Mise en œuvre par

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

HOCHSCHULE KEHL
UNIVERSITY OF APPLIED SCIENCES
Designing and Developing Public Administration

Dorsch Impact

ETUDE DU CADRE JURIDIQUE RELATIF À L'ANONYMISATION DES DOCUMENTS JUDICIAIRES PUBLIÉS AU SÉNÉGAL ET EN CÔTE D'IVOIRE (ETUDE B)

Promotion of the Rule of Law and Justice in Africa

(ProLa) MAY 2025

CONSULTANCY AND TECHNICAL STUDIES

(CN 81292882)

Fama Dieng, Ewald Eisenberg, Marc Gnahoré,
Ismaël Kouassi Yayi Oka, Clemens Schweizer

Abstract

> L’étude met en lumière les tensions entre les principes juridiques de protection des données personnelles et les pratiques effectives en matière d’anonymisation des décisions judiciaires en Côte d’Ivoire et au Sénégal, tout en proposant des pistes concrètes pour renforcer la transparence judiciaire dans le respect des droits individuels.

L'étude examine le cadre juridique de l'anonymisation des décisions judiciaires publiées en Côte d'Ivoire et au Sénégal, en mettant l’accent sur la protection des données personnelles dans les décisions de justice. Ce travail s'inscrit dans le cadre du projet régional "Promotion de l'État de droit et de la justice en Afrique", visant à améliorer l'accès à la justice et à renforcer la transparence judiciaire tout en respectant les droits des individus concernés.

L'étude analyse les normes juridiques nationales, régionales et internationales en matière de protection des données personnelles. Elle identifie les défis spécifiques liés à la publication des décisions de justice, notamment pour des groupes vulnérables comme les mineurs ou dans des affaires de violence sexuelle et de protection des données personnelles dans des dossiers très médiatisés. Les auteurs examinent les textes régissant la matière et évaluent également les éventuelles lacunes juridiques susceptibles d'entraver une meilleure protection des données. Ils se penchent aussi sur la pratique dans les deux pays en interrogeant un certain nombre de personnes clés à travers des entretiens semi-directifs.

L’étude met en lumière l'importance du principe de proportionnalité et du principe de minimisation qui en découle. Les entretiens avec des professionnels du secteur juridique dans les deux pays, ainsi que l'examen des plateformes de publication des décisions judiciaires existantes, révèlent une certaine divergence entre les principes du droit d’un côté et la pratique du terrain de l’autre.

Des recommandations sont proposées afin de mieux aligner la pratique avec les principes juridiques établis et d’harmoniser les procédures d’anonymisation pour une meilleure protection des données personnelles.

Sigles et abréviations

ARTCI	Autorité de Régulation des Télécommunications/TIC (Côte d'Ivoire)
CNDJ	Centre National de Documentation Juridique (Côte d'Ivoire)
CNIL	Commission Nationale de l'Informatique et des Libertés (France)
CDP	Droits civils et politiques
EPN	Etablissement Public National
ONG	Organisation non gouvernementale
CDP	Commission de Protection des Données Personnelles
CEDEAO	Communauté Économique des États de l'Afrique de l'Ouest
OCDE	Organisation de Coopération et de Développement Économiques
RAPDP	Réseau Africain des autorités de Protection des Données Personnelles
UA	Union Africaine
UE	Union Européenne
UNESCO	Organisation des Nations Unies pour l'Éducation, la Science et la Culture

Table des matières

Sigles et abréviations 4
1. Contexte de l'étude 6
2. Objectifs de l'étude 7
3. Méthodologie 7
3.1 Côte d'Ivoire 7
3.2 Sénégal 9
4. Analyse du cadre juridique 10
4.1 Cadre juridique à l'international et au niveau sous-régional 10
4.1.1 La situation à l'international en matière de protection des données personnelles 10
4.1.2 Le cadre juridique continental et régional de protection des données personnelles 11
4.2 Cadre juridique en Côte d'Ivoire 16
4.2.1 La publication des décisions de justice 16
4.2.2 Loi sur la protection des données à caractère personnel 16
4.2.3 Loi d'accès à l'information 18
4.2.4 Synthèse du cadre juridique en Côte d'Ivoire 19
4.3 Cadre juridique au Sénégal 20
4.3.1 La Loi n° 2008-12 du 25 janvier 2008 portant protection des données à caractère personnel 20
4.3.2 Autres textes 22
4.3.3 Synthèse du cadre juridique au Sénégal 22
4.4 Autres pays d'Afrique de l'Ouest 23
4.5 Comparaison des trois législations 23
5. Pratique en matière d'anonymisation des données dans les décisions de justice 25
5.1 Côte d'Ivoire 25
5.1.1 La plateforme du Tribunal du Commerce 26
5.1.2 La plateforme de la Cour des comptes 26
5.1.3 La plateforme du centre national de documentation juridique 28
5.2 Sénégal 31
5.2.1 Méconnaissance profonde de la notion d'anonymisation des décisions de justice 31
5.2.2 Manque de conscience quant au principe d'anonymisation 31
5.2.3 La commission de Protection des Données Personnelles (CDP) 32
5.2.4 Le projet d'anonymisation de la Cour Supreme 33
5.2.5 La loi générale sur l'accès à l'information 33
6. Situation par rapport aux thématiques de la délinquance juvénile, des violences sexuelles et sexistes et des cas très médiatisés 34
6.1 Sénégal 34
6.2 Côte d'Ivoire 37
7. Conclusions 38
8. Recommandations 39
8.1 Recommandations générales 39
8.2 Recommandations spécifiques pour la Côte d'Ivoire 40
8.3 Recommandations spécifiques pour le Sénégal 41
REFERENCES JURIDIQUES 42
BIBLIOGRAPHIE 43

1 Contexte de l'étude

Le projet régional de la GIZ "Promotion de l'État de droit et de la justice en Afrique" (PRoLA) vise à renforcer l'État de droit et le système judiciaire en Afrique, notamment en Côte d'Ivoire, au Ghana, au Sénégal et en Tanzanie.

Dans ce contexte, l'objectif du module contribue à l'Agenda 2063 de l'Union africaine, "L'Afrique que nous voulons" (Aspiration 3, Objectif 11 sur l'État de droit), ainsi qu'aux Objectifs du Développement Durable (ODD) 5 « égalité des sexes » et 16 « paix, justice et institutions efficaces ».

L'approche méthodologique du projet régional vise à promouvoir l'État de droit en plaidant pour un meilleur accès à la justice dans les tribunaux étatiques et en renforçant les mécanismes de règlement des litiges extrajudiciaires. Par conséquent, le projet régional s'efforce d'améliorer les services juridiques et de prendre des mesures pour renforcer les institutions étatiques et non étatiques dans leurs efforts visant à améliorer l'accès à la justice.

Les résultats attendus du module sont les suivants :

1. Renforcement de l'accès à la justice pour les citoyens vulnérables, en particulier les femmes ;
2. Renforcement de l'accès à la justice pour les acteurs économiques ;
3. Alignement des structures judiciaires avec l'autonomie du pouvoir judiciaire ;
4. Garantie d'un accès facilité à l'information juridique pour les praticiens du droit.

Les recherches montrent que, dans de nombreux pays africains, les tribunaux sont surchargés d'affaires impliquant des citoyens vulnérables et des petits acteurs économiques. Ainsi, il est essentiel de trouver des solutions alternatives et rentables pour régler les conflits. Pour atteindre cet objectif, tous les citoyens et les entreprises privées doivent pouvoir accéder à la justice, soit par le biais des tribunaux publics, soit par des mécanismes extrajudiciaires de règlement des litiges. Cependant, les capacités des organisations gouvernementales et non gouvernementales restent insuffisantes pour garantir un accès adéquat à la justice.

L'étude B, qui retient notre attention, traite du cadre juridique relatif à l'anonymisation des documents judiciaires publiés en Côte d'Ivoire et au Sénégal.

Elle devait non seulement se concentrer sur les réglementations et normes nationales, régionales et internationales applicables en la matière, mais aussi inclure une analyse comparative des réglementations existantes dans d'autres pays francophones d'Afrique de l'Ouest.

Étant donné la vulnérabilité de certains groupes de personnes, l'étude devait également aborder la question de l'anonymisation des données personnelles, notamment dans les cas de délinquance juvénile, de violences sexuelles ou sexistes, ainsi que dans les affaires très médiatisées.

Cette étude visait à mettre en lumière les **exigences légales,** les **conclusions** et les **recommandations en matière de protection des données à caractère personnel lors de la publication des décisions de justice.**

Elle s'est concentrée sur l'analyse des normes juridiques relatives à la protection des données personnelles intervenant dans la publication des décisions de justice, notamment dans les cas de délinquance juvénile, de violence sexuelle ou sexiste, ou d'affaires très médiatisées. Nous avons également cherché à identifier d'éventuelles lacunes ou vides juridiques, où la législation actuelle nécessiterait des évolutions afin de garantir une meilleure protection des données à caractère personnel et d'éviter toute atteinte aux intérêts individuels.

Nous avons également examiné les défis techniques posés par la mise en œuvre de l'anonymisation des données personnelles ainsi que les ressources nécessaires (humaines, matérielles et financières) qui doivent être mobilisées pour garantir une protection efficace des données à caractère personnel.

2 Objectifs de l'étude

- Comprendre les exigences légales applicables en matière de protection des données personnelles lors de la publication des décisions de justice,
- Analyser les normes nationales, régionales et internationales applicables au Sénégal et en Côte d'Ivoire
- Etablir une analyse comparative avec des réglementations existantes dans d'autres pays francophones d'Afrique de l'Ouest

3 Méthodologie

Pour cette étude, nous avons d'abord déterminé le champ exact de la recherche, qui consistait à analyser à la fois le cadre législatif et les pratiques ainsi que les principes régissant la protection des données personnelles lors de la publication des décisions judiciaires.

Pour répondre à cette problématique, nous avons identifié les normes juridiques pertinentes, que nous avons ensuite analysées et interprétées. Par ailleurs, nous avons mené des entretiens individuels semi-directifs avec des experts et des personnes-ressources qualifiées. Enfin, nous avons examiné d'éventuelles solutions techniques en matière de protection des données, notamment sur les plateformes existantes et à venir. Dans une section consacrée au benchmarking, nous avons également étudié les mécanismes de protection des données appliqués à la publication des décisions de justice dans d'autres pays.

3.1 Côte d'Ivoire

En Côte d'Ivoire, nous avons conduit quarante-sept (47) entretiens auprès de professionnels issus de divers secteurs d'activité liés à la justice.

Cet échantillon a été réparti en fonction de la profession et du type d'activité exercé de la manière suivante :

PROFESSION	EFFECTIF
Magistrats	7
Greffiers	9
Avocats	10
ONG	15
Cabinets de professionnels de DCP	3
Journalistes d'investigation	3
Total	**47**

Les entretiens ont été menés dans trois (3) localités : Abidjan, Bouaké et Korhogo.

Ces entretiens, d'une durée moyenne d'une heure et dix (1h10) minutes, ont été réalisés en face-à-face, principalement dans les bureaux des personnes interrogées.

Déroulement des entretiens : Avant la conduite des entretiens, nous redoutions que le sujet de l'anonymisation suscite des inhibitions ou des réticences chez les participants. Cependant, il n'en a rien été. Une fois passés les premiers échanges permettant d'établir un climat de confiance et de rassurer les interlocuteurs sur l'anonymat de l'enquête, les personnes interrogées se sont exprimées librement et avec enthousiasme. Nombre d'entre elles ont estimé être dans leur "bon droit" en abordant les thèmes de l'anonymisation, de la protection de la vie privée et des données personnelles.

Dans certains cas, ces discussions ont conduit à une véritable prise de conscience quant aux risques liés aux manquements en matière d'anonymisation des décisions de justice. Cette prise de conscience s'est parfois accompagnée d'un sentiment de colère et de récriminations à l'égard du "système" en place.

L'entretien a également offert à certains participants une occasion unique d'exprimer un ressenti souvent passé sous silence et insuffisamment pris en compte. En tant qu'acteurs du droit, ils ont fait part d'un certain malaise à agir dans un contexte où la loi sur la protection des données à caractère personnel n'est pas toujours respectée, alors qu'ils la considèrent comme un droit fondamental.

Dans le secteur de la protection des données personnelles, une attitude d'agacement, voire de dénonciation, est apparue face aux pratiques ancrées, jugées pénalisantes et parfois désespérantes pour les cabinets et les employés concernés. Il a ainsi été relevé que le domaine de la protection des Données à Caractère Personnel (DCP) en Côte d'Ivoire est encore à un stade embryonnaire, bien que la loi en la matière existe depuis une dizaine d'années. Selon les acteurs du secteur, le « plafond de verre » n'est pas encore prêt à être brisé.

> L'entretien a offert à certains participants une occasion unique d'exprimer un ressenti souvent passé sous silence [...] alors qu'ils considèrent [la loi] comme un droit fondamental.

Les principaux obstacles mentionnés sont la méconnaissance du cadre juridique, le caractère relativement nouveau du sujet et les difficultés des professionnels pour se mettre en conformité juridique. La publication de données à caractère personnel n'est que l'une des nombreuses manifestations des problèmes structurels qui affectent ce secteur.

3.2 Sénégal

Au Sénégal, l'étude du cadre juridique relatif à l'anonymisation des documents judiciaires constitue une démarche novatrice et encore peu explorée par les acteurs de la justice sénégalaise. Afin d'approfondir cette question, une étude juridique approfondie a été menée et une série d'entretiens a été conduite avec des professionnels du droit et des spécialistes du numérique. Ces échanges ont permis de recueillir des données essentielles pour analyser les pratiques et perceptions relatives à l'anonymisation des décisions de justice.

Ainsi, nous avons réalisé 51 entretiens avec des acteurs et praticiens du droit, ainsi qu'avec d'autres professionnels dont le travail influence directement le cadre de cette étude.

PROFESSION	EFFECTIF
Magistrats	12
Greffiers	7
Avocats	5
Journalistes	3
Société civile	7
Membre de la CDP	3
Universitaires	3
AUTRES : membres de GAINDE 2000, archivistes des tribunaux, étudiants en droit.....	11
Total	**51**

Cette diversité de participants garantit une représentation équilibrée des différentes perspectives professionnelles et des préoccupations relatives à l'anonymisation des documents judiciaires. Les entretiens se sont déroulés sur l'ensemble du territoire sénégalais, bien que la majorité des participants réside dans la région de Dakar.

Ces entretiens, d'une durée moyenne d'une (1) heure, ont été réalisés principalement dans les bureaux des personnes identifiées. Pour certains participants, un entretien téléphonique complété par des échanges de courriels a été privilégié.

Déroulement des entretiens : Les entretiens menés avec les acteurs de la justice ainsi qu'avec d'autres professionnels impliqués dans des projets ou programmes ont été particulièrement enrichissants, en raison de l'importance et de l'actualité du sujet abordé. Les discussions ont porté sur le cadre juridique relatif à l'anonymisation des documents judiciaires au Sénégal, suscitant un vif intérêt parmi les personnes interrogées.

Les participants se sont montrés très ouverts et accessibles. Leur engagement et leur aisance à aborder le sujet ont grandement facilité les échanges. Les informations et les perspectives qu'ils ont partagées ont été d'une grande utilité pour la rédaction et l'analyse de cette étude. Leurs contributions ont permis d'approfondir la compréhension des défis et des opportunités liés à l'anonymisation des décisions de justice, offrant ainsi une meilleure appréhension des enjeux actuels dans ce domaine.

4 Analyse du cadre juridique

4.1 Cadre juridique à l'international et au niveau sous-régional

4.1.1 La situation à l'international en matière de protection des données personnelles

Les normes internationales jouent un rôle essentiel dans l'établissement de principes directeurs pour la protection des données personnelles. L'analyse de ces normes permet d'identifier les standards recommandés en matière de protection des données et d'anonymisation.

Au niveau international, les principaux textes concernés sont :

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe de 2018 avec ses amendements de 1999 (Convention 108+)

- Les lignes directrices de l'Organisation de Coopération et de Développement Economiques (OCDE) relatifs à la protection de la vie privée et des données personnelles de 1980
- Les principes de l'UNESCO relatifs à la protection des données personnelles et de la vie privée de 2018
- La Convention de l'Union Africaine sur la Cybersécurité et la Protection des Données Personnelles de 2014 (Convention de Malabo)
- La Directive sur la protection des Données à Caractère Personnel de la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO) de 2010
- La Loi additionnelle A/SA.1/01/10 relative à la protection des données personnelles au sein de la CEDEAO de 2010
- Le Règlement Général de la Protection des Données (RGPD) de 2018

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe de 2018 avec ses amendements de 1999 (Convention 108+)

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, aussi appelée Convention 108+, est un instrument juridique élaboré par le Conseil de l'Europe. Adoptée en 1981, elle constitue la première convention internationale contraignante traitant de la protection des données personnelles dans le cadre des technologies de l'information et de la communication.

Le Sénégal, parmi huit pays africains et latino-américains, a adhéré à cette convention en 2016.

La Convention 108+ vise à garantir la protection des droits fondamentaux des individus en matière de traitement automatisé des données à caractère personnel. Son article premier stipule que son objectif est de « protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales, notamment du droit à la vie privée. »

Elle établit plusieurs principes fondamentaux, notamment :

- La légitimité du traitement
- La limitation de la finalité
- La qualité des données
- La sécurité du traitement
- La transparence
- Les droits des personnes concernées
- La responsabilité des responsables du traitement

Elle accorde aux individus des droits essentiels, tels que :

- Le droit d'accès aux données les concernant
- Le droit de rectification
- Le droit d'opposition au traitement de leurs données

L'article 5 de la Convention 108+ introduit le principe de minimisation des données, selon lequel:

- Les données doivent être obtenues et traitées de manière loyale et licite
- Elles doivent être collectées pour des finalités déterminées, explicites et légitimes
- Elles doivent être adéquates, pertinentes et non excessives par rapport aux finalités poursuivies
- Elles doivent être exactes et mises à jour si nécessaire
- Leur conservation ne doit pas excéder la durée nécessaire aux finalités pour lesquelles elles sont traitées

Ces obligations garantissent une protection proportionnée et limitée des données personnelles, évitant ainsi leur traitement excessif.

Les lignes directrices de l'Organisation de Coopération et de Développement Economiques (OCDE) relatifs à la protection de la vie privée et des données personnelles

Les principes de l'OCDE relatifs à la protection de la vie privée et des données personnelles, élaborés en 1980, constituent un cadre de recommandations visant à guider les États dans l'élaboration de leurs législations. Bien que non contraignants, ces principes ont influencé de nombreux textes nationaux et internationaux, notamment la Directive 95/46/CE de l'Union européenne, qui a précédé le RGPD.

Les principes clés de l'OCDE incluent :

- Collecte loyale et licite des données
- Limitation de la finalité et pertinence des données collectées
- Exigence de qualité et de mise à jour des données
- Transparence et information des personnes concernées

Aujourd'hui encore, ces principes jouent un rôle central dans la définition des standards internationaux en matière de protection des données personnelles.

Les principes de l'UNESCO relatifs à la protection des données personnelles et de la vie privée

L'UNESCO, institution spécialisée des Nations Unies, s'engage à traiter les données personnelles de manière responsable et non discriminatoire, en tenant compte des questions de genre.

Les principes relatifs à la protection des données personnelles et de la vie privée ont été adoptés officiellement par le Comité de haut niveau sur la gestion des Nations Unies lors de sa 36e réunion en octobre 2018.

L'UNESCO définit les données personnelles comme toute information permettant d'identifier directement ou indirectement un individu. Elle utilise le terme « traitement des données » pour désigner toutes les opérations effectuées sur ces données, y compris la collecte, le stockage, l'utilisation, le transfert et l'effacement.

4.1.2 Le cadre juridique continental et régional de protection des données personnelles

En Afrique, la protection des données personnelles est une préoccupation croissante. Bien que le continent ne dispose pas encore d'un cadre juridique régional contraignant comparable au RGPD européen, certaines initiatives ont vu le jour.

La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (Convention de Malabo – 2014)

En 2011, l'Union africaine (UA) a initié un projet de convention sur la cybersécurité en Afrique. Après plusieurs révisions, ce projet a abouti à l'adoption de la Convention de Malabo en 2014, lors du 23e sommet de l'UA en Guinée équatoriale.

L'objectif principal de cette convention est de protéger les données personnelles et de renforcer la confiance numérique sur le continent africain. Toutefois, elle n'est pas encore entrée en vigueur,

car elle nécessite la ratification de 15 États membres. En date de juin 2021, seuls 9 pays (Angola, Ghana, Guinée, Mozambique, Île Maurice, Namibie, Rwanda, Sénégal et Zambie) l'avaient ratifiée.

Cette convention vise à :

- Établir un cadre juridique crédible pour la protection des données en Afrique
- Encourager la création d'autorités de protection des données dans les États membres
- Garantir une libre circulation des données tout en protégeant les droits fondamentaux

La Convention de Malabo constitue une avancée majeure pour la cybersécurité et la protection des données en Afrique. Toutefois, son adoption tardive et son entrée en vigueur limitée freinent son impact effectif sur le continent.

La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles est censée servir de référence pour les législations sur la protection des données sur le continent. Ses articles 8(1) et 8(2) visent à établir un cadre juridique assurant la protection des données personnelles et un mécanisme garantissant que leur traitement respecte les **droits fondamentaux** des individus. Cette approche reflète une prise de conscience croissante de Etats africains de l'importance de concilier protection des droits individuels et sécurité numérique.

En adoptant cette convention, les États membres de l'Union africaine manifestent leur engagement à créer un environnement numérique sûr et harmonisé. Cette initiative traduit aussi la reconnaissance de la nécessité de normes régionales adaptées aux défis spécifiques de la cybersécurité et de la protection des données en Afrique.

Directive sur la protection des Données à Caractère Personnel de la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO)

En janvier 2010, la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO) a adopté une directive sur la protection des données personnelles afin d'harmoniser les législations des États membres. Cette directive reflète la volonté des pays de la sous-région d'adopter des normes communes dans un contexte marqué par l'essor rapide des technologies de l'information et de la communication (TIC).

La directive joue un rôle clé en :

- Établissant un cadre juridique cohérent et harmonisé facilitant les échanges de données au sein de la région ;
- Garantissant le respect des droits des individus en matière de traitement des données personnelles ;
- Encourageant la coopération entre États membres pour une mise en œuvre efficace des normes adoptées.

Elle met également l'accent sur la nécessité, pour chaque État membre, d'adopter des réglementations nationales adaptées, et de renforcer les capacités institutionnelles chargées de leur application.

Loi additionnelle A/SA.1/01/10 relative à la protection des données personnelles au sein de la CEDEAO

En février 2010, la CEDEAO a adopté la Loi additionnelle A/SA.1/01/10, qui vise à établir un cadre normatif détaillé sur la protection des données personnelles dans la région.

Cette loi définit plusieurs concepts clés, tels que :

- Consentement
- Autorité de protection des données
- Données personnelles et données sensibles
- Responsable du traitement et sous-traitant
- Données relatives à la santé

Cependant, elle ne précise pas certaines notions importantes comme le profilage, l'anonymisation, la pseudonymisation ou encore la violation des données personnelles.

Elle impose à chaque État membre de mettre en place une Autorité nationale indépendante de protection des données, dotée des moyens nécessaires pour garantir :

- Son impartialité
- Son secret professionnel
- L'exercice de ses responsabilités et pouvoirs

Concernant les droits des personnes concernées, la loi reconnaît notamment le droit à l'information sur l'usage qui est fait de leurs données personnelles.

Enfin, elle définit les obligations du responsable du traitement, notamment en matière de confidentialité, de sécurité, de conservation et de durabilité des données. Ces obligations sont en grande partie alignées avec les principes fondamentaux de protection des données en vigueur à l'échelle internationale.

Protocole MOU entre l'alliance Smart Africa (SA) et le NADPA/RAPDP

L'alliance Smart Africa (SA) et le NADPA/RAPDP (Réseau Africain des Autorités de Protection des Données Personnelles) ont signé un protocole d'accord entré en vigueur le 10 mars 2022 à Dakar.

Présentation des acteurs

- Smart Africa est une alliance regroupant 32 pays africains, des organisations internationales et des entreprises privées, avec pour objectif de promouvoir le développement du numérique en Afrique. Créée en 2013, elle représente aujourd'hui plus de 815 millions de personnes.
- Le NADPA/RAPDP est un réseau d'autorités nationales africaines ayant pour mission de promouvoir la protection des données personnelles et de la vie privée comme un droit humain fondamental. Il a été créé en 2016 à Ouagadougou, lors du 2e Forum africain des Autorités de Protection des Données Personnelles.

Objectifs du protocole d'accord

Cet accord vise à renforcer la coopération panafricaine en matière de protection des données. Il repose sur les engagements suivants :

- Soutenir les États africains dans l'élaboration ou la mise à jour de leur législation sur la protection des données et la création d'autorités nationales compétentes ;
- Harmoniser les politiques et réglementations en matière de protection des données en Afrique;
- Développer des formations conjointes pour les autorités africaines de protection des données à travers la Smart Africa Digital Academy (SADA) ;
- Favoriser la coopération juridique entre les autorités africaines pour soutenir la digitalisation du continent.

Effets extraterritoriaux du Règlement Général sur la Protection des Données (RGPD) de l'UE

Le Règlement Général sur la Protection des Données (RGPD), adopté le 27 avril 2016, vise à renforcer la protection des données personnelles dans l'Union européenne. Bien qu'il s'applique principalement aux pays de l'UE, son effet extraterritorial signifie qu'il peut aussi concerner des personnes et entités établies hors de l'Europe.

L'article 3(1) du RGPD stipule que :

> « Le présent règlement s'applique au traitement de données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union, que ce traitement ait lieu ou non dans l'Union. »

Selon ce critère, il n'est pas nécessaire que le traitement des données ait lieu sur le territoire de l'UE, le simple fait que l'établissement du responsable du traitement des données se trouve sur le territoire de l'UE est suffisant pour l'application du RGPD. La réglementation a donc également des effets extraterritoriaux en dehors de l'Union Européenne, ce qui fait qu'il s'agit d'un texte juridique avec un champ d'application qui produit également des effets en Côte d'Ivoire et au Sénégal.

Le RGDP n'entre pas en ligne de compte en ce qui concerne la publication des jugements des tribunaux lorsqu'il s'agit de la publication classique en format papier ou en format audio-visuel. Cela vaut aussi bien pour la publication en format papier dans un organe de publication ou dans une revue juridique spécialisée que pour la publication dans les médias.

Mais en cas de publication sur Internet, le RGDP joue un rôle si le responsable du traitement des données est établi dans l'Union européenne. Dans certaines constellations cela peut être le cas. Mais ce n'est pas systématique, car le responsable du traitement des

données sera souvent établi en en dehors de l'UE, soit en Afrique, soit en Amérique ou en Asie.

A cause de l'applicabilité indirecte, il convient ici de mentionner les dispositions du RGDP relatives à la publication de données à caractère personnel dans le cadre de décisions de justice, pour les cas où la publication des décisions de justice ivoirienne ou sénégalaise soit faite avec le concours d'un responsable de traitement installé sur le territoire de l'UE.

Le Règlement Général sur la Protection des Données (RGPD) n'interdit pas en tant que telle la publication des décisions de justice sur internet, mais impose des règles strictes pour la protection des données personnelles dans ce cadre. Les décisions de justice peuvent être publiées, car cela répond à un principe de transparence et d'information du public. Toutefois, certaines mesures doivent être prises pour protéger la vie privée des individus concernés.

Le RGPD impose que seules les données strictement nécessaires soient publiées. Cela signifie que les jugements et arrêts doivent exclure les informations personnelles sans rapport avec l'affaire ou non nécessaires à la compréhension du public.

L'article 5 (1) du RGPD impose le principe de minimisation des données à caractère personnel. Cet article établit que les données personnelles publiées doivent être : « **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées ».

Le principe de minimisation des données signifie que seules les informations personnelles strictement nécessaires pour atteindre le but du traitement (ici, l'information du public à travers la publication de décisions de justice) doivent être incluses dans le traitement informatique. Autrement dit, dans le cadre de la publication des décisions de justice, cela implique que les informations personnelles qui ne sont pas essentielles à la compréhension de l'affaire, ou sans lien direct avec l'objectif de la publication, doivent être omises ou anonymisées.

Le principe de minimisation des données à caractère personnels se trouve d'ailleurs aussi dans le droit français. La loi française n° 2018-493 relative à la protection des données personnelles modifie le cadre législatif français, notamment la loi Informatique et Libertés (loi n° 78-17 du 6 janvier 1978), pour se conformer au RGPD. Elle ne répète pas spécifiquement tous les principes énoncés dans le RGPD mais les incorpore, en insistant ainsi sur l'applicabilité du principe de minimisation en France.

Application de l'article 5(1)(c) aux cas de décisions de justice

Dans la pratique, l'article 5(1)(c) du RGDP s'applique à la publication des décisions de justice de la manière suivante :

- Anonymisation des parties privées afin d'éviter une identification directe ou indirecte des individus concernés.
- Exclusion des informations personnelles non pertinentes, c'est-à-dire celles qui n'ont pas d'impact sur la compréhension publique de la décision judiciaire.
- Limitation des données publiées aux informations strictement nécessaires, garantissant un équilibre entre le droit à l'information du public et le droit au respect de la vie privée.

Bien que l'article 5(1)(c) soit central, le Considérant 39 du RGPD précise également ce principe en affirmant que :

> « Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement. »

Cela implique aussi des obligations de protection renforcée pour les données sensibles, notamment celles publiées dans le cadre de décisions judiciaires.

Le RGPD prévoit également des dispositions spécifiques pour certaines catégories de personnes en raison de la sensibilité de leurs données. L'article 9(1) du RGPD stipule que :

« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, est interdit.»

Dans ces cas, les obligations de protection des données sont renforcées.

Ainsi, il apparaît que le RGPD n'interdit pas la publication des décisions de justice en ligne. Cependant, il impose des précautions strictes et des pratiques d'anonymisation afin de protéger les données personnelles des individus concernés.

Lorsque la publication a lieu en ligne, le RGPD impose les restrictions suivantes :

- **Anonymisation des parties privées**

Dans les décisions de justice publiées, les noms des parties privées (c'est-à-dire les personnes physiques non publiques) doivent être anonymisés. Cette anonymisation consiste généralement à remplacer les noms et prénoms par des initiales ou par des termes génériques tels que "Monsieur X" ou "Madame Y".

L'objectif est de réduire l'impact sur la vie privée des parties concernées et de garantir le respect de leur droit à la protection de leurs données personnelles.

- **Exceptions pour les personnes publiques**

Les noms des professionnels du droit (juges, avocats, procureurs) et des institutions publiques peuvent rester visibles. Toutefois, même dans ces cas, le principe de minimisation demeure applicable :

Seules les informations pertinentes pour la compréhension de la décision doivent être publiées.

- **Principe de minimisation**

Le RGPD impose que seules les données strictement nécessaires soient publiées. Ainsi, les jugements et arrêts doivent exclure :

  - Les informations personnelles sans lien direct avec l'affaire.
  - Les informations non nécessaires à la compréhension du public.

- **Droits des individus concernés**

Les individus concernés par une publication peuvent exercer certains droits, notamment le droit à l'effacement (aussi appelé "droit à l'oubli") dans certaines situations.

Cela signifie qu'une personne peut, sous certaines conditions, demander la suppression de ses données personnelles d'une décision de justice publiée en ligne, surtout si cette publication lui porte préjudice dans sa vie privée.

- **Encadrement légal national**

Les lois nationales en matière de protection des données viennent compléter le RGPD afin d'encadrer la publication des décisions de justice.

Outre les dispositions internationales, il est essentiel d'examiner les cadres juridiques internes de la Côte d'Ivoire et du Sénégal.

4.2 Cadre juridique en Côte d'Ivoire

4.2.1 La publication des décisions de justice

Aucun texte n'encadre la publication des décisions de justice en Côte d'Ivoire. Toutefois, si la loi le prévoit expressément, certaines mesures relatives à la sécurité des personnes concernées peuvent être prises avant la publication. Mais, dans l'ensemble, nos interlocuteurs ont été formels : « En Côte d'Ivoire, il n'existe pas de principe qui gouverne la publication des décisions de justice. »

Les décisions de justice sont rendues au nom du peuple de Côte d'Ivoire et sont **publiques,** sauf disposition contraire. Cette publicité vise à assurer **la transparence du système judiciaire.**

Nous allons examiner si d'autres textes de loi, bien qu'ils ne se réfèrent pas expressément à la publication des décisions de justice, contiennent des éléments permettant d'empêcher la divulgation de certaines données à caractère personnel.

4.2.2 Loi sur la protection des données à caractère personnel

La vie privée se réfère à la sphère personnelle d'un individu, comprenant ses informations, ses activités et ses relations, qui ne sont pas destinées à être partagées ou exposées publiquement sans son consentement. Cela englobe un large éventail d'aspects de la vie quotidienne, notamment les communications privées, les données personnelles, les lieux visités, les habitudes, les informations judiciaires et les données de santé.

La **protection de la vie privée** est un concept fondamental dans de nombreuses sociétés et est souvent reconnue comme un droit fondamental. Les lois sur la protection de la vie privée varient d'un pays à l'autre, mais elles ont généralement pour objectif de protéger les individus contre la collecte, l'utilisation et la diffusion non autorisées de leurs informations personnelles. Avec l'avènement de la technologie numérique et de l'Internet, la protection de la vie privée est devenue un sujet particulièrement crucial.

Les préoccupations majeures concernent la divulgation en ligne d'informations privées, la collecte de données par les entreprises, la surveillance gouvernementale et d'autres aspects liés à la vie moderne. Ces sujets sont au cœur de nombreux débats et de l'élaboration de législations spécifiques.

L'un des principaux objectifs de **la loi ivoirienne n° 2013-450 du 19 juin 2013 portant sur la protection des données à caractère personnel** est d'assurer la protection de la vie privée en encadrant l'utilisation des informations personnelles détenues par des institutions. La loi établit des règles strictes concernant la collecte, l'utilisation, la divulgation, l'exactitude, la conservation, la sécurité et la suppression des renseignements personnels.

L'Autorité de Régulation des Télécommunications/ TIC de Côte d'Ivoire (ARTCI) est l'institution chargée de veiller sur la protection des données personnelles en vertu de cette loi.

Principes fondamentaux de la loi sur la protection des données à caractère personnel

Les principes fondamentaux de cette loi reposent sur les éléments suivants :

- **Consentement informé:** les individus doivent être informés de la collecte, de l'utilisation et de la divulgation de leurs données personnelles et doivent donner leur consentement de manière éclairée.
- **Finalité limitée:** les informations personnelles doivent être collectées pour des finalités spécifiques et légitimes, et ne doivent pas être utilisées à des fins incompatibles avec celles initialement prévues.
- **Minimisation des données:** les organisations doivent collecter uniquement les informations nécessaires pour atteindre la finalité spécifiée, en évitant la collecte excessive de données.
- **Exactitude des données:** les informations personnelles doivent être exactes, mises à jour et corrigées si nécessaire. Les individus ont le droit de mettre à jour ou de rectifier leurs données.
- **Sécurité des données :** les organisations doivent mettre en place des mesures de sécurité appropriées pour protéger les informations personnelles contre tout accès non autorisé, divulgation, perte ou destruction.
- **Durée de conservation limitée :** les données personnelles ne doivent être conservées que pour la durée strictement nécessaire à la finalité prévue, sauf si une période de conservation plus longue est légalement requise.
- **Droits d'accès et de correction :** les individus doivent pouvoir accéder à leurs informations personnelles détenues par une organisation et demander leur correction si nécessaire.
- **Transparence :** les organisations doivent être transparentes quant à leurs pratiques de collecte, d'utilisation et de divulgation des informations personnelles et fournir des informations claires sur leur politique de confidentialité.
- **Responsabilité :** les organisations sont responsables de la protection des informations personnelles qu'elles collectent et traitent, même lorsqu'elles font appel à des tiers.

Lien entre la loi ivoirienne et la publication des décisions de justice

La loi de 2013 sur la protection des données à caractère personnel ne traite pas expressément la question de la divulgation d'informations personnelles dans les décisions de justice. Toutefois, le principe de minimisation des données, qui figure dans cette loi, doit aussi être appliqué dans ce contexte lorsque les décisions de justice publiées en ligne contiennent des informations à caractère personnel.

L'article 16 de la loi établit les conditions générales

du traitement des données, notamment en matière de finalité, de proportionnalité et de pertinence des données collectées et traitées. Il stipule que :

> « Les données à caractère personnel doivent être collectées et traitées de manière loyale, légitime et légale. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. »

Ce principe signifie que :

- Les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes.
- Le traitement des données doit être pertinent et ne pas excéder les finalités initiales.

Ainsi, seules les données strictement nécessaires pour atteindre l'objectif déclaré doivent être collectées et traitées, afin d'éviter toute collecte excessive ou inutile.

Le principe de minimisation des données en Côte d'Ivoire est très proche de celui du RGPD européen. Bien que la formulation diffère légèrement, leur portée est similaire : limiter l'usage des données personnelles aux informations strictement nécessaires pour protéger la vie privée des individus.

Il convient donc d'interpréter le principe de minimisation contenu dans la législation ivoirienne de manière similaire au contexte européen. . Cela implique que cette règle doit s'appliquer à la collecte, au traitement et au stockage des données personnelles lors de la publication des décisions de justice.

Une telle interprétation du principe est sans alternative eu égard à son contexte et au but recherché par l'article 16 de la loi de 2013 sur la protection des données à caractère personnel ne. Elle permettra **d'améliorer de manière significative la protection des droits des personnes concernées par les décisions de justice.**

Application concrète du principe de minimisation des données

Dans la pratique, ce principe signifie que les entités qui **publient, collectent ou traitent** des données personnelles doivent :

- Éviter de collecter des informations superflues ou sans lien avec la finalité du traitement.
- Limiter les données publiées ou traitées aux informations essentielles, notamment dans les contextes sensibles comme la publication de décisions de justice.
- Garantir que les données personnelles non strictement nécessaires soient :
  - » Anonymisées ;
  - » Non collectées ;
  - » Supprimées après le traitement.

En cas de non-respect de ce principe, la loi prévoit des sanctions administratives et pénales, sous le contrôle de l'ARTCI. Cette institution est responsable de la protection des données personnelles en Côte d'Ivoire.

Dans ce contexte, il est essentiel de souligner le lien étroit entre le principe de minimisation des données et celui de proportionnalité. Ces deux principes sont complémentaires et jouent un rôle crucial dans la gestion des données personnelles.

Le **principe de minimisation** exige que seules les données strictement nécessaires soient collectées, conservées et traitées, en fonction des finalités spécifiques du traitement. Autrement dit, il s'agit de réduire la quantité de données collectées afin de limiter les risques de collecte excessive et d'intrusion dans la vie privée.

Le **principe de proportionnalité**, quant à lui, est un principe plus large qui vise à garantir que les moyens mis en œuvre pour atteindre un objectif soient appropriés et non excessifs par rapport à cet objectif. Dans le contexte de la protection des données personnelles, cela signifie que le traitement des données doit être justifié et ne doit pas aller au-delà de ce qui est strictement nécessaire pour réaliser les finalités visées.

4.2.3 Loi d'accès à l'information

La **loi n° 2013-867 du 23 décembre 2013, relative à l'accès à l'information d'intérêt public**, également appelée loi sur la liberté de l'information, est une législation qui vise à promouvoir la transparence gouvernementale en permettant au public d'accéder à certaines informations détenues par les

organismes publics.

Cette loi a été conçue pour garantir aux citoyens :

- La possibilité de connaître les activités du gouvernement
- Le droit de demander des informations officielles
- Une meilleure transparence des processus décisionnels

Principes fondamentaux du droit d'accès à l'information

Les principes de cette loi se définissent comme suit :

- **Principe de transparence:** les autorités publiques sont tenues de rendre accessibles un certain nombre d'informations au public.
- **Droit d'accès:** les individus ont le droit de demander et de recevoir des informations détenues par des organismes publics.
- **Étendue de l'information:** la loi précise les types d'informations accessibles au public (documents administratifs, décisions gouvernementales, données budgétaires, etc.).
- **Procédure de demande:** des procédures claires sont définies pour les demandes d'information, y compris les délais de réponse et les recours en cas de refus.
- **Exceptions:** l'accès à certaines informations peut être restreint pour des raisons de sécurité nationale, de confidentialité ou d'autres motifs légitimes.
- **Protection des informations sensibles:** des mesures de protection sont prévues pour les informations confidentielles.
- **Responsabilité:** les organismes publics sont responsables de la gestion et de la divulgation appropriée des informations publiques.
- **Sanctions:** des sanctions peuvent être appliquées en cas de violation de la loi, qu'il s'agisse d'un refus injustifié de fournir une information ou d'une divulgation inappropriée d'informations confidentielles.

Cependant, la loi sur la liberté d'information n'oblige nullement de publier les données à caractère personnelle lors de la publication en ligne des décisions de justice.

Autres législations applicables

En Côte d'Ivoire, deux autres lois peuvent être pertinentes dans ce contexte :

- Loi N02018-570 du 13 juin 2018 relative à la protection des témoins, victimes, dénonciateurs, experts et autres personnes concernées

L'article 7.2 de cette loi prévoit des dispositions pour protéger l'identité, la vie privée et les données à caractère personnel des témoins, victimes, dénonciateurs, experts et autres personnes concernées.

Toutefois, cette protection ne s'applique qu'aux personnes admises dans un programme de protection, en vertu de cette loi.

Ainsi, cette loi n'a qu'un effet indirect et ne concerne que des cas isolés en matière d'anonymisation des décisions de justice.

- Loi n° 2013-450 du 19 juin 2023 relative à la lutte contre la cybercriminalité

L'article 21 de cette loi fait référence aux données à caractère personnel. Il prévoit que sera puni :

> « Quiconque procède à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable par écrit à recevoir de telles prospections. »

Cependant, ce cas ne concerne pas la divulgation de données personnelles lors de la publication des décisions de justice.

4.2.4 Synthèse du cadre juridique en Côte d'Ivoire

En somme, ni la loi de 2013 relative à l'accès à l'information d'intérêt public, ni la loi de 2018 relative à la protection des témoins, victimes, dénonciateurs, experts et autres personnes concernées, ni la loi de 2013 relative à la lutte contre la cybercriminalité ne concernent pas la question de l'anonymisation des données personnelles lors de la publication des décisions de justice.

Par contre, le principe de minimisation des données, inscrit dans la loi n° 2013-450 du 19 juin 2013 sur la protection des données à caractère personnel, doit être interprété de manière à garantir aussi la protection des données lors de la publication en ligne des décisions de justice.

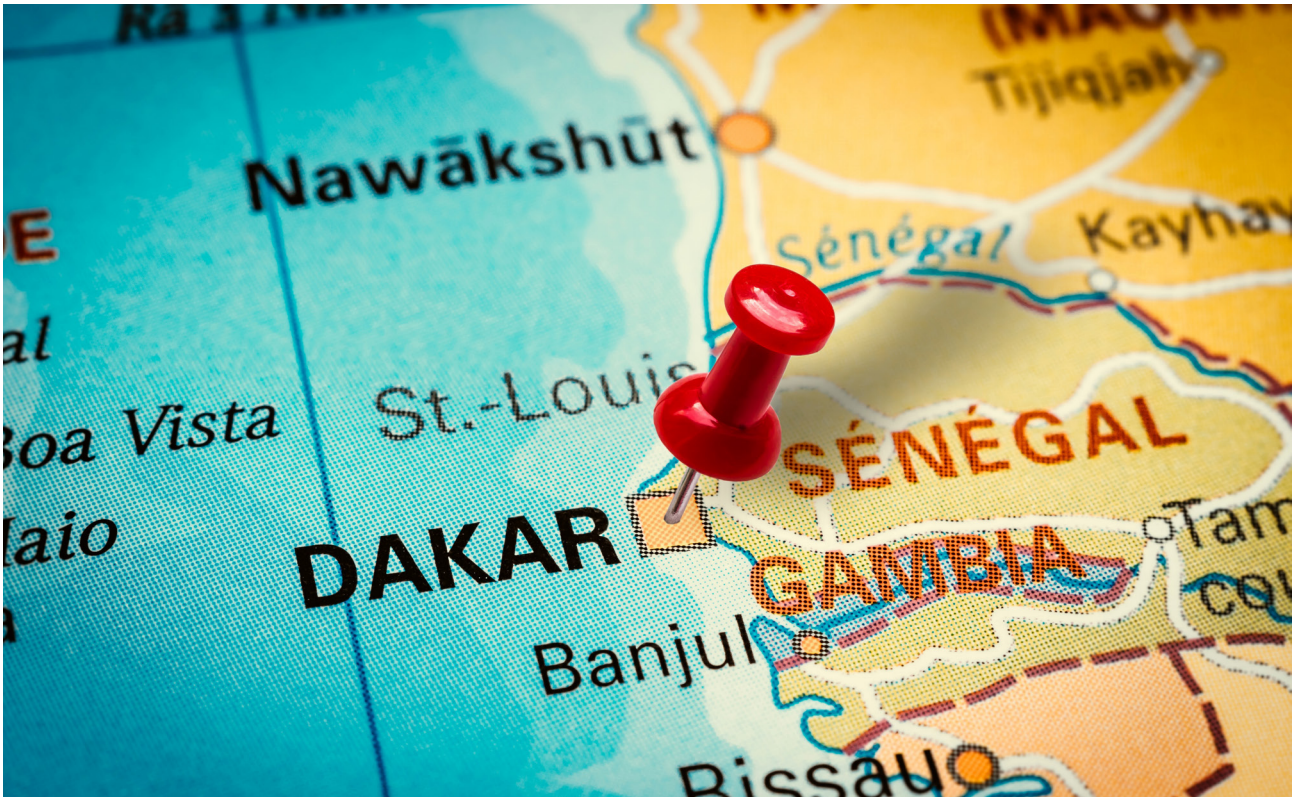
En effet, lors de la publication des décisions de justice, les informations personnelles qui ne sont pas essentielles à la compréhension de l'affaire, ou qui n'ont pas de lien direct avec l'objectif de la publication, doivent être supprimées ou anonymisées.

Reconnaissance du principe de protection des données en Côte d'Ivoire

Ce raisonnement conduit à la conclusion que, dans le droit interne ivoirien, le principe de protection des données à caractère personnel existe bien.

Il reste à examiner, dans la partie consacrée à l'étude des pratiques en Côte d'Ivoire, si les instances et agents chargés de la publication des décisions de justice tiennent effectivement compte de ce principe.

4.3 Cadre juridique au Sénégal



Au Sénégal, le principal texte de référence en matière de protection des données personnelles est la loi n° 2008-12 du 25 janvier 2008, portant sur la protection des données à caractère personnel, complétée par le décret d'application n° 2009-1113 du 21 septembre 2009.

4.3.1 La Loi n° 2008-12 du 25 janvier 2008 portant protection des données à caractère personnel

Pour le Sénégal, cette législation constitue le cadre juridique de référence en matière de collecte, traitement, conservation et divulgation des données personnelles.

La protection des données personnelles dans un pays repose généralement sur un cadre juridique spécifique qui établit les droits et responsabilités des acteurs impliqués dans leur traitement. Le Sénégal est l'un des premiers pays africains à avoir adopté une loi sur la protection des données personnelles.

La **loi n° 2008-12 du 25 janvier 2008** constitue le fondement juridique de la protection des données personnelles au Sénégal. Cette loi a été complétée par le décret d'application n° 2009-1113 du 21 septembre 2009. Elle définit les principes fondamentaux et les dispositions spécifiques qui encadrent la collecte, le traitement et la conservation des données personnelles.

La loi définit les données à caractère personnel comme toute information relative à une personne physique identifiée ou identifiable. Elle précise que ces données peuvent inclure :

- Le nom et l'adresse
- Un identifiant unique
- Des informations sensibles telles que les données de santé ou de vie sexuelle

Elle établit également des principes de base pour le traitement des données personnelles, notamment :

- Licéité, loyauté et transparence
- Finalité déterminée
- Pertinence et proportionnalité
- Durée de conservation limitée

Le traitement des données personnelles est considéré comme légitime si la personne concernée donne son consentement. Toutefois, des exceptions sont prévues, notamment par l'article 33, qui permet de déroger à cette exigence dans certains cas.

De plus, l'article 47 de la loi interdit toute prospection directe sans consentement préalable de la personne concernée.

La loi sénégalaise protège les droits des individus en prévoyant plusieurs garanties :

- Obligation d'information et de transparence (articles 58 et suivants)
- Droit d'accès aux données (article 62)
- Droit d'opposition (article 68)
- Droit de rectification et de suppression (article 69)

Toutefois, elle ne mentionne ni le droit à la limitation du traitement, ni le droit à la portabilité des données.

L'article 39 précise que le responsable du traitement doit s'assurer que son sous-traitant offre des garanties suffisantes en matière de mesures techniques et organisationnelles.

L'article 71 impose au responsable du traitement de prendre toutes les précautions nécessaires pour éviter que les données ne soient altérées, endommagées ou accessibles à des tiers non autorisés.

L'article 9 de la loi de 2008 stipule que le traitement des données personnelles doit respecter certaines conditions, notamment le consentement de la personne concernée, sauf si le traitement est autorisé par la loi.

La publication des décisions de justice pourrait être considérée comme une exception à cette règle, si elle relève de :

- L'intérêt public
- L'exercice d'une mission de service public

Toutefois, il est essentiel que cette publication respecte le principe de proportionnalité et ne divulgue que les informations nécessaires à l'objectif poursuivi.

Des mesures de sécurité doivent également être mises en place afin d'éviter :

- Tout accès non autorisé aux données
- Toute utilisation abusive des informations publiées

Ainsi, en plus d'énoncer les droits des individus sur leurs données, la loi sur la protection des données établit également les obligations des entités qui collectent et traitent ces informations, y compris lors de la publication en ligne.

Le principe de proportionnalité comprend également le principe de minimisation des données, ce qui a déjà été analysé dans le cas de la Côte d'Ivoire. Ce principe s'applique donc également au cadre sénégalais.

Comme expliqué précédemment, ce principe est étroitement lié au principe de proportionnalité. Il exige que le traitement des données soit justifié et ne dépasse pas ce qui est strictement nécessaire pour atteindre la finalité visée.

Ce principe découle des dispositions de l'article 34 et de l'article 35 (2) de la loi n° 2008-12 :

- L'article 34 stipule que « la collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse. »
- L'article 35 (2) précise que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées.

Ces formulations sont identiques à celles de l'article 16 de la loi ivoirienne de 2013 sur la protection des données.

Il est donc logique de conclure que le principe de minimisation des données prévu par la loi sénégalaise produit les mêmes effets que ceux déjà décrits pour la Côte d'Ivoire.

Autorité de protection des données et sanctions en cas de non-respect de la loi

Une caractéristique essentielle de la loi sénégalaise est la création d'une autorité indépendante, chargée de veiller au respect des règles de protection des données personnelles.

L'Autorité de Protection des Données à Caractère Personnel (APDP) joue un rôle clé en :

- Émettant des directives
- Résolvant des plaintes
- Promouvant les bonnes pratiques en matière de protection des données

La loi prévoit des sanctions en cas de non-respect de ses dispositions, sous deux formes :

Sanctions administratives

- Avertissement au responsable du traitement en cas de manquement aux obligations légales
- Mise en demeure de mettre fin aux infractions constatées
- Retrait provisoire de l'autorisation, d'une durée de 3 mois, pouvant devenir définitif en l'absence de mise en conformité

Sanctions pénales

- Peine d'emprisonnement de 1 à 7 ans
- Amende de 500 000 à 10 millions de francs CFA

4.3.2 Autres textes

Il y a quelques autres textes au Sénégal qui pourraient nous intéresser dans le contexte de l'anonymisation des données à caractère personnel. Il s'agit de textes suivants :

- Loi n°2008-11 du 25 janvier 2008 portant sur la Cybercriminalité
- Loi n°2008-08 du 25 janvier 2008 sur les transactions électroniques
- Loi n°2008-41 du 20 août 2008 portant sur la cryptologie

Ces textes ne contiennent rien quant à la question de la protection des données à caractère personnel lors de la publication des décisions de justice.

4.3.3 Synthèse du cadre juridique au Sénégal

Il faut donc noter que bien que le texte de la loi sénégalaise n° 2008-12 du 25 janvier 2008 portant protection des données à caractère personnel ne parle pas expressément de l'anonymisation des décisions de justice lors de la publication, le principe de minimisation qui est contenu dans la loi est une application du principe de proportionnalité sur le traitement des données a une incidence sur la publication des données personnelles lors de la publication des décisions de justice. Cela a comme conséquence que toute donnée non essentielle (comme les informations personnelles) doit être soit anonymisée, soit supprimée si elle n'est pas cruciale pour la compréhension du jugement.

Par ailleurs, l'application du principe de minimisation des données personnelles lors de la publication des décisions de justice au Sénégal s'impose aussi par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe de 2018 avec ses amendements de 1999 (Convention 108+). Comme cela a été expliqué ci-dessus, le Sénégal a adhéré depuis 2016 à ladite Convention.

4.4 Autres pays d'Afrique de l'Ouest

Le cas du Mali

Le Mali a adopté la loi n° 2019-044 du 22 juillet 2019 relative à la protection des données à caractère personnel. Cette loi définit les catégories de données personnelles régies par la législation, ainsi que les principes fondamentaux applicables à leur traitement, notamment les principes de licéité, loyauté et transparence.

Elle établit également les droits des personnes concernées et précise les obligations des parties prenantes impliquées dans le traitement des données. Parmi ces droits, figurent :

- Le droit d'accès
- Le droit de rectification
- Le droit d'opposition
- Le droit de suppression

Concernant le consentement, celui-ci doit être libre, spécifique et éclairé.

La loi régule aussi les transferts internationaux de données personnelles, en imposant des garanties spécifiques à respecter.

Elle a également conduit à la création d'une autorité de protection des données, l'Agence de Régulation des Télécommunications/TIC du Mali, chargée non seulement de veiller à la mise en œuvre de la loi, mais aussi de garantir son respect.

Enfin, cette loi prévoit des sanctions en cas de non-conformité, qui peuvent inclure des amendes et des sanctions pénales.

Comme en Côte d'Ivoire et au Sénégal, la loi malienne n° 2019-044 encadre strictement le traitement des données personnelles en appliquant le principe de minimisation. Ce principe oblige les responsables de traitement à limiter la collecte et la conservation des données aux strictes nécessités des finalités déclarées. La loi exige également que le traitement des données soit proportionné aux objectifs poursuivis, garantissant une utilisation respectueuse et justifiée des informations personnelles des individus.

4.5 Comparaison des trois législations

L'analyse comparative des législations relatives à la protection des données à caractère personnel en **Côte d'Ivoire, au Sénégal et au Mali** révèle plusieurs **similitudes:**

1. Des textes de loi relativement similaires : les trois pays ont adopté des lois structurées de manière comparable, définissant le champ d'application, les principes fondamentaux et

les responsabilités des parties prenantes.

2. Une reconnaissance des droits fondamentaux : le droit d'accès, de rectification et d'opposition est expressément reconnu dans les trois législations. Des procédures spécifiques sont prévues pour exercer ces droits.

3. Le consentement comme base du traitement des données : les lois énoncent les conditions d'un consentement valide, permettant la collecte et la divulgation des données personnelles.

4. Des normes de sécurité strictes : elles garantissent la confidentialité et l'intégrité des données, imposant aux responsables du traitement des obligations précises en matière de protection.

Les trois législations ne traitent pas explicitement l'anonymisation des données personnelles lors de la publication des décisions de justice.

Néanmoins, l'obligation d'anonymisation est inhérente au principe de minimisation des données et au principe de proportionnalité, qui sont inscrits dans les trois législations nationales.

Les lois sur la protection des données personnelles dans les décisions de justice adoptent des standards convergents, inspirés :

- Du Règlement Général sur la Protection des Données (RGPD) de l'Union européenne
- De la Convention 108+ du Conseil de l'Europe
- Des cadres juridiques sous-régionaux

Le principe de minimisation des données est souvent associé aux notions de pertinence, nécessité et proportionnalité.

Pour évaluer l'application effective de l'anonymisation des décisions de justice, il est essentiel d'examiner les pratiques sur le terrain.

Une question se pose alors : l'interprétation des lois sur la protection des données personnelles a-t-elle eu un impact sur la pratique de l'anonymisation des décisions de justice ?

> Il n'existe aucune procédure d'anonymisation, ni aucun service dédié à cette tâche dans les greffes d'Abidjan, de Bouaké et de Korhogo.

Ce point est particulièrement crucial dans les affaires impliquant des groupes vulnérables, tels que :

- Les mineurs en situation de délinquance juvénile
- Les victimes de violences sexuelles ou sexistes
- Les affaires très médiatisées

5 Pratique en matière d'anonymisation des données dans les décisions de justice

5.1 Côte d'Ivoire

Il convient tout d'abord de noter l'absence de jurisprudence spécifique des tribunaux ivoiriens sur l'anonymisation des décisions de justice.

L'analyse des entretiens réalisés met en évidence plusieurs constats :

- Une méconnaissance généralisée de la notion d'anonymisation
- Un cadre juridique international et national existant mais peu appliqué
- Un vide juridique en matière d'anonymisation des décisions de justice avant leur publication.

Concernant l'organisation de la justice, le greffe joue un rôle central dans :

- L'analyse et le traitement des documents envoyés au tribunal
- L'archivage des documents juridiques
- La consultation et la délivrance d'extraits ou de copies

Cependant, dans les greffes d'Abidjan, de Bouaké et de Korhogo, les interviews menés révèlent qu'il n'existe aucune procédure d'anonymisation, ni aucun service dédié à cette tâche.

Un débat sur l'accès à l'information et l'anonymisation

Certains juristes interrogés rappellent que la publicité des audiences est un principe fondamental de la justice, garantissant transparence et accessibilité au système judiciaire.

Les séances publiques sont généralement la norme, mais des exceptions existent, notamment lorsque des informations sensibles nécessitent une protection spéciale (ex. : affaires impliquant des mineurs).

Toutefois, il faut se demander si l'anonymisation pourrait constituer une entrave au droit d'accès à l'information ?

Une évolution des mentalités sur l'anonymisation

Au cours des entretiens, certaines voix discordantes se sont exprimées :

- Des professionnels du droit et des organisations civiles plaident pour une introduction rapide d'une obligation d'anonymisation dans le droit ivoirien
- Certains experts s'interrogent sur l'existence d'une obligation implicite d'anonymisation, fondée sur les principes de protection des données
- Des cabinets d'accompagnement juridique estiment que la loi sur la protection des données impose déjà une anonymisation obligatoire, mais que des manquements graves persistent dans la publication des décisions de justice.

Impact du RGPD et des réglementations internationales

Les entreprises manipulant des données à caractère personnel doivent se conformer :

- À la loi ivoirienne sur la protection des données personnelles
- Au RGDP pour les cas impliquant des personnes ou entités situées dans l'UE

Cette conformité est devenue un enjeu concurrentiel, notamment pour les entreprises ayant une activité internationale.

Cependant, les cabinets spécialisés dénoncent plusieurs difficultés :

- Un exercice de leur métier rendu difficile par des contraintes administratives.
- Une concurrence déloyale exercée par leur propre autorité de régulation.

État des pratiques en Côte d'Ivoire

L'examen des plateformes qui publient régulièrement des décisions de justice révèle une

mise en œuvre mitigée du principe d'anonymisation. Nous avons analysé les trois plateformes suivantes :

https://tribunalcommerceabidjan.ci/decisions

https://www.courdescomptes.ci/_publications.php

https://www.cndj.ci/publications/publications

5.1.1 La plateforme du Greffe du Tribunal de Commerce

La plateforme du Tribunal de Commerce d'Abidjan est le fruit d'une synergie agissante entre les bailleurs de fonds, notamment la Banque mondiale, et l'État ivoirien, qui l'a mis en œuvre par la décision N°01 PR du 11 janvier 2012 portant création, organisation et fonctionnement des tribunaux de commerce et le décret 2012-628 du 06 juillet 2012, qui ont secrété la loi N°2014-424 du 14 juillet 2014, elle-même modifiée par la loi N°2016-1110 du 08 décembre 2016.

En seulement dix années d'existence, cette juridiction spécialisée est devenue une véritable institution du macrocosme judiciaire ivoirien, jouissant d'une bonne réputation, exaltée par :

- la conscience professionnelle de ses animateurs (juges professionnels, juges consulaires, greffiers, personnel administratif et technique) ;
- le volume et la qualité des affaires traitées et publiées sur un site dédié.

S'inscrivant dans l'ère du temps, elle a amorcé et poursuit la dématérialisation des procédures, pour la satisfaction des justiciables de plus en plus exigeants.

Avec son avènement, il y a dorénavant trois tribunaux de premier degré à Abidjan à savoir :

- Le Tribunal de 1re Instance d'Abidjan Plateau,
- Le Tribunal de 1re Instance de Yopougon,
- Le Tribunal de Commerce d'Abidjan.

Les litiges attribués au Tribunal de Commerce d'Abidjan sont :

Les contestations relatives aux engagements et transactions entre commerçants au sens de l'Acte Uniforme sur le droit commercial général.

- Les contestations entre associés d'une société commerciale ou d'un groupement d'intérêt économique.
- Les procédures collectives d'apurement du passif.
- Les contestations et oppositions relatives aux décisions prises par le Tribunal de Commerce.
- Les contestations entre toutes personnes, relatives aux actes de commerce au sens de l'Acte Uniforme relatif au Droit Commercial Général (NB : dans les actes mixtes, la partie non commerçante demanderesse peut saisir les tribunaux de première instance).
- Les contestations relatives aux actes de commerce accomplis par les commerçants à l'occasion de leur commerce et l'ensemble de leurs contestations commerciales comportant même un objet civil.
- Les litiges attribués par les lois spéciales aux tribunaux de commerce.

Par ailleurs, le Tribunal de Commerce d'Abidjan gère le Registre du Commerce et du Crédit Mobilier (RCCM).

Le ressort territorial du Tribunal de Commerce d'Abidjan englobe celui des tribunaux de 1re instance d'Abidjan-Plateau et de Yopougon.

Le Tribunal de Commerce d'Abidjan est composé de:

- Juges professionnels (magistrats de carrière).
- Juges consulaires (opérateurs économiques choisis sur une liste d'aptitude établie par la chambre de Commerce et d'Industrie de Côte d'Ivoire).
- Greffiers.
- Personnels Administratifs.

La plateforme du tribunal du commerce publie les décisions de justice en l'état avec les noms et toutes les coordonnées des parties en conflit (nom et prénoms – siège social – adresses géographiques – contact téléphonique). Aucune mention sur le consentement des concernés n'a été constatée. Il n'existe sur le site aucune politique de confidentialité.

5.1.2 La plateforme de la Cour des

comptes

La Cour des comptes publie des rapports sur l'exécution du budget de l'État et des rapports sur l'audit de performance.

PRÉSENTATION

Haute juridiction financière chargée du contrôle des finances publiques, la Cour des comptes a été créée par la Constitution du 1er août 2000. Installée officiellement le 09 janvier 2018, elle est actuellement régie par la loi organique n° 2018-979 du 27 décembre 2018 déterminant ses attributions, sa composition, son organisation et son fonctionnement. La Constitution du 08 novembre 2016 confère à la Cour des comptes le double statut de juridiction suprême de contrôle des finances publiques et d'Institution de la République.

La Cour des comptes juge les comptes des comptables publics, les comptes des comptables de fait et les fautes de gestion. Elle contrôle la gestion des services de l'État, des établissements publics nationaux et des collectivités territoriales. Elle contrôle également la gestion de tout organisme ou association qui bénéficie d'un concours financier de l'État, ainsi que de tout organisme bénéficiant du concours financier des entreprises publiques et de leurs filiales. Elle assiste le Parlement et le Gouvernement dans le contrôle de l'exécution des lois de finances et dans les domaines relevant de sa compétence.

La Cour des comptes reçoit la déclaration authentique de patrimoine du Président de la République, du Vice-président et des membres de la Haute Autorité pour la Bonne Gouvernance lors de leur entrée en fonction et à la fin de celle-ci.

La Cour des comptes est composée de magistrats du siège, de magistrats du Parquet près ladite Cour et de membres du greffe. Elle est dotée d'un Secrétariat général.

Les magistrats du siège sont le Président de la Cour des comptes, les Présidents de chambre, les conseillers maîtres, les conseillers référendaires et les auditeurs. Dans l'exercice de leurs fonctions, les magistrats de la Cour des comptes sont assistés de vérificateurs comptables et d'agents administratifs.

Le Secrétaire général assure, sous l'autorité du Président, le fonctionnement du greffe et des services administratifs de la Cour.

Les membres du greffe sont le greffier en chef et les greffiers.

Le Parquet général est placé sous l'autorité du Ministre de la Justice. Dirigé par le Procureur général, le Parquet général comprend le Procureur général, un 1er avocat général et des avocats généraux

FONCTIONNEMENT

Le Président de la Cour des comptes est chargé de l'administration et de la discipline de la Cour. Il en assure la direction générale, l'organisation et la coordination des travaux. Il répartit, par ordonnance, les magistrats dans les chambres. Il contrôle les travaux et les activités des magistrats autres que ceux du ministère public. Il arrête le règlement intérieur de la Cour des comptes, après délibération de l'assemblée générale de la Cour. Il assure la gestion administrative des personnels et des moyens affectés à la Cour. Il préside les audiences solennelles, la chambre du conseil, les chambres réunies. Il peut, en outre, présider toutes les autres formations de la Cour.

La Cour comprend cinq (5) Chambres réparties en fonction de leurs attributions :

La Chambre 1 est en charge du contrôle des comptes de l'État. Elle est en outre chargée du contrôle de l'exécution de la loi de finances, de la déclaration générale de conformité, des audits de performance des programmes et des rapports annuels de performance.

La Chambre 2 est en charge du contrôle non juridictionnel des Collectivités territoriales et des Districts autonomes.

La Chambre 3 est en charge du contrôle non juridictionnel des établissements publics nationaux, des sociétés d'État, des sociétés à participation financière publique, des organismes recevant des fonds publics, des services concédés, des organismes de sécurité et de prévoyance sociale, ainsi que des organismes bénéficiaires de la générosité publique.

La Chambre 4 est en charge du contrôle juridictionnel. Elle est notamment chargée du jugement des comptes des comptables publics, des comptes des comptables de fait et des fautes de gestion.

Enfin, **la Chambre 5** est en charge du contrôle de la qualité des rapports et des arrêts produits par les différentes Chambres. Elle est en outre chargée de la production du rapport public annuel.

Le Procureur général assure les fonctions du ministère public près la Cour des comptes. Il assure l'administration et la discipline du Parquet général. Il peut requérir l'application de la loi devant toutes les chambres et en toutes matières. Il veille à la bonne application des lois et règlements au sein de la Cour. La présence du ministère public est obligatoire devant les assemblées générales, la chambre du conseil, les chambres réunies, lors des audiences ordinaires et solennelles.

La Cour des comptes se réunit en audience ordinaire pour juger les affaires qui sont de sa compétence. L'audience solennelle est publique.

Les extraits de procès-verbaux des greffes et les documents parcourus ont permis le constat:

La Cour des comptes **ne publie pas véritablement des données à caractère personnel,** bien qu'aucune politique de confidentialité n'ait été identifiée sur son site.

Les entretiens menés n'ont pas permis de conclure qu'il existe un service d'anonymisation ou qu'il y ait une politique d'anonymisation des décisions publiées sur le site web.

Il en ressort que **la protection des données à caractère personnel n'est pas prise en compte, car toutes les décisions sont publiées avec toutes les informations pouvant permettre d'identifier les protagonistes.**

5.1.3 La plateforme du centre national de documentation juridique : Outil par excellence de la recherche juridique en Côte d'Ivoire

Tous les interviewés ont une fois eu recours à ce site.

PRÉSENTATION

Le Centre National de Documentation Juridique (en abrégé CNDJ), Établissement Public National (EPN) à caractère administratif, créé par décret n°95-470 du 15 juillet 1995, modifié par le décret n°2016-843 du 19 Octobre 2016, s'est vu confier par la volonté de l'État de Côte d'Ivoire la mission d'assurer la promotion et la diffusion du droit en Côte d'Ivoire.

Le CNDJ comprend deux (2) organes de décisions

- **Le conseil de Gestion ;**
- **la Direction.**

A- Le Conseil de Gestion

Le Conseil de Gestion est composé comme suit :

- Le représentant du Ministère en charge de la justice ;
- Le représentant du ministère en charge de l'Economie et des Finances ;
- Le représentant du Ministère en charge du budget;
- Le représentant du Ministère en charge de la fonction publique ;
- Le représentant de la Chambre Judiciaire ;
- Le représentant du Secrétariat général du Gouvernement ;
- Les représentants des unités de Formation et de Recherche des Sciences juridiques des Universités publiques, au nombre de deux, désignés par le Ministre chargé de l'Enseignement supérieur ;
- Le représentant du Centre ivoirien de Recherche juridique;
- Le représentant de l'ordre des avocats.

La présidence du conseil de gestion est assurée par le représentant du Garde des Sceaux, Ministre de la Justice et des Droits de l'Homme.

Le président et les membres du conseil de gestion sont nommés par décret pris en conseil des Ministres, sur proposition des autorités dont ils relèvent. Ils sont révoqués dans les mêmes conditions.

En cas de vacance de siège par décès, démission ou révocation d'un membre du conseil de gestion, il est pourvu à son remplacement dans les mêmes conditions que celles de sa nomination.

La fonction de membre de conseil de gestion est incompatible avec tout emploi rémunéré par le CNDJ.

Les membres du conseil de gestion perçoivent une prime de responsabilité dont le montant est fixé par un arrêté conjoint du Garde des Sceaux, Ministre de la Justice et des Droits de l'Homme et du Ministre chargé du budget.

Le conseil de gestion suit, de façon permanente, la bonne exécution des missions confiées au CNDJ.

Il contrôle la préparation et l'exécution du budget, et examine le compte rendu financier produit par l'agent comptable en fin d'exercice.

En outre, sont soumis à l'autorisation préalable du conseil de gestion les actes suivants du Directeur :

- La modification des textes organiques ;
- L'adoption du programme annuel d'activités ;
- La fixation des tarifs des prestations du CNDJ ;
- La création ou la suppression des services et des antennes.

Le conseil de gestion se réunit aussi souvent que l'intérêt de l'établissement l'exige et, au moins quatre fois par an.

La convocation du conseil de gestion par le Président se fait quinze jours au moins avant la réunion.

Le conseil de gestion ne peut délibérer que si la majorité de ses membres est présente.

Si le quorum n'est pas atteint, le conseil de gestion est de nouveau convoqué dans les huit jours suivants et peut délibérer valablement si un tiers des membres est présent.

Les délibérations sont prises à la majorité des membres présents. En cas de partage des voix, celle du président est prépondérante.

Le président du conseil de gestion peut inviter, avec voix consultative, aux réunions du conseil, toute personne dont il estime utile d'entendre les avis.

B- La Direction

Le CNDJ est dirigé par un Directeur nommé par décret pris en conseil des Ministres, sur proposition du Garde des Sceaux, le ministre de la Justice et des Droits de l'Homme. Il a rang de Directeur Général d'Administration centrale.

Le Directeur est l'ordonnateur du budget du CNDJ.

Il assure l'administration et la direction du CNDJ.

Il accomplit, à cet effet, tous actes nécessaires à la réalisation des missions du CNDJ.

Il représente le CNDJ devant les juridictions et dans tous les actes de la vie civile.

Il assure le secrétariat du conseil de gestion.

l est l'Ordonnateur principal du budget de l'établissement et représente le CNDJ en justice et dans les actes de la vie civile.

La direction du CNDJ comprend trois départements:

- Le département des Affaires juridiques
- Le Département des ressources humaines et Financières ;
- Le département de l'informatique

B-a Le département des Affaires juridiques

Le département des Affaires juridiques est chargé de :

- assurer la collecte et la sélection de l'information juridique
- assurer l'étude et l'analyse de l'information juridique ;
- publier et de diffuser l'information juridique ;
- organiser des sessions de formation en matière juridique ;
- assurer les relations extérieures et la communication.

Le Département des affaires juridiques comprend trois services :

- Le service juridique ;
- Le service de la documentation ;
- Le service de la communication

Les départements sont dirigés par des chefs de département nommés par décision du Directeur, après approbation du conseil de gestion.

B-b Département des ressources humaines et financières.

Le Département des Ressources Humaines et Financières est chargé de:

- assurer la gestion du personnel ;d'élaborer et d'exécuter le budget ;
- assurer la préparation des marchés,
- les conventions et du programme d'investissement;
- assurer la gestion du patrimoine ;
- assurer la vente de la documentation juridique.

Le département des ressources humaines et financières comprend deux services :

- Le service du personnel et du patrimoine ;
- Le service des finances et de la comptabilité.

Les départements sont dirigés par des chefs de département nommés par décision du Directeur, après approbation du conseil de gestion.

B-c Département de l'informatique

Le département informatique est chargé :

- d'assurer les études, la réalisation et la mise en œuvre des applications Informatiques ;
- d'assurer l'alimentation et la gestion des bases ou banques de données ;
- d'assurer la maintenance du système et l'évaluation des besoins en matériel informatique ;
- d'exécuter les travaux de saisie et de mise en forme ;
- d'assurer la formation des utilisateurs et des administrations fournisseurs d'informations ;
- de donner des conseils et d'assurer l'assistance en informatique juridique ;
- d'assurer l'édition de la documentation.

Le département de l'informatique comprend deux services :

- Le service de l'informatique ;
- Le service de reprographie.

Les services sont dirigés par des chefs de service nommés par décision du directeur, après approbation du conseil de gestion.

L'analyse des interviews réalisée au CNDJ, met en exergue trois aspects principaux :

- **La mission de production du savoir du CNDJ**

Le CNDJ a une mission de production de l'information juridique à ce titre, il produit plusieurs documents (232 à la date de rédaction dudit rapport). C'est une performance remarquable pour ce qui est de l'accès à l'information.

- **Les difficultés du processus de publication des décisions de justice rendu**es

Les décisions de justice publiées sur le site du CNDJ doivent d'abord être collectées. Cette collecte se fait à travers des déplacements vers les greffes des juridictions. Cela se passe en moyenne deux (2) fois par an et nécessite une logistique assez lourde, due notamment aux déplacements sur de longues distances avec un personnel en nombre insuffisant et peu outillé. La collecte serait plus facile si les juridictions ivoiriennes étaient interconnectées avec un véritable service d'informatisation et d'archivage numérique qui permettrait d'avoir toutes les informations sans se déplacer et en temps réel.

Le CNDJ a souvent du mal à collecter les données à cause de décisions incomplètes (factum du juge à part, qualité du greffier à part, pas d'informations sur les parties, motifs incomplets, etc.), ou les décisions sont seulement disponibles en version papier, sans version électronique.

- **La volonté manifeste d'amélioration de ses services et des prestations.**

Selon ses responsables du CNDJ que nous avons interviewés, il n'y a **aucune obligation de publication des décisions de justice de manière anonymisée.** Malgré cela, le CNDJ se met petit à petit au goût du jour en anonymisant de façon basique les décisions avant la publication. Cette attitude répond bien à un positionnement pragmatique

> Malgré une obligation légale en vertu du principe de minimisation, l'absence de directives claires conduit à un risque majeur de divulgation inappropriée d'informations confidentielles et de violation des droits fondamentaux.

qu'a la reconnaissance d'une obligation juridique d'anonymisation selon la loi de 2008 sur la protection des données à caractère personnel. En effet, depuis les débuts de la publication des décisions de justice par la CNDJ en 1996, il y a eu beaucoup de plaintes de personnes qui ont vu leurs noms dans les décisions publiées. Le CNDJ a donc estimé qu'une anonymisation des décisions serait salutaire. Mais celle-ci ne répond pas vraiment aux standards et devrait être développé davantage pour devenir conforme aux exigences de la loi sur la protection des données à caractère personnel.

Un épisode illustre très bien cette attitude. Dans le cadre de l'appui budgétaire de l'Union européenne à l'État de Côte d'Ivoire et pour la mise en œuvre de l'indicateur « Publication des décisions de justice' », les décisions collectées ont été traitées par thème uniquement sans traitement informatique préalable, ni traitement par mots clés ni résumé. Ce qui exclut toute anonymisation des décisions. Car elles ont été publiées au format PDF identique à la minute produite par la juridiction.

Ces décisions se sont retrouvées donc en l'état, avec les identités des parties. Pour remédier à certains inconvénients pour les personnes concernées, le CNDJ a adopté une position flexible : La partie ayant vu la décision sur Internet, peut se rendre au CNDJ pour demander des explications et le retrait de ladite décision en ligne aux motifs que sa publication avec son identité lui porte préjudice.

5.2 Sénégal

Il ressort de l'analyse des entretiens menés au Sénégal :

5.2.1 Méconnaissance profonde de la notion d'anonymisation des décisions de justice

Il faut noter que pour la plupart des acteurs rencontrés, l'anonymisation des décisions de justice s'avère être une notion ou une pratique inconnue jusqu'ici. Les professionnels du droit interrogés ont montré un manque de familiarité avec le concept d'anonymisation des décisions de justice. Pour la plupart d'entre eux, l'anonymisation apparaît comme une notion ou une pratique nouvelle.

Cette méconnaissance souligne un besoin urgent de sensibilisation et de formation sur l'importance de l'anonymisation dans le contexte judiciaire. En effet, l'anonymisation vise à protéger la vie privée des individus concernés par les décisions de justice en supprimant ou en rendant non identifiables les éléments de données personnelles avant leur publication. Une meilleure compréhension de ce processus est essentielle pour garantir le respect des droits individuels et la confidentialité des informations sensibles tout en garantissant le droit à l'information des populations donc, il est important que les acteurs de la justice se familiarise avec cette notion.

5.2.2 Manque de conscience quant au principe d'anonymisation

Au Sénégal, les interlocuteurs interviewés ont estimé qu'une obligation d'anonymisation des décisions de justice lors d'une publication en ligne n'existerait pas. Pour soutenir cette appréciation, ils se sont référés à l'absence de textes au Sénégal qui règlementeraient de façon expresse l'anonymisation.

Cette lacune soulève des préoccupations majeures en matière de protection des données personnelles et de respect de la vie privée. Il apparaît que, malgré une obligation légale en vertu du principe de minimisation de divulgation des données, l'absence de directives claires et des procédures établies pour l'anonymisation des documents judiciaires, conduit à un risque majeur de divulgation inappropriée

d'informations confidentielles et de violation des droits fondamentaux des individus impliqués dans des affaires judiciaires. Il est donc impératif que le Sénégal développe des directives adéquate venant « d'en haut » qui insistent sur l'anonymisation des décisions de justice pour assurer une protection efficace des données personnelles et une transparence équilibrée dans le système judiciaire.

En outre, des formations paraissent nécessaires pour faire connaître aux agents des administrations judiciaires et les autres acteurs en lien avec la justice les obligations découlant de la législation qui protège les données à caractère personnel. Lors de ces formation il faut insister sur les obligations d'anonymisation découlant de la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel et les bonnes pratiques en la matière.

5.2.3 La commission de Protection des Données Personnelles (CDP)

La Commission de Protection des Données Personnelles (CDP) est une Autorité Administrative Indépendante (AAI) instituée par la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel. Elle est composée de onze (11) membres choisis en raison de leur compétence juridique et/ou technique. Par ailleurs, un Commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la Commission. Leur mandat est de quatre (4) ans renouvelables une fois.

- **Fonctionnement de la Commission :**

Les onze membres de la Commission se réunissent, sur convocation du Président de la Commission, en séance plénière une à deux fois par mois. La Commission fonctionne sur la base d'un règlement intérieur... La CDP dispose d'un budget autonome dont les crédits sont alloués par le Ministère de l'Economie et des Finances.

- **Mission de la commission :**

Les missions assignées à la Commission de Protection des Données Personnelles (CDP) sont :

UNE MISSION DE VEILLE, DE SENSIBILISATION, DE CONSEILS ET DE PROPOSITIONS

- Veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions légales ;
- Informe les personnes concernées et les responsables de traitement de leurs droits et obligations ;
- S'assure que les Technologies de l'Information et de la Communication (TIC) ne comportent pas de menace au regard des libertés publiques et de la vie privée des Sénégalais ;
- Homologue les chartes d'utilisation présentées par des responsables de traitement de l'information ou de données ;
- Tient un répertoire des traitements des données à caractère personnel à la disposition du public ;
- Conseille les personnes et organismes qui ont recours aux traitements des données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements ;
- Présente au gouvernement toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;
- Publie les autorisations accordées et les avis émis dans le répertoire des traitements des données à caractère personnel ;
- Établit chaque année un rapport d'activités remis au Président de la République et au Président de l'Assemblée nationale ;
- Formule toutes recommandations utiles en vue de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions en vigueur ;
- Coopère avec les autorités de protection des données à caractère personnel des pays tiers et participe aux négociations internationales en matière de protection des données à caractère personnel.

UNE MISSION D'INSTRUCTION DES DOSSIERS

- Reçoit les formalités préalables (les déclarations, les demandes d'autorisation)

à la création de traitements des données à caractère personnel ;

- Reçoit les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;
- Répond à toute demande d'avis ;
- Autorise les transferts transfrontaliers de données à caractère personnel.

UNE MISSION DE CONTROLE ET D'INVESTIGATION

- Informe sans délai le procureur de la République des infractions dont elle a connaissance ;
- Peut charger un ou plusieurs de ses membres ou des agents de ses services de procéder à des vérifications portant sur tout traitement et, le cas échéant, d'obtenir des copies de tout document ou support d'information utile à sa mission ;
- Peut prononcer une sanction à l'égard d'un responsable de traitement.

5.2.4 Le projet d'anonymisation de la Cour Supreme

Depuis plus d'une dizaine d'année, la Cour suprême s'est engagée à travailler avec la commission de Protection des Données Personnelles sur la problématique de la protection des données personnelles, notamment la question de l'anonymisation des données judiciaires. La Cour suprême a décidé d'anonymiser la publication des décisions qu'elle juge être intéressant en vertu du respect de la vie privée des justiciables. La cour s'est impose cette pratique d'anonymisation et a une vocation d'anonymisation de toute sa jurisprudence.

5.2.5 La loi générale sur l'accès à l'information

Bien qu'étant un droit consacré par la constitution sénégalaise, l'accès à l'information ne fait pas l'objet d'une loi spécifique au Sénégal, mais est réparti entre différentes lois relatives aux archives, à la passation des marchés publics, à la déclaration du patrimoine des responsables publics, à la société de l'Information, etc. L'absence d'une loi spécifique n'empêche toutefois pas la société civile ou d'autres institution de mener des actions concrètes visant à rendre effectif ce droit d'accès à l'information.

Cependant, il faut noter que le Sénégal est dans un processus d'adoption de cette loi générale sur l'accès à l'information, mais cette législation connait des exceptions notamment :

- ✓ Les informations confidentielles reçues d'un tiers ou concernant un tiers ;
- ✓ Les informations qui sont de nature à porter atteinte à la sécurité publique et à la défense nationale ;
- ✓ Les informations relatives aux procédures pendantes devant une juridiction et n'ayant pas fait l'objet d'une décision de justice ;
- ✓ Les informations relatives à une mission d'inspection, de contrôle ou d'enquête non clôturée ;
- ✓ Les informations susceptibles de mettre en danger la vie, la santé ou la sécurité des personnes ou de leurs biens ;
- ✓ Les informations dont la divulgation porterait gravement préjudice aux intérêts nationaux ;
- ✓ Les renseignements susceptibles de porter atteinte à la vie privée, au secret médical et à la dignité de la personne

6 Situation par rapport aux thématiques de la délinquance juvénile, des violences sexuelles et sexistes et des cas très médiatisés

En ce qui concerne les affaires spécifiques, c'est-à-dire les affaires liées à la délinquance juvénile, les affaires liées aux violences sexuelles et sexistes et les affaires très médiatisées, nous avons pu faire les observations suivantes.

6.1 Sénégal

L'anonymisation des données vise à protéger la vie privée des individus tout en permettant l'utilisation de données à des fins légitimes.

Notons que l'anonymisation cible dans le cadre de l'étude des domaines spécifiques tels que la délinquance juvénile, les affaires médiatisées et la violence sexuelle et sexiste. Ce sont des domaines où les enjeux de protection de la vie privée sont particulièrement sensibles.

Au Sénégal, il n'y a pratiquement pas de procédure spéciale de traitement et de gestion de ces cas, sauf décisions spéciales des tribunaux (cas spécifique de la protection).

» **La délinquance juvénile**

Dans le contexte de la **délinquance juvénile,** où des mineurs se retrouvent en conflit avec la loi, la protection de leur identité revêt une importance cruciale en raison des implications significatives que cela peut avoir sur leur vie future. La nature sensible de cette question nécessite une approche proactive visant à prévenir toute stigmatisation ou préjudice potentiel. En ce sens, au Sénégal non seulement les audiences correctionnelles des mineurs délinquants ne sont pas rendues publiques, mais également les décisions judiciaires qui découlent de ces procédures sont traitées avec la plus grande confidentialité. En effet, l'audience des mineures en **matière correctionnelle** est non publique, elle se tient en chambre de conseil. Chaque affaire est jugée séparément. Parmi les personnes admises à assister au débat, on peut citer les témoins de l'affaire, les parents ou civilement responsables, les tuteurs, les avocats, les représentants des services ou institution en charge des enfants, les délégués à la liberté surveillée. Toutes ces personnes sont astreintes au respect de la confidentialité.

L'article 579 Code de Procédure Pénale interdit la publication par tout moyen du compte rendu des débats, du jugement et de toute indication concernant l'identité, la personnalité du mineur délinquant. Les infractions à ces dispositions sont punies d'une amende de 20 000 frs à 50 000 frs et d'un emprisonnement de 2 mois à 2 ans.

En matière de **protection judiciaire** (assistance éducative), il est également souhaitable que toutes les informations concernant des mineurs susceptibles d'être entendus parviennent aux services de prévention ou au Président du Tribunal pour enfant qui sont soumis au secret professionnel. Le législateur a tenté de trouver un équilibre entre protection du secret (condition pour que s'installe une relation de confiance entre celui qui s'exprime et celui qui écoute) et protection des mineurs rendant nécessaire la diffusion des informations reçues.

L'anonymisation soigneuse des informations liées à la délinquance juvénile s'avère ainsi très essentielle pour s'assurer que les données ne puissent pas être exploitées de manière à identifier directement ou indirectement les jeunes délinquants. Cela implique la suppression minutieuse de toutes les informations susceptibles de révéler l'identité des jeunes délinquants, que ce soit par le biais de détails spécifiques, de lieux ou d'autres éléments distinctifs. La protection de l'identité des jeunes délinquants vise à garantir qu'ils puissent bénéficier d'une seconde chance sans le fardeau potentiel d'une réputation entachée. En mettant en œuvre ces mesures de confidentialité rigoureuses, la justice pénale pour les mineurs peut mieux atteindre ses objectifs de réhabilitation tout en préservant la dignité et l'avenir des jeunes impliqués.

Dans ces conditions, il va de soi que l'anonymisation des décisions de justice concernant la délinquance juvénile est une nécessité au regard du principe de la protection des mineurs.

» **Les violences sexuelles et sexistes**

Dans le domaine particulièrement délicat de la v**iolence sexuelle et sexiste,** où les victimes sont confrontées à des traumatismes sérieux, la protection de leur vie privée devient une priorité incontestable. L'anonymisation des données dans ce domaine sensible revêt une importance capitale en vue de prévenir toute forme de stigmatisation et de victimisation supplémentaire pour les personnes déjà éprouvées par ces actes. Le processus d'anonymisation vise à dissocier de manière rigoureuse toutes les informations susceptibles permettant l'identification des victimes, contribuant ainsi à créer un environnement plus sûr et plus respectueux de leur dignité.

La nécessité d'anonymiser les données relatives aux victimes mais aussi aux auteurs d'actes de violence sexuelle découle de la sensibilité extrême entourant ces informations. Ces données sont hautement délicates et leur mauvaise utilisation pourrait entraîner des préjudices considérables pour les personnes concernées.

La rigueur dans le processus d'anonymisation garantit que les détails spécifiques susceptibles de révéler l'identité des parties impliquées soient soigneusement effacés. Ce niveau de protection renforcée sert à préserver l'intégrité des victimes,

à promouvoir la confidentialité nécessaire dans les procédures judiciaires et à encourager la dénonciation d'actes répréhensibles sans craindre des conséquences indésirables ou des préjudices pour les victimes.

Au Sénégal, les audiences correctionnelles sur les violences sexuelles sont publiques sauf si un mineur est impliqué. Pour les cas où un mineur est impliqué il est donc impératif que la publication des décisions des mineurs en matière de violence sexuelle se fasse de manière anonymisé. Pour les autres cas qui n'impliquent pas de mineurs, l'anonymisation s'impose aussi, mais en vertu du principe de minimisation et du principe de proportionnalité tel que cela a été déjà évoqué ci-dessus. Ces principes imposent que ne soient publiées lors d'une publication sur internet que les données qui soient strictement nécessaires pour la compréhension du cas. L'identité ni de la victime ni de l'acteur de l'acte de violences ne sont nécessaires pour la compréhension du cas.

» **Les affaires très médiatisées**

Au Sénégal, lorsque des affaires revêtent un intérêt très particulier, les journalistes assistent aux audiences. Au nom du droit à l'information ils relient l'information au public. Par ailleurs, force est de reconnaitre qu'il existe des affaires plus médiatisées que d'autres telles que les affaires des politiciens, des hommes d'affaires, de corruption, de viol et de meurtre.

Pour ces affaires très médiatisées, on note une pression accrue des médias qui représente un défi supplémentaire pour les personnes confrontées au traitement du cas. La médiatisation augmente considérablement le risque d'intrusion dans la vie privée des parties impliquées. Les affaires qui font l'objet d'une couverture médiatique intense peuvent entraîner une exposition publique non seulement des accusés, mais aussi des témoins et d'autres parties prenantes. Dans ce contexte, l'anonymisation des données s'avère être une mesure cruciale pour prévenir les atteintes à la vie privée de toutes les personnes impliquées dans la procédure judiciaire.

L'anonymisation doit être étendue pour couvrir non seulement les accusés, mais également les témoins et d'autres parties prenantes, telles que les experts ou les plaignants. Cela garantit que les détails spécifiques qui pourraient permettre l'identification de ces individus soient soigneusement protégés. En particulier, pour les témoins, l'anonymisation peut être essentiel pour encourager leur coopération sans crainte de représailles ou d'exposition publique indue. L'anonymisation complète des données implique souvent le retrait de détails spécifiques tels que les noms, les adresses, les professions et d'autres informations personnelles qui pourraient être exploitées pour identifier les parties impliquées. Cette approche proactive contribue à établir un équilibre entre le besoin de transparence dans les procédures judiciaires et le respect du droit fondamental à la vie privée des individus, en particulier dans le contexte des affaires très médiatisées.

Enfin, la **protection des témoins** constitue aussi une préoccupation primordiale, nécessitant une approche soigneuse de l'anonymisation des données pour assurer la sécurité et la confidentialité de ces individus essentiels au processus judiciaire. Les témoins, en particulier dans des affaires sensibles ou criminelles, peuvent en effet craindre des représailles potentielles en raison de leur coopération avec les autorités judiciaires. L'anonymisation des données va au-delà de la simple dissimulation des noms. Elle englobe également la confidentialité des informations relatives à la localisation, à l'identité et à d'autres détails personnels qui pourraient permettre une identification directe ou indirecte des témoins.

La préservation de l'anonymat des témoins est impérative pour encourager leur collaboration sans entrave. Cela peut inclure des mesures telles que la substitution de détails spécifiques par des identifiants uniques, la suppression des informations susceptibles de révéler des liens familiaux ou professionnelles, et la protection des données sensibles relatives à la vie personnelle des témoins. La confidentialité de la localisation des témoins est également un aspect important, car la divulgation de ces informations pourrait exposer les témoins à des risques sérieux.

En veillant à l'anonymisation rigoureuse des données relatives aux victimes de violence sexuelles comme dans les cas d'affaires très médiatisés ou sexiste, le système judiciaire peut

créer un environnement dans lequel les concernés se sentiront plus en sécurité et protégé. Dans tous ces cas l'anonymisation des données à caractère s'impose en de façon plus importante que pour des cas « normaux », car les intérêts qui sont en jeu de la part des personnes concernées pèsent davantage. En vertu du principe de minimisation et du principe de proportionnalité, les données à caractère personnelles sont à protéger et ne doivent donc pas être divulguées à travers la publication des décisions de justice.

6.2 Côte d'Ivoire

La situation en Côte d'Ivoire est très semblable à celle du Sénégal en ce qui concerne la protection des données à caractère personnel pour les cas de délinquance juvénile, les cas de violences sexuelles ou sexistes et les cas très médiatisés.

» **La délinquance juvénile**

Pour ce qui est de la protection des données personnelles en matière pénale, l'art. 823 al. 4 et 6 du nouveau Code de Procédure Pénale (loi n°2018-975 du 27 décembre 2018) disposent pour les cas impliquant des mineurs : « La publication du compte rendu des débats des tribunaux pour enfants dans les livres, la presse, la radiophonie, la cinématographie ou de quelque manière que ce soit, est interdite.

La publication par les mêmes procédés, de tout test ou de toute illustration concernant l'identité et la personnalité des mineurs délinquants est également interdite. Les infractions à ces dispositions sont punies.

Le jugement est rendu en audience publique, en la présence du mineur. Il peut être publié, mais sans que le nom du mineur puisse être indiqué, à peine d'une amende.

Ces dispositions visent à protéger la vie privée et l'anonymat des mineurs impliqués dans des affaires judiciaires, qu'ils soient prévenus ou jugés. Cette protection s'applique à la fois aux mineurs victimes et aux mineurs délinquants, afin d'éviter toute stigmatisation ou atteinte à leur avenir et leur réinsertion sociale.

» **Les cas de violences sexuelles et sexistes et les affaires très médiatisées**

Pour ces cas, il n'y a pas de textes spécifiques régissant la protection des données à caractère personnels. Mais comme au Sénégal, dans ces cas l'anonymisation des données à caractère s'impose de façon plus importante que pour des cas « normaux », car les intérêts qui sont en jeu de la part des personnes concernées pèsent davantage. En vertu du principe de minimisation et du principe de proportionnalité, les données à caractère personnelles sont à protéger et ne doivent donc pas être divulguées à travers la publication des décisions de justice.

Par ailleurs, il est de notoriété publique qu'en dehors des plateformes de publication des décisions de justice, les réseaux sociaux et certaines chaînes de télévision en ont fait des publications, certaines à la recherche de médiamat aux mépris des règles régissant la protection de la vie privée.

Les interlocuteurs de médias rencontrés ont indiqué avoir reçu l'autorisation des personnes concernées.

Les journalistes d'investigation ont répondu que toutes les affaires médiatisées qu'ils ont eu à traiter l'ont été sur la base du code d'éthique et de déontologie à travers le respect des droits (respecter et protéger les droits individuels, y compris la vie privée, la dignité et la diversité) et la confidentialité (maintenir la confidentialité des informations sensibles et ne divulguer des informations qu'avec le consentement approprié ou lorsque requis par la loi).

Ils reconnaissant toutefois ne pas être informés de l'existence d'une loi sur la protection des données à caractère personnel en Côte d'Ivoire.

Se rapportant à l'anonymisation, les professionnels des médias ont indiqué que leurs services en cas de refus des personnes concernées par les affaires à traiter utilisent des lettres alphabétiques et des codifications alphanumériques pour anonymiser.

7 Conclusions

Les conclusions de l'étude sur le cadre juridique de l'anonymisation des documents judiciaires publiés en Côte d'Ivoire et au Sénégal révèlent plusieurs points clés :

1. **Disparité entre normes et pratiques :** L'étude souligne que, bien que les principes de proportionnalité et de minimisation des données existent dans les textes juridiques, ces principes ne sont souvent pas appliqués dans la pratique de la publication en ligne des décisions de justice. Cela se manifeste par une divergence entre les dispositions légales et la manière dont les décisions judiciaires sont publiées, très souvent sans anonymisation suffisante pour protéger la vie privée des individus impliqués.

2. **Cadre juridique présentant certaines lacunes :** En analysant les législations nationales et internationales, l'étude a identifié certaines lacunes concernant un manque de clarté. Il serait mieux quel l'obligation d'anonymisation serait expressément nommée dans la loi au lieu de figurer seulement dans des principes que les personnes concernées par la publication ne comprennent pas toujours suffisamment. Ceci est particulièrement important pour la gestion des cas sensibles tels que les affaires de violence sexuelle. Ces lacunes exposent les individus concernés à un risque accru d'atteinte à la vie privée. Cependant, pour ce qui est de la délinquance juvénile, le besoin pour une protection rigoureuse des données personnelles est mieux pris en considération à travers les codes de procédure pénale. Car dans ces cas, l'obligation d'anonymisation se trouve aussi au niveau des dispositions concernant la procédure pénale.

3. **Pratiques d'anonymisation insuffisantes :** Des plateformes de publication des décisions de justice, bien que pas très nombreuses, commencent à exister, du moins dans certaines configurations. Ces plateformes ne disposent pas toujours de protocoles efficaces pour garantir l'anonymisation. L'étude a relevé que la capacité des gestionnaires des plateformes à anonymiser dépend fortement des ressources humaines et techniques, qui sont souvent très limitées.

4. **Besoin d'évolution législative et de mise en conformité entre règles de droit et pratique :** L'étude conclut sur l'importance d'une évolution législative pour mieux mettre en lumière le besoin de garantir la protection des données personnelles dans la publication des décisions de justice et pour mettre en conformité le droit avec la pratique sur le terrain. En réponse aux faiblesses observées, l'étude propose des mesures concrètes pour améliorer la mise en œuvre des pratiques d'anonymisation et assurer une meilleure harmonisation avec les normes internationales. Cela inclut la formation des praticiens de justice, l'amélioration des infrastructures techniques, et l'établissement de règles juridiques et procédures claires pour assurer la conformité avec les principes de minimisation et de proportionnalité.

8 Recommandations

Etant donné que la situation en Côte d'Ivoire et au Sénégal soit assez semblable, il est possible de formuler d'abord sur la base de cette étude, des recommandations générales pour les deux pays. Par la suite s'imposent aussi quelques recommandations spécifiques pour chacun de deux pays.

8. 1 Recommandations générales

Les recommandations générales visant à améliorer le cadre d'anonymisation des documents judiciaires publiés en Côte d'Ivoire et au Sénégal, se concentrent sur plusieurs axes :

1. Renforcement des dispositifs juridiques :

Clarifier les lois nationales relatives à la protection des données personnelles pour inclure explicitement l'anonymisation des décisions de justice, surtout dans les cas impliquant des groupes vulnérables, comme les mineurs et les victimes de violence sexuelle ou sexiste et aussi les affaires très médiatisées.

2. Formation et sensibilisation des acteurs judiciaires:

Organiser des sessions de formation pour les magistrats, greffiers, avocats et autres acteurs judiciaires afin de renforcer leur compréhension et leur capacité à appliquer les principes de minimisation et de proportionnalité dans le traitement des données personnelles.

3. Développement de standards techniques pour l'anonymisation:

Mettre en place des outils techniques et des protocoles standardisés d'anonymisation des décisions de justice, assurant ainsi que les informations sensibles soient systématiquement protégées.

4. Surveillance et évaluation des pratiques:

Établir un mécanisme de suivi et d'évaluation pour s'assurer que les pratiques d'anonymisation des décisions de justice restent conformes aux normes de protection des données personnelles.

5. Collaboration régionale et internationale:

Encourager les échanges de bonnes pratiques entre pays africains et avec des institutions internationales pour un renforcement mutuel des capacités et une harmonisation des normes.

8.2 Recommandations spécifiques pour la Côte d'Ivoire

- Vulgariser la loi N0 2013-450 relative à la protection des données à caractère personnel ;
- Interconnecter toutes les juridictions ivoiriennes pour faciliter la collecte des décisions de justice;
- Doter les juridictions de connexion internet pour faciliter la transmission entre les juridictions des décisions déjà anonymisées ;
- Mettre en place des logiciels de gestion intégrée utilisé par les juges et les greffiers dans toutes les juridictions pour faciliter la tâche des greffiers, des juges et du CNDJ, car la recherche physique des décisions de justice sur les lieux est fastidieuse, parfois les décisions sont incomplètes, etc. ;
- Renforcer les capacités des personnels sur la codification et l'anonymisation des données à caractère personnel et le cryptage ;
- Accroître les ressources humaines, notamment des juristes et des informaticiens ;
- Accroître les ressources matérielles (ordinateurs performants, scanner performant de grandes capacités et puissances) ;
- Renfoncer le mécanisme de gestion des griefs par l'ARCTI ;
- Désigner des points focaux dans les différentes juridictions pour la collecte des données (décisions de justice) ;
- Accroître le budget du Centre National de Documentation Juridique (CNDJ) en vue de lui permettre d'employer du personnel qualifié en nombre suffisant pour assurer la collecte , l'anonymisation et la publication d'environ 150 000 décisions de justice par an;
- Développer l'archivage numérique dans toutes les juridictions du pays ;
- Réaliser des benchmarkings auprès des pays pionniers en la matière pour identifier les bonnes pratiques en la matière au niveau international ;
- Renforcer la coopération avec les Partenaires Techniques et Financiers pour identifier des opportunités de formation des différentes juridictions sur leurs rôles et tâches dans le processus d'anonymisation (ces formations pourraient s'organiser en coopération avec le CNDJ dans sa fonction de cabinet de formation. Il y'a d'ailleurs une formation qui existe au niveau de l'ENA sur l'anonymisation et qui pourrait servir de base) et pour faire profiter les 26 juridictions qui n'ont pas encore profité des opportunités de formation.

8.3 Recommandations spécifiques pour le Sénégal

- Appuyer le projet d'anonymisation de la Cour suprême qui est le leader en matière d'anonymisation des décisions de justice ; cette pratique de la Cour suprême pourrait servir de modèle pour les autres juridictions ;
- Établir des mécanismes de contrôle et de suivi pour vérifier la conformité des décisions de justice anonymisées avec la réglementation en vigueur. Cela permettra de garantir l'efficacité de l'anonymisation et de prévenir les violations de la vie privée ;
- Proposer la création de lignes directrices nationales sur l'anonymisation des décisions de justice. Ces directives pourraient aborder les questions telles que la collecte, la sécurité, la conservation et la divulgation de données sensibles tout en respectant les droits à la vie privée ;
- Appuyer la mise en œuvre d'une plateforme unique et centrale de publication des décisions de justice et y prévoir d'anonymiser toute les décisions justice de toutes les juridictions ;
- Accélérer le processus d'adoption de la loi générale sur l'accès à l'information. Il sera particulièrement important de prévoir dans cette législation des exceptions pour garantir la protection des informations à caractère personnel qui sont sensibles et confidentielles, tout en assurant un accès adéquat à l'information pour le public ;
- Appuyer et renforcer la Commission de Protection des Données Personnelles (CDP) à mettre en place des mécanismes de recours plus solides pour les personnes dont les données personnelles ont été mal traitées dans le cadre judiciaire ;
- Appuyer les tribunaux en termes de ressources humaines afin de faciliter la collecte et le traitement des décisions de justice ;
- Organiser des sessions de sensibilisation et de formation pour les professionnels du droit et les acteurs du système judiciaire afin de les familiariser avec les principes et les pratiques de l'anonymisation des décisions de justice ;
- Renforcer le personnel informaticien afin de s'assurer de la qualité technique de tout le processus d'anonymisation. Former ce personnel aux besoins en matière d'anonymisation des données.;
- Mettre en place des systèmes d'accès restreints ou de contrôle pour certains types de décisions de justice concernant par exemple : la délinquance juvénile, les affaires de violences sexuelles et sexistes et les affaires très médiatisées, limitant l'accès aux personnes directement impliquées dans l'affaire ou aux professionnels du droit
- Mettre en place un mécanisme de révision périodique des politiques de publication des documents judiciaires pour s'assurer qu'elles restent conformes aux évolutions des normes de protection de la vie privée et des avancées technologiques.

Il est crucial de trouver un équilibre entre ces deux objectifs : droit à l'accès aux données et respect des droits individuels de protection des données à caractère personnel. Les propositions de solutions visent à combler les lacunes identifiées, à renforcer la protection des données dans les décisions de justice et à améliorer les méthodes d'anonymisation utilisées. Les recommandations s'adressant aux décideurs et aux acteurs de la justice ainsi qu'aux organisations qui assistent les justiciables, peuvent contribuer à créer un environnement propice à une meilleure concordance entre règles de droit et la pratique, harmoniser les législations et favoriser la coopération internationale pour la résolution efficace des problèmes communs. Ainsi on pourra arriver à une meilleure protection des données personnelles lors de la publication des décisions de justice pour garantir une protection adéquate des droits individuels.

REFERENCES JURIDIQUES

International :

- Déclaration universelle des droits de l'homme (DUDH) 1948
- Pacte international relatif aux droits civils et politiques (1966)
- Charte Africaine des droits de l'homme et des peuples (1981)
- Convention relative aux droits de l'enfant (1989)
- Charte Africaine pour le bien-être de l'enfant (1990)
- Règlement Général de la Protection des Données (RGPD) 2016
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe de 2018 avec ses amendements de 1999 (Convention 108+)
- Convention de l'Union Africaine sur la Cybersécurité et la Protection des Données Personnelles de 2014 (Convention de Malabo)
- Directive sur la protection des Données à Caractère Personnel de la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO) de 2010
- Loi additionnelle A/SA.1/01/10 relative à la protection des données personnelles au sein de la CEDEAO de 2010
- Règlement Général de la Protection des Données (RGPD) de 2018

Côte d'Ivoire :

- Loi N°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel
- Loi N°2013-450 du 19 juin 2013 relative à la lutte contre la cybercriminalité
- Loi N°2018-570 du 13 juin 2018 relative à la protection des témoins, victimes, dénonciateurs, experts et autres personnes concernées
- Loi N°2018-975 du 27 septembre 2018 portant code de procédure pénale

Sénégal :

- Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, complète par le décret d'application n° 2009-1113 du 21 septembre 2009 posant les bases juridiques relatives à la collecte, au traitement, à la conservation et à la divulgation des données personnelles.
- Loi n°2008-11 du 25 janvier 2008 portant sur la Cybercriminalité
- Loi n°2008-08 du 25 janvier 2008 portant sur les transactions électroniques
- Décret n°2008-721 du 30 juin 2008 portant application de la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel susvisée
- Loi n°2008-41 du 20 août 2008 portant sur la cryptologie
- Loi 66-61 du 21 juillet 1966 portant code de procédure pénale et modifications subséquentes

BIBLIOGRAPHIE

- Allechi, D., L'application du RGDP et la loi ivoirienne au responsable de traitement et au sous-traitant, Le village de la Justice-La communauté des métiers du droit, 31 Juillet 2019
- https://www.village-justice.com/articles/les-obligations-responsable-traitement-sous-traitant-regard-loi-ivoirienne,32147.html
- CNIL, Les grands principes des règles de protection des données
- https://www.cnil.fr/fr/cnil-direct/question/quels-sont-les-grands-principes-des-regles-de-protection-des-donnees
- Essehi, E.-F., Régime juridique des enfants en conflit avec la loi, tout ce qu'il faut savoir, Ivoire-juriste 2021, https://www.ivoire-juriste.com/2021/11/regime-juridique-des-enfants-en-conflit-avec-la-loi-tout-ce-quil-faut-savoir.html

Promotion of the Rule of Law and Justice in Africa

CONSULTANCY AND TECHNICAL STUDIES

Mise en œuvre par

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

HOCHSCHULE KEHL
UNIVERSITY OF APPLIED SCIENCES
Designing and Developing Public Administration

Dorsch Impact