, 28(1).

Guagnin, D. and Leon, H. 2012. *Managing privacy through accountability*. Palgrave Macmillan UK.

Hallinan, D. and Borbesius, F.Z. 2020. "Opinions can be incorrect (in our opinion) on data protection law's accuracy principle". *International Data Privacy Law*, 1, 10(1)

Hoeren, Thomas. 2018. "Big data and data quality". in Thomas Hoeren and Barbara Kolany-Raiser (eds), *Big data in context legal, social and technological insights*, Springer.

Joshi, Aurko. 2021. "Data quality and data governance: Where to begin". https://www.collibra.com/blog/data-quality-vs-data-governance. Accessed 11 June 2021.

Kavanagh, Camino. 2017. The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century. https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf. Accessed 25 May 2021.

Klaus Wiedemann, Klaus. 2018. "Automated processing of personal data for the evaluation of personally traits: Legal and ethical issues". Max Plank Institute for Innovation and Competition Research Paper No. 18-04, 3. IAPP https://iapp.org/resources/article/automated-processing/. Accessed 29 May 2021.

Kosta, Eleni. 2013. *Consent in European data protection law*. Nijhoff Publishers.

Lee A. 2002. *Bygrave, data protection law: Approaching its rationale, logic and limits*. Kluwer International.

Makulilo, Alex B. and Mophethe, Kuenu. 2016. "Privacy and data protection in Lesotho". *African Data Privacy Laws*, 337–347.

Makulilo, Alex Boniface. 2012. "Privacy and data protection in Africa: A state of the art". *International Data Privacy Law*, 2(3), 163.

Mayer-Schonberger, Victor. 1997. "Generational development of data protection in Europe". In Phillip Agre and Marc Rotenberg (eds), *Technology and privacy: The new landscape.* Cambridge: MIT Press.

Mercer, Shannon Togawa. 2020. "The limitations of European data protection as a model for global privacy regulation". American Journal of International Law Unbound, 114: 20–25.

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Susan E. Wallace, Bell, J. Smith, H., Aidinlis, S. and Kaye, J. 2018. "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK". *Computer Law and Security Review*, 34: 222–233.

Mwiburi, Abel Juma. 2019. *Preventing and combating cybercrime in East Africa. Lessons from Europe's cybercrime frameworks*. Berlin: Duncker and Humblot.

OECD. 2021. Guidelines on the protection of privacy and transborder flows of personal data. https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 9 June 2021.

Oman, Soren. 2010. "Implementing data protection in law". *Stockholm Institute for Scandinavian Law*, 1.

Orji, Uchenna Jerome. 2012. "The defects of the draft African Union convention on the establishment of a credible legal framework for cybersecurity". Institute of Electrical and Electronics Engineers, 1. https://ccdcoe.org/uploads/2018/11/AU-130101-DraftCSConvention.pdf.

Otto, B., Wende, K.; Schmidt, A. and Osl, P. 2007. "Towards a framework for corporate data quality management". 16th Australasia Conference on Information Systems University of Southern Queensland, Toowoomba Australia, 916–926.

Parliament of the Republic of South Africa. 2021. https://pmg.org.za/files/RNW2764-150825.docx> accessed 9 June 2021.

Pike, E.R. 2020. "Defending data: Towards ethical protections and comprehensive data governance". *Emory Law Journal*, 69: 687.

Pormeister, Kart. 2017. "Genetic data and the research exemption: Is the GDPR going too far?". *International Data Privacy Law*, 7(2): 137–140.

Schwartz, Paul M. 2019. "Global data privacy: The EU Way". 94 New York University Law Review, 94: 771.

Scott, Mark and Cerulus, Lauren. 2018. "Europe's new data protection rules export privacy standards worldwide". *Politico*, January 31.

Shumba, Tapiwe. 2015. "Revisiting legal harmonization under the Southern African Development Community treaty: The need to amend the treaty". *Law Democracy Development*, 19:1.

Terwase, I.T., Abdul-Talib, Asmat-Nizam and Zengeni, K.T. 2015. "The role of ECOWAS on economic governance, peace and security perspectives in West Africa". *Mediterranean Journal of Social Sciences,* 6(3): 257.

Tikk, Eneken and Schia, Niels Nagelhus. 2020. "The role of the UN Security Council in cybersecurity". In Eneken Tikk and Mika Kerttunen (eds), *Handbook of International Cybersecurity*. Routledge.

Traca, Joao Luis and Embry, Bernado. 2011. "An overview of the legal regime for data protection in Cape Verde". *International Data Privacy Law*, 1, 3.

United Nations. 2021. Recent developments in the field of information telecommunications in the context of international security. https://ccdcoe.org/incyder-articles/united-nations-recent-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security/. Accessed 25 May 2021.

UN General Assembly. 2021. Final substantive report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. Accessed 26 October 2021.

Wagner, Julian. 2018. "The transfer of personal data to third countries under the GDPR: When does a recipient country provide an adequate level of protection? *International Data Privacy Law*, 8(4): 319.

Wiedemann, Klaus. 2018. "Automated processing of personal data for the evaluation of personally traits: Legal and ethical issues". Max Plank Institute for Innovation and Competition Research Paper No. 18–04, 3.

Weber, K., Otto, B. and Osterle, H. 2009. “One size fits all - A contingency approach to data governance”. *Journal of Data and Information Quality*, 1(1): 1–27.

Wong, Rebecca. 2012. “The data protection directive 95/46/EC: Idealisms and realisms”. *International Review of Law Computers and Technology,* 1.

Zimnerman, C. and Cabinakova, J. 2015. “A conceptualizing of accountability as a privacy principle”. In BIS, W. Abramowicz (ed). Springer International publishing.

Zornes, Aaron. 2006. Corporate data governance best practice. The CDI Institute Market Plus TM Depth Report.

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