n°4
Octobre
2023

APIA

Revue Semestrielle de la Propriété Intellectuelle en Afrique

Editorial	7
Portraits	8
Zoom	12
Étude	20
Fiche Pays	30
Echos de l'APIA	33
Panorama de jurisprudence	36
La décision du semestre	38
Le semestre du numérique	42
Activités académiques	78
Le semestre du pèlerin	87
Bibliographie	102

ISSN 3000-0025

Revue Semestrielle de la Propriété Intellectuelle en Afrique

Revue de l'Association pour la Promotion de la Propriété Intellectuelle en Afrique (APIA)

Association enregistrée sous le n° W912014459

www.apia-asso.org

COMITE EDITORIAL

Directeur de publication
NGOMBÉ Yvon Laurier
Fondateur et Président de l'Association APIA
presidence@apia-asso.org

Rédacteurs en chef
KPOLO Christian, ÉKANDZI Nilce
secretariat@apia-asso.org

Secrétaires éditoriaux
KOUADIO Firmin, NGOMBÉ John-Pierce
publication@apia-asso.org

*****

Comité scientifique

FOMETEU Joseph
Professeur Titulaire, Université de Ngaoundéré
Expert auprès de l'OMPI (Cameroun)

JOHNSON-ANSAH Ampah
Chef du Département de Droit Privé
Université de Lomé (Togo)

KIMINOU René
Avocat, Professeur Titulaire
Université des Antilles et de la Guyane
(France et Congo)

MONTCHO-AGBASSA Éric
Professeur Agrégé, Université de Cotonou (Bénin)

NDEMA-ELONGUE Max-Lambert
Magistrat hors hiérarchie (Cameroun)
Expert auprès de l'OMPI

NGOMBÉ Yvon Laurier
Docteur en droit, Avocat
Chargé d'enseignements, Expert auprès de l'OMPI
(France et Congo)

NWAUCHE Enyinna
Professeur Titulaire,Nelson Mandela School of Law
University of Fort Hare (Afrique du Sud)

RANDRIANIRINA Iony
Professeure, Université de Grenoble
(France et Madagascar)

THIAM Samba
Professeur Titulaire Classe exceptionnelle
Université Cheikh Anta Diop de Dakar (Sénégal)
Avocat, Membre du CAMES

*****

Comité de rédaction

BILONG BILONG Abel
Docteur en droit, Chargé d'enseignements

ÉKANDZI Nilce
Docteur en droit, Avocat
Membre du CEIPI, Expert auprès de l'OMPI

ÉKÉMÉ Isabelle
Mandataire agréée auprès de l'OAPI

FOUDA Armelle
Mandataire agréée auprès de l'OAPI

GOUADI Koussiama
Mandataire agréé auprès de l'OAPI

KOUADIO Firmin
Juriste, auteur

KOSO OMAMBODI Jean-Paul
Docteur en droit, Avocat
Enseignant-Chercheur

KPOLO Christian
Docteur en droit, Avocat, Enseignant-Chercheur
Université de Lorraine et Université d'Abidjan

MABOUANA Roger
Avocat

MOUBÉRI Abel
Ingénieur

NGANZI NDONI Théodore
Docteur en droit, Avocat
Enseignant-Chercheur

NGOMA Marie-Alfred
Journaliste

NGOUÉ Aline
Docteure en droit, Chargée d'enseignements

OMAR AMINE Yasser
Docteur en droit, Avocat
Enseignant-Chercheur

RANDRIANIRINA Roland
Ingénieur

TANO-BIAN Jeanine
Docteure en droit, Consultante en cybersécurité,
Enseignante-Chercheur Université d'Abidjan

SAMB Abibatou
Avocate

SOUMARÉ Youssou
Juriste, Ancien directeur du département juridique
Bureau sénégalais du Droit d'auteur

WEMBO Paulin
Magistrat auditeur

NOTE A L'ATTENTION DES AUTEURS

Toutes les personnes souhaitant publier leurs manuscrits doivent les envoyer sous forme numérique au format Word (en pièce jointe) à l'adresse publication@apia-asso.org

Le manuscrit doit être accompagné d'un résumé en français et anglais d'un maximum de 1500 signes/caractères (espaces non-compris). Les contributions sont soumises à la lecture/validation du Comité scientifique puis éventuellement à une relecture du Comité de rédaction. Le manuscrit doit être soumis au minimum 90 jours avant la date de publication souhaitée (15 janvier pour le numéro d'avril, 1er août pour le numéro d'octobre).

La RSPIA accueille des articles qui intéressent principalement (mais pas exclusivement) le droit de la propriété intellectuelle en Afrique. Elle accueille également toutes productions scientifiques relatives au droit des affaires en Afrique, aux questions émergeantes et transverses ou aux analyses impliquant une approche comparative ayant un lien avec les législations africaines. Le comité scientifique dispose d'un pouvoir d'appréciation discrétionnaire de la pertinence du sujet proposé par les auteurs.

Le nombre de pages maximum souhaité, en fonction du type d'article, est le suivant :

- Libre propos ou aperçu rapide : 5 pages
- Décision du semestre : 5 pages
- Commentaires de législation : 10 pages
- Etudes ou articles de fond : 20 pages

Les auteurs cèdent à titre gratuit et exclusif leurs droits patrimoniaux sur le manuscrit. Les auteurs sont seuls responsables des opinions émises dans leurs manuscrits.

Les relectures et révisions des contributions de ce numéro ont été assurées par Yvon Laurier Ngombé, A. N., John-Pierce Ngombé et Christian Kpolo

SOMMAIRE

ÉDITORIAL

« Un long chemin vers la protection ? », p. 7
Par Yvon Laurier Ngombé

PORTRAITS

« Miriam Makeba, Angélique Kidjo et Aïcha Koné », p. 8
Par Le Bureau de l'APIA

ZOOM

« Actualité de la propriété intellectuelle en Afrique anglophone en 2022 », p. 12
Par Enyinna Nwauche

ÉTUDE

« Le droit d'auteur à l'épreuve du droit à l'image dans l'exploitation des œuvres des arts visuels en RDC », p. 20
Par Théodore Nganzi Ndoni

FICHES PAYS

« Côte d'Ivoire », p. 30
Par Firmin Kouadio

ÉCHOS DE L'APIA

« *Le Balafon,* Podcast de l'APIA », p. 33
Par Le Bureau de l'APIA

« 2e Journée de la Recherche Scientifique de l'APIA », p. 35
Par Le Bureau de l'APIA

PANORAMA DE JURISPRUDENCE

p. 36
Par Christian Kpolo

LA DÉCISION DU SEMESTRE

« Questions de compétence relatives aux litiges portant sur la propriété de la marque. A propos de l'affaire " Elsafeer Falcon Pack Egypt Industries c/ Falcon Pack et al." », p. 38 *Par Yasser Omar Amine*

LE SEMESTRE DU NUMÉRIQUE

Cybersécurité & E-Santé

« La responsabilité des prestataires d'infogérance des établissements de santé en cas de vulnérabilités informatiques : étude de droit français », p. 42
Par Christian Kpolo

« Sécurité des réseaux dans les espaces OAPI et OHADA », p. 64
Par Jeanine Tano-Bian

« Entrée en vigueur attendue : la Convention sur la cybersécurité de Malabo », p. 71
Par Jeanine Tano-Bian & Christian Kpolo

« Les dispositions relatives à la cybersécurité dans la nouvelle loi de la RDC sur le numérique », p. 72
Par Jeanine Tano-Bian & Christian Kpolo

Commerce électronique

« Les dispositions relatives à la responsabilité des intermédiaires techniques dans la nouvelle loi de la RDC sur le numérique », p. 74
Par Yvon Laurier Ngombé

Données personnelles et NTIC

« Revue d'actualité du droit des données à caractère personnel en Afrique », p. 76
Par Aline Mbenoun-Ngoué

ACTIVITÉS ACADÉMIQUES

Recension de travaux scientifiques, p. 78
Par Montcho Agbassa Éric, Ampah Johnson-Ansah & Yvon Laurier Ngombé

Actualité universitaire, p. 85
Par Aline Mbenoun-Ngoué

LE SEMESTRE DU PÉLÈRIN

Au-delà de la Propriété intellectuelle

« L'arbitrage et les procédures collectives en droit OHADA et marocain », p. 87
Par Youssouf Adoum Youssouf

« La CCJA et la propriété intellectuelle ou lorsque les plaideurs s'emmêlent », p. 95
Par Yvon Laurier Ngombé

Au-delà de l'Afrique

« Les IA dans les balances de la justice ou le purgatoire d'"une récente entrée dans le paradis" », p. 97
Par Yvon Laurier Ngombé

« Un paradis fiscal n'est pas forcément un paradis numérique », p. 99
Par Yvon Laurier Ngombé

« L'originalité de la marque : quand les juridictions se jouent des *faux-amis* », p. 100
Par Christian Kpolo

« Clarification par la Cour de cassation française de la date limite de dépôt d'une demande divisionnaire de seconde génération », p. 101
Par Christian Kpolo

BIBLIOGRAPHIE, p. 102
Par Iony Randrianirina, Firmin Kouadio, Christian Kpolo, Yvon Laurier Ngombé

EDITORIAL

Un long chemin vers la protection ?

Par Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APLA

Voici maintenant soixante ans, ou plutôt voici à peine soixante ans ou encore déjà soixante ans…qu'importe. En 1963 sur les rives d'un majestueux et célèbre fleuve, se tenait une réunion qui ouvrait le débat et la voie de la protection d'un sujet particulier de la propriété intellectuelle. En effet, du 5 au 10 août 1963 s'est tenue à Brazzaville, au Congo, une « Réunion africaine d'étude sur le droit d'auteur » (organisée par l'union de Berne et l'Unesco). Il a été résolu, à la suite de cette réunion, d'envisager la protection, par le droit d'auteur, du folklore.

Depuis cette date, plusieurs législateurs en Afrique (à commencer par la Tunisie en 1966) mais pas seulement (ainsi la Bolivie en 1967) ont essayé d'ouvrir la porte du droit d'auteur aux « œuvres du folklore ». La loi-type de Tunis de 1976 qui a longtemps servi de modèle aux législateurs africains prévoyait la possibilité de protéger cet objet plutôt mal identifié.

S'ensuivaient un engouement doctrinal, puis d'inévitables et parfois passionnantes (voire passionnées) controverses. Par la suite, il a semblé à plusieurs spécialistes et à de nombreux législateurs que le folklore devait être soumis à un régime particulier au regard de sa spécificité. Certains textes retenaient davantage la notion d'expression du folklore plutôt que celle d'œuvre du folklore. Aujourd'hui l'expression internationalement consacrée est celle d'expression culturelle traditionnelle. Qu'importe le vocabulaire, l'objet demeure le même et sa protection au titre du droit d'auteur est toujours prévue par plusieurs lois africaines relatives à la propriété littéraire et artistique, parfois dans un chapitre spécifique.

Pour de nombreux spécialistes, les expressions culturelles traditionnelles ne seraient pas une propriété intellectuelle. En réalité, la voie choisie à l'échelle internationale et aux niveaux régionaux est celle des propriétés intellectuelles. La seule question est alors celle de savoir laquelle. Dans l'espace ARIPO c'est un droit *sui generis* inspiré du droit d'auteur et renvoyant aux droits coutumiers.

Les regards sont désormais tournés vers l'instrument en voie d'adoption par l'OMPI. Les Etats dont sont originaires les expressions culturelles traditionnelles les plus diffusées dans le monde espèrent en réalité une protection effective afin d'éviter des appropriations culturelles ou une forme d'enrichissement injuste de certains exploitants.

Le succès d'un instrument international contribuerait à l'effectivité de la protection attendue, les lois internes déjà nombreuses ne pouvant y aboutir. Soixante ans après, une adoption définitive et une ratification massive du texte de l'OMPI serait un pas décisif vers une protection effective.

Finalement qu'importe le régime de propriété intellectuelle, pourvu que la protection soit efficace et effective.

Y.L.N.

PORTRAITS

Miriam Makeba, Angélique Kidjo et Aïcha Koné

"Les femmes et la propriété intellectuelle : Accélérer le rythme de l'innovation et de la créativité". Tel est le thème de la Journée Mondiale de la Propriété Intellectuelle pour l'année 2023.

L'Association pour la Promotion de la Propriété Intellectuelle en Afrique (APIA) se devait de marquer le coup. Et pour se faire, le bureau de l'Association a proposé au comité de rédaction de consacrer la Rubrique « Portrait » de ce numéro à trois Divas de la musique Africaine.

Célébrer la Journée Mondiale de la Propriété Intellectuelle à travers le prisme des femmes, en particulier des artistes africaines, est une opportunité pour mettre en lumière non seulement le talent, mais aussi l'impact culturel, social et politique de celles qui ont marqué ou qui marquent l'histoire de la musique. La RSPIA est donc très honorée de proposer un portrait croisé de Miriam Makeba, Angélique Kidjo et Aïcha Koné.

Miriam Makeba : La Voix de l'Afrique du Sud sous l'Apartheid

Vie et Parcours

Miriam Makeba, surnommée "Mama Africa", est née le 4 mars 1932 à Johannesburg, en Afrique du Sud. Sa vie a été profondément marquée par la lutte contre l'apartheid. Née dans un pays et à une époque où la ségrégation et l'oppression étaient quotidiennes, son parcours a été parsemé d'épreuves et de combats.

Carrière Musicale

- **Débuts** : Miriam a commencé sa carrière musicale avec le groupe Manhattan Brothers avant de créer son propre groupe, The Skylarks, qui mélangeait jazz et musique traditionnelle sud-africaine.
- **Exil** : En 1959, après avoir joué dans le documentaire anti-apartheid "Come Back, Africa", elle a été exilée d'Afrique du Sud.
- **Succès international** : Makeba est devenue la première artiste africaine à populariser la musique africaine en dehors du continent, avec des hits comme "Pata Pata" et "The Click Song". Son duo avec Harry Belafonte a contribué à élargir son audience hors d'Afrique.
- **L'ONU et le retour en grâce** : En 1963, elle témoigne devant l'ONU contre l'apartheid et son passeport sud-africain est révoqué. Malgré cet exil forcé, elle continue de promouvoir la musique et la culture africaine à travers le monde.

Anecdotes notables

- **Mariage et militantisme** : Miriam Makeba a été mariée à Hugh Masekela et plus tard à Stokely Carmichael, des figures notoires du militantisme, le premier dans la musique et le second dans les droits civiques.
- **Retour symbolique** : Après la libération de Nelson Mandela en 1990, Miriam Makeba retourne en Afrique du Sud, renouant avec sa terre natale après des décennies d'exil.

Inspiration et Influence

Miriam Makeba a puisé son inspiration dans ses racines sud-africaines et les luttes de son peuple. Sa musique reflète à la fois la richesse de la culture africaine et un vibrant message de résistance contre l'oppression. Elle a inspiré de nombreux artistes et activistes à travers le monde par sa grâce, son courage et sa détermination.

Héritage musical, social et politique

- **Musical** : Miriam Makeba a laissé un répertoire qui continue d'être célébré pour sa beauté et son authenticité, devenant ainsi une icône intemporelle de la musique africaine.
- **Social** : En dépit de son succès mondial, elle a toujours prôné l'égalité, les droits de l'homme et la justice sociale.
- **Politique** : Miriam Makeba est devenue un symbole de la lutte contre l'apartheid, utilisant sa voix et sa plateforme internationale pour faire connaître les horreurs du régime ségrégationniste sud-africain.

La vie et l'héritage de Miriam Makeba sont une preuve poignante de l'influence d'une artiste bien au-delà de son art. Malgré un succès international, elle n'a jamais abandonné son identité ni ses convictions. Miriam Makeba incarne la résilience de l'esprit humain et la puissance qu'une personne a, non seulement pour créer de la beauté à travers la musique mais également pour influencer le changement positif dans le monde. Les échos de sa voix et de sa lutte résonnent encore dans les mouvements de justice sociale et les notes de musique contemporaine.

* * *

Angélique Kidjo : L'Étoile de la World Music et militante humanitaire

Vie et Parcours

- **Naissance et enfance** : Angélique Kidjo est née le 14 juillet 1960 à Ouidah, au Bénin. Elle grandit dans un environnement où diverses musiques, notamment celles des traditions tribales, du pop, du jazz et du R&B, se mêlent.
- **Exil** : En raison du régime oppressif et du climat politique instable au Bénin, Angélique Kidjo s'exile en France à l'âge de 23 ans pour poursuivre sa passion, la musique, et échapper à la menace constante.

Carrière musicale

- **Début en France** : À Paris, elle s'imprègne de divers styles musicaux et se fait rapidement remarquer pour sa voix puissante et sa présence sur scène électrisante.
- **Percée internationale** : Sa carrière prend une envergure internationale avec des albums comme "Logozo" et "Agolo", ce dernier lui valant sa première nomination aux Grammy Awards.
- **Grammys et reconnaissances** : Au cours de sa carrière, Angélique Kidjo a remporté quatre Grammy Awards et a été reconnue pour son style musical unique qui fusionne différents genres.

Anecdotes Notables

- **Rencontres marquantes** : Elle a notamment collaboré avec de nombreux artistes célèbres, dont Manu Dibango, Carlos Santana, Peter Gabriel, Ziggy Marley et Alicia Keys, tissant des liens entre diverses cultures musicales.
- **TED Talk** : Angélique Kidjo a donné une conférence TED, partageant sa vision de l'Afrique, ses expériences et sa sagesse sur la scène mondiale.

Inspiration et Influence

- **Racines et diversité musicale** : Inspirée par les musiques traditionnelles de son Bénin natal, le funk, le jazz, et bien plus, Angélique Kidjo crée un son universel, défiant les frontières et les genres. Elle a été inspirée par Miriam Makeba et Bella Bellow.
- **Droits des femmes** : Elle puise également dans ses expériences de femme africaine pour aborder les thèmes de l'égalité des sexes, de l'autonomisation des femmes et de la justice sociale dans son œuvre.

Héritage musical, social et politique

- **Ambassadrice de l'UNICEF** : Elle utilise sa notoriété pour attirer l'attention sur des questions telles que l'éducation, la santé et les droits des filles et des femmes en Afrique et dans le monde.
- **Bibliothèque de chansons** : Son héritage musical est une bibliothèque de chansons qui célèbrent l'Afrique, sa culture, ses luttes et ses espoirs.
- **Fondation Batonga** : Elle co-fonde la Fondation Batonga, qui œuvre pour l'éducation des jeunes filles en Afrique, démontrant son engagement dans le changement social et éducatif.
- **Influence mondiale** : Angélique Kidjo a non seulement influencé la musique mondiale, mais aussi introduit les sonorités africaines dans la pop mondiale, en se faisant la voix des sans voix.

Angélique Kidjo, avec son mélange distinctif de divers styles musicaux et son engagement pour la justice sociale et les droits des femmes, est une force avec laquelle il faut compter dans l'industrie musicale mondiale et au-delà. Elle démontre avec éloquence comment la musique peut être un pont entre les cultures, les peuples et les causes, laissant un héritage qui résonnera pour les générations à venir, tant sur le plan musical que social. Son militantisme en faveur des causes juste est perceptible dans son combat pour une meilleur protection des droits des créateurs dont l'expression la plus aboutie est sans nul doute son action au sein de La Confédération internationale des sociétés d'auteurs et compositeurs (CISAC) au sein de laquelle elle a occupé le poste de Vice-Présidente.

* * *

Aïcha Koné : La Voix Mélodieuse de la Côte d'Ivoire

Vie et Parcours

- **Enfance et Premiers pas** : Née le 21 mai 1957 à Abidjan, Côte d'Ivoire, Aïcha Koné est une chanteuse mandingue dont les mélodies ont conquis non seulement l'Afrique de l'Ouest, mais aussi le monde. Sa carrière commence à l'adolescence lorsqu'elle remporte un concours de chant, annonçant une étoile montante dans l'univers de la musique africaine.
- **Péripéties politiques** : Son parcours artistique est marqué par une carrière luxuriante mais aussi par son interaction avec la politique, notamment lorsqu'elle est contrainte à l'exil pendant une période de troubles politiques en Côte d'Ivoire.

Carrière Musicale

- **Ascension** : Aïcha gagne rapidement une reconnaissance continentale pour sa voix puissante et expressive, étant acclamée dans divers pays africains.
- **Caractéristiques musicales** : Sa musique, principalement zouk et coupé-décalé, est également infusée de sonorités traditionnelles, ce qui crée une fusion séduisante et unique.
- **Chansons engagées** : À travers sa musique, elle traite de thèmes sociaux et politiques pertinents, prêtant sa voix aux opprimés et aux laissés-pour-compte.

Anecdotes Notables

- **Survivante** : Aïcha est aussi connue pour sa résilience face aux multiples défis, y compris des problèmes de santé et des obstacles politiques, et continue de performer et de produire de la musique.
- **L'Artiste accomplie** : Elle a chanté devant des personnalités notoires.

Inspiration et Influence

- **Inspiration sociale** : Koné s'inspire profondément de la société qui l'entoure, utilisant sa musique comme un outil pour discuter des questions sociales et politiques.
- **Harmonies de la tradition** : Elle intègre habilement les harmonies de la musique traditionnelle africaine avec des genres plus modernes, formant une synergie captivante entre l'ancien et le nouveau.

Héritage musical, social et politique

- **Pionnière de la musique** : Aïcha Koné est perçue comme une des pionnières de la musique africaine, ayant ouvert la voie à de nombreux artistes du continent.
- **Impact social** : Grâce à ses chansons et son implication sociale, elle a joué un rôle essentiel dans l'éveil de la conscience sociale et politique dans différentes régions d'Afrique.
- **Éducatrice** : Au-delà de sa carrière musicale, elle a également consacré du temps à éduquer la jeune génération sur les valeurs, les traditions et l'histoire africaine.

Aïcha Koné, avec sa voix émouvante et ses mélodies évocatrices, demeure une figure emblématique dans le monde de la musique africaine. Sa capacité à mélanger le moderne et le traditionnel, tout en abordant des questions cruciales avec sensibilité et audace, lui confère une place respectée dans l'histoire de la musique et de la culture africaine. Son héritage continue d'inspirer, de mobiliser et d'éduquer, faisant d'elle plus qu'une artiste, mais également une actrice du changement et une gardienne de la tradition et de la conscience africaine.

Le Bureau de l'APIA.

Actualité de la propriété intellectuelle en Afrique anglophone en 2022

Par Enyinna Nwauche
Full Professor, Nelson Mandela School of Law
University of Fort Hare (South Africa)

I. ARIPO

A. Traités

Modifications récentes du protocole d'Harare sur les brevets et les dessins industriels

L'une des résolutions du Conseil d'administration de l'ARIPO lors de sa 46e session, qui s'est tenue à Maputo, au Mozambique, du 21 au 25 novembre 2022, a été l'adoption des modifications apportées au Protocole de Harare sur les brevets et les dessins industriels, ainsi qu'à ses Règlements d'exécution, qui sont entrés en vigueur le 1er janvier 2023.

Les points saillants des modifications de 2022 au Protocole de Harare sont les suivants :

1. Le préambule du Protocole de Harare a été modifié pour inclure la Convention de Paris et les articles du Traité de coopération en matière de brevets.

2. Les nouveaux paragraphes 2 et 3 de la Section 1 définissent clairement les brevets, dessins industriels et modèles d'utilité de l'ARIPO et leur effet national dans les États membres.

3. La nouvelle Section 1*bis* modifie la Section 1 et introduit une nouvelle Section 1bis indiquant clairement qu'un brevet, un dessin industriel ou un modèle d'utilité de l'ARIPO peut avoir effet dans l'un seulement ou dans tous les États contractants.

4. La nouvelle Section 2(3) facilite clairement les demandes conjointes désignant différents États contractants.

5. La nouvelle Section 2(7) soutient clairement la Règle 5(2) en confirmant que la demande peut être déposée dans n'importe quelle langue mais doit être traduite en anglais dans un délai de 2 mois.

6. La nouvelle Section 2(8) définit clairement le droit de priorité de chaque brevet, dessin industriel ou modèle d'utilité.

7. La nouvelle Section 3(1A à 1D) précise qu'une demande de brevet ARIPO ne concerne qu'une invention clairement divulguée de telle sorte que toute personne versée dans la technique puisse reproduire l'invention.

8. Il est nécessaire d'établir un lien entre les exigences physiques définies dans les instructions administratives, comme indiqué dans la nouvelle version de la section 3, 2(A).

9. La nouvelle Section 3(6A) offre clairement aux États membres la possibilité d'accepter ou de refuser un brevet accordé ou en voie d'octroi par le Bureau de l'ARIPO. L'ancienne Section 3(6) sera renumérotée en 3(6B).

10. La nouvelle Section 3(11A) définit clairement la nouveauté d'une invention, et l'ancienne Section 3(11) sera renumérotée en Section 3(11G).

11. La Section 3(11B) définit clairement les documents d'antériorité comme tout ce qui est rendu public dans le monde par divulgation écrite (y compris les dessins et autres illustrations), divulgation orale ou par utilisation ou exposition, est considéré comme antériorité pourvu que cette divulgation ait eu lieu avant la date de dépôt de la demande ou, si une priorité est

revendiquée, avant la date de priorité valablement revendiquée à cet égard. De plus, une divulgation de l'invention lors d'une exposition officielle ou officiellement reconnue ne sera pas prise en compte si elle a eu lieu moins de six (6) mois avant la date de dépôt de la demande ou, si une priorité est revendiquée, avant la date de priorité valablement revendiquée à cet égard.

12. La Section 3(11C) définit clairement l'exposition en relation avec la Convention sur les expositions internationales.

13. La nouvelle Section 3(11D) définit le concept inventif d'une invention.

14. La nouvelle Section 3(11E) définit clairement l'applicabilité industrielle d'une invention déposée à l'ARIPO.

15. La nouvelle Section 3(11F) définit clairement les possibilités de modification d'une demande.

16. La Section 3(13A) prévoit une licence partielle ou totale à l'égard des États désignés.

17. La nouvelle Section 3(13B) définit la cession d'un brevet ARIPO.

18. Les nouvelles Sections 14A à 14E définissent clairement la propriété des droits de brevet d'un brevet ARIPO et indiquent clairement qu'en cas de contrefaçon, le droit national prévaut.

19. Les nouvelles Sections 3(15A à 15B) définissent clairement les procédures pour le dépôt de demandes divisionnaires auprès du Bureau.

20. La nouvelle Section 3(16) définit clairement les termes et l'interprétation des revendications, de la description et des dessins dans une demande ARIPO.

21. La nouvelle Section 3(17) à 3(17)(iii) précise clairement les délais fixés dans les Instructions administratives et les Règlements pour la mise en œuvre du Protocole de Harare.

21. La nouvelle Section 3(18) définit clairement les procédures de révocation ou d'annulation d'un brevet ARIPO.

22. La Règle 5(3) a été modifiée pour permettre le dépôt électronique.

23. Nouvelle Règle 5bis pour permettre le dépôt électronique de brevets, dessins industriels et demandes de modèles d'utilité.

24. La Règle modifiée 18bis(2) stipule que la nouveauté et l'applicabilité industrielle, au lieu de la "démarche inventive", dans les États contractants du Protocole, doivent être appliquées en ce qui concerne les modèles d'utilité car pour les modèles d'utilité, la démarche inventive n'est pas prise en compte et seule la nouveauté par rapport à la documentation locale est prise en considération.

25. L'abrogation de la Règle 21(3) vise à supprimer l'obligation pour le Bureau de rappeler au demandeur ou au titulaire du brevet de renouveler le brevet ou la demande de brevet au moins un mois avant la date à laquelle une taxe annuelle de maintien doit être payée. Ceci suit l'exemple d'autres bureaux similaires où les demandeurs doivent surveiller les dates de renouvellement de leurs brevets ou demandes de brevet respectifs.

27. Modification de la Règle 22(1) pour inclure la communication électronique entre le Bureau et les États désignés.

Modifications récentes du protocole de Banjul sur les marques

L'une des résolutions du Conseil d'administration de l'ARIPO lors de sa 46e session, tenue à Maputo, au Mozambique, du 21 au 25 novembre 2022, a été l'adoption des modifications apportées au Protocole de Banjul sur les marques ainsi qu'à ses Règlements d'exécution, qui sont entrés en vigueur le 1er janvier 2023.

Les changements comprennent une modification de la règle 13Bis qui inclut l'annulation d'une marque enregistrée en vertu de l'article 8:2 qui doit être communiquée à l'Office de l'ARIPO en plus d'autres actions telles que les changements dans les indications enregistrées, les retraits de demandes, l'annulation de classes désignées ou la réduction de classes.

Des modifications ont également été apportées aux redevances du protocole de Banjul.

B. Cadre réglementaire émergent

Protocole sur les indications géographiques

Le Conseil administratif de l'ARIPO, lors de sa 45e session en 2021, a convenu de créer le Groupe de travail ad hoc sur les Indications Géographiques. En 2022, des consultations sont en cours pour établir un cadre réglementaire pour la gestion des Indications Géographiques. Un sous-groupe de travail sur les Indications Géographiques, composé du Ghana, du Kenya, du Libéria, du Malawi, du Mozambique et de la Zambie, délibère sur un cadre juridique approprié, le processus d'enregistrement, le contrôle de la qualité et les mécanismes de mise en application.

II. AFRIQUE DU SUD

A. Législation

Législation Émergente

La Réforme de la Loi sur le Droit

Le processus de réforme législative du droit d'auteur sud-africain a débuté en 2009, lorsque le ministère du commerce, de l'industrie et de la concurrence (actuellement le DTIC, anciennement le DTI) a commandé une série d'études. À la suite de ces études et de l'engagement du public, le DTI a créé en 2010 la Commission d'examen du droit d'auteur, présidée par le juge Ian Farlam, qui a délibéré sur des questions telles que les pratiques de distribution des sociétés de gestion collective. La CRC a recommandé que le DTI entame le processus de modification de la loi sur le droit d'auteur de 1978. Des projets d'amendements à la loi sur le droit d'auteur ont été publiés pour consultation publique en 2015 et un projet de loi d'amendement du droit d'auteur (CAB) a été présenté à l'Assemblée nationale. Plusieurs versions du CAB ont été présentées à l'Assemblée nationale et ont fait l'objet de nombreux commentaires et auditions publics. En 2019, l'Assemblée nationale sud-africaine et le Conseil national des provinces (NCOP) ont adopté le projet de loi, qui a ensuite été envoyé au président pour qu'il le sanctionne afin qu'il devienne une loi. Le président n'a pas donné son aval au CAB mais l'a renvoyé au Parlement en juin 2020 en invoquant des réserves constitutionnelles. En août 2020, le Parlement a entamé le processus de prise en compte des réserves présidentielles par le biais d'appels à commentaires et d'auditions publiques qui sont toujours en cours.

B. Jurisprudence

Blind SA c. Ministre du Commerce, de l'Industrie et de la Concurrence et Autres [2022] ZACC 33

Le mercredi 21 septembre 2022 à 9h30, la Cour constitutionnelle a rendu sa décision dans le cadre d'une demande de confirmation de l'ordonnance d'invalidité constitutionnelle rendue par la High Court d'Afrique du Sud, Division Gauteng, Pretoria (Haute Cour). La High Court a déclaré la loi 78 de 1978 sur le droit d'auteur inconstitutionnelle dans la mesure où elle ne prévoit pas d'exceptions qui permettraient, grâce à la conversion d'œuvres protégées par le droit d'auteur, d'obtenir des formats adaptés permettant l'accès à ces œuvres. Elle a ordonné que les dispositions du Copyright Amendment Bill [B 13B - 2017] (CAB), telles qu'elles figurent à l'article 19D du CAB, soient interprétées comme si elles étaient spécifiquement incorporées dans les

dispositions de la loi sur le droit d'auteur afin d'éliminer l'incompatibilité de la loi avec la Constitution.

Devant la Cour constitutionnelle, le requérant, Blind SA, et le premier défendeur, le ministre du commerce, de l'industrie et de la concurrence (le ministre) ont convenu que la loi sur le droit d'auteur était inconstitutionnelle dans la mesure où elle avait été déclarée telle par la High Court. Le professeur Owen Dean, Media Monitoring Africa Trust (MMA) et la Commission internationale de juristes (CIJ) ont respectivement été admis en tant que premier, deuxième et troisième *amici*.Le cœur du problème concernait l'affirmation de Blind SA selon laquelle la Loi sur le Droit d'Auteur limite la disponibilité des œuvres protégées par le droit d'auteur dans des formats accessibles aux personnes ayant des handicaps visuels et imprimés. La Loi sur le Droit d'Auteur exige le consentement du titulaire des droits pour convertir des œuvres en formats adaptés à l'utilisation par des personnes ayant des handicaps visuels et imprimés. En conséquence, ces personnes rencontrent des limitations sévères pour accéder aux œuvres protégées que les personnes sans ces handicaps ne rencontrent pas. Un processus législatif est en cours pour modifier la Loi sur le Droit d'Auteur. Ce processus dure depuis 2015. Le 28 mars 2019, le Parlement a adopté le CAB. Le CAB visait à introduire l'article 19D en vertu duquel des personnes prescrites peuvent, sans l'autorisation du titulaire du droit d'auteur, réaliser, fournir et entreprendre toute étape intermédiaire pour fournir une copie accessible à une personne handicapée ; offrant ainsi des exceptions aux protections du droit d'auteur afin de permettre aux personnes aveugles et malvoyantes et aux personnes ayant d'autres handicaps d'accéder à ces œuvres dans des formats adaptés à leurs handicaps particuliers. Le 16 juin 2020, le CAB a été renvoyé devant l'Assemblée nationale par le Président en vertu de l'article 79(1) de la Constitution. Mécontent de ce long processus législatif, Blind SA a saisi la High Court pour obtenir une ordonnance déclarant la Loi sur le Droit d'Auteur inconstitutionnelle dans la mesure où elle limite injustement les droits des personnes ayant des handicaps visuels et imprimés.

Le 7 décembre 2021, la High Court a déclaré la Loi sur le droit d'auteur inconstitutionnelle dans la mesure où elle ne prévoit pas d'exceptions permettant aux personnes souffrant de handicaps visuels et imprimés d'accéder à ces œuvres. Cette demande n'a pas été contestée. La High Court a noté que, conformément à la déclaration d'intention de ratifier le Traité de Marrakech visant à faciliter l'accès aux œuvres publiées pour les personnes aveugles, malvoyantes ou ayant d'autres handicaps imprimés, le Parlement a adopté le CAB qui propose l'insertion de la nouvelle section 19D pour créer des exceptions au profit des aveugles et des personnes souffrant de handicaps visuels et imprimés. La Cour a jugé ce retard inacceptable et contraire à l'article 36(1) de la Constitution, car il perpétue injustement la violation des droits des aveugles et des personnes souffrant de handicaps visuels et imprimés.

Dans une décision unanime rédigé par le juge Unterhalter, la Cour constitutionnelle a confirmé la décision de la High Court concernant l'inconstitutionnalité.

La Cour a d'abord identifié le cas invoqué par Blind SA comme étant la rareté des œuvres littéraires publiées dans des formats accessibles à l'usage des personnes souffrant de déficiences visuelles et de troubles de la lecture. Cette rareté est imputable à la difficulté d'obtenir l'autorisation requise des titulaires de droits d'auteur sur les œuvres littéraires. Après avoir identifié le cas avancé par Blind SA, la Cour a ensuite identifié ce qui n'était pas en cause dans cette affaire : (a) la nécessité d'accéder à des œuvres littéraires non publiées ; (b) l'importation et

l'exportation d'œuvres protégées par le droit d'auteur et ; (c) une contestation visant à soumettre le retard du Parlement à une révision constitutionnelle.La Cour a affirmé que la législation protégeant les droits des titulaires de droits d'auteur doit tenir compte des impacts différents de cette protection sur différentes catégories de personnes. Les personnes souffrant de handicaps visuels et imprimés subissent de grandes difficultés en raison de l'exigence d'autorisation, ce qui constitue une discrimination injuste basée sur le handicap et viole ainsi l'article 9(3) de la Constitution. De plus, cette exigence méconnait les droits de ces personnes tels que définis dans les articles 10 (dignité), 16(1)(b) (liberté d'expression), 29(1) (droit à l'éducation) et 30 (langue et culture) de la Constitution.

La Cour a ensuite examiné si les pouvoirs conférés au Ministre en vertu de l'article 13 pour émettre des règlements concernant les exceptions générales à la reproduction des œuvres pouvaient sauver la loi de l'inconstitutionnalité. La Cour a conclu que la reproduction d'œuvres littéraires, même interprétée de manière large, était insuffisante pour convertir ces œuvres en formats accessibles. Par conséquent, l'article 13 ne sauvait pas la Loi de son inconstitutionnalité.

Après cet examen, la Cour a évalué les remèdes pour remédier à l'inconstitutionnalité. Elle a décidé qu'une lecture intégrale de la section 19D du CAB était trop large et imprécise. Ainsi, la Cour a formulé un ordre répondant au cas présenté par Blind SA. Cet ordre déclare notamment les sections 6 et 7 (octroyant des droits exclusifs aux titulaires de droits d'auteur) et la section 23 (définissant les circonstances d'infraction au droit d'auteur) de la Loi sur le droit d'auteur comme étant inconstitutionnelles. De plus, des termes clés ont été définis pour rendre la lecture de la disposition immédiatement opérationnelle.

En conséquence, la Cour a confirmé la décision de la Haute Cour déclarant la Loi sur le droit d'auteur inconstitutionnelle, mais seulement dans la mesure identifiée ci-dessus. Elle a ordonné une lecture intégrale de l'article 13 de la Loi sous le titre "section 13A Exceptions applicables aux personnes bénéficiaires". Cette lecture doit durer 24 mois afin de permettre au Parlement de remédier au défaut de la loi sur le droit d'auteur ayant donné lieu à son invalidité.

III. NIGERIA

A. Législation

Loi nigériane sur le Droit d'auteur 2022

La Loi nigériane sur les droits d'auteur 2022 a été promulguée par l'ancien président Buhari, mettant fin à des décennies de plaidoyer et d'activisme pour la réforme de la Loi nigériane sur le Droit d'auteur de 1988. Les objectifs de la Loi sont de protéger les droits des auteurs pour qu'ils obtiennent des rémunérations justes, garantir un accès approprié aux œuvres protégées, faciliter la conformité du Nigeria aux obligations internationales, et renforcer la capacité réglementaire de la Commission nigériane des droits d'auteur.

Principaux éléments de la Loi de 2022 :

- **Droit de suite modifié** : La Loi abrogée de 1988 prévoyait que les auteurs (y compris les héritiers et successeurs) des œuvres artistiques, littéraires et musicales avaient le droit de partager les recettes de la vente de l'original de cette œuvre ou manuscrit lors d'une vente aux enchères publiques ou par un revendeur. La Loi de 2022 exclut maintenant explicitement les œuvres architecturales et les œuvres d'art appliqué.

Exceptions et limitations au droit d'auteur :

- **Défense renforcée du "Fair Dealing"** : la Loi de 2022 intègre des éléments des dispositions du "Fair Use" de la Loi américaine sur les droits d'auteur.
- La disposition de la loi de 2022 qui incorpore certaines parties des dispositions de la loi américaine sur le droit d'auteur relatives à l'utilisation équitable ("Fair Use"). La loi de 1988 prévoyait une exception pour l'utilisation équitable dans la deuxième annexe de cette loi et incluait, entre autres, la recherche, l'usage privé, la critique, la revue, le compte rendu d'événements d'actualité, la parodie, le pastiche ou la caricature comme motifs d'utilisation équitable. La loi de 2022 a intégré l'utilisation équitable dans le corps de la loi et a ajouté "la recherche non commerciale et l'étude privée" comme motifs supplémentaires. L'ajout de facteurs, sans doute empruntés à la loi américaine sur le droit d'auteur, à prendre en considération pour déterminer l'utilisation équitable est important. Il s'agit notamment du but et du caractère de l'utilisation, de la nature de l'œuvre, de la quantité et du caractère substantiel de la partie utilisée par rapport à l'ensemble de l'œuvre et de l'effet de l'utilisation sur le marché potentiel ou sur la valeur de l'œuvre.

- **Accès aux œuvres en vertu du Traité de Marrakech** : La Loi de 2022 prévoit la mise en œuvre des obligations du Nigeria en tant qu'État partie au Traité de Marrakech visant à faciliter l'accès aux œuvres publiées pour les personnes aveugles, malvoyantes ou empêchées de lire les imprimés.

Licences obligatoires

- **Dispositions relatives au contenu en ligne :** La Loi de 2022 permet désormais à un titulaire de droits d'auteur d'émettre un avis demandant à un fournisseur de services de retirer un contenu contrefaisant.

- **Protection renforcée pour les interprètes** : La Loi de 1988 protégeait les artistes-interprètes de manière rudimentaire. La Loi de 2022 renforce la protection des artistes-interprètes en les définissant ; en déterminant la nature et l'étendue des droits exclusifs qui leurs sont accordés; en ajoutant tels que la fixation d'une interprétation ou exécution non fixée, la location ou le prêt au public d'une fixation d'une interprétation ou exécution, et la mise à la disposition des membres du public ; la reconnaissance des droits moraux d'un artiste interprète ou exécutant et des droits des artistes interprètes ou exécutants sur les interprétations ou exécutions collectives..

- **Interdiction de contourner les mesures de protection technologique** :

- La loi de 2022 interdit le contournement d'une mesure technique de protection (MTP), le commerce d'une technologie, d'un produit, d'un service ou d'une pièce conçue pour contourner une MTP, ainsi que la fabrication d'un produit ou d'un dispositif conçu pour contourner une MTP. Il existe des exceptions à cette interdiction destinées à protéger les utilisations licites, telles que les exceptions et limitations au droit d'auteur et l'amélioration de l'interopérabilité d'un programme d'ordinateur.

Loi sur la facilitation des affaires (dispositions diverses) 2022, loi no. 5

Le 8 février 2023, le président Buhari a signé une loi qui introduit des mesures visant à faciliter les affaires au Nigeria en éliminant les obstacles perçus et vise à garantir la transparence, l'efficacité et la productivité. La loi modifie la législation pertinente, y compris la modification de la première annexe de la loi sur les brevets et les dessins, Cap. P2, Lois de la Fédération du Nigeria, 2004, en insérant un nouveau paragraphe "13A" qui autorise le ministre du Commerce et de l'Industrie à établir des règlements définissant la procédure de demande, d'octroi, d'utilisation et de retrait des licences obligatoires.

Loi nigériane sur les start-ups 2022

Dans le but stratégique de stimuler l'innovation au Nigeria, la Loi nigériane de 2022 sur les start-ups a été récemment promulguée. Cette loi vise à répondre à plusieurs défis rencontrés par les startups nigérianes, notamment l'absence d'un environnement favorable, un cadre réglementaire flou, un soutien insuffisant au contenu local, une protection et des incitations insuffisantes, comme des exonérations fiscales, des incitations pour attirer des capitaux étrangers et l'accès à une liste exclusive d'opportunités de financement public et privé.

Le Conseil pour l'innovation et l'entrepreneuriat numériques est chargé de mettre en œuvre les dispositions de la loi et comprend le président, le gouverneur de la banque centrale du Nigeria, des représentants du Forum consultatif des startups, le directeur général du régulateur nigérian de l'information et de la technologie et d'autres responsables gouvernementaux et privés clés.

Une partie des responsabilités statutaires du Conseil et du Secrétariat est de veiller à ce que les titulaires de droits de propriété intellectuelle soient encouragés à exploiter ces droits en les internationalisant et en les commercialisant. À cette fin, le secrétariat collaborera avec la Commission nigériane des droits d'auteur et les registres des marques, brevets et dessins, pour veiller à ce qu'ils désignent une section distincte sur le portail des startups pour faciliter l'enregistrement de la propriété intellectuelle.

IV. BOTSWANA

Politique de propriété intellectuelle du Botswana 2022

La Vision nationale de développement 2036 du Botswana sert d'ancre à cette initiative en envisageant une économie « efficace, dynamique et basée sur la connaissance, avec un accès à une main-d'œuvre qualifiée et compétitive au niveau international, des technologies de pointe et des infrastructures » (République du Botswana, 2016). Cette Vision reconnaît le rôle de la science, de la technologie, de l'innovation et de la créativité dans la création d'une économie axée sur la connaissance, nécessitant ainsi le développement d'un environnement propice à travers des politiques, cadres institutionnels et législatifs efficaces en matière de Propriété Intellectuelle (PI). Le pays a un potentiel exceptionnel en matière de PI ; cependant, il n'a pas reconnu la PI comme un moteur du développement économique.

Cela est démontré par le manque d'intégration de la PI dans les Plans Nationaux de Développement (PND), entraînant une allocation insuffisante de ressources pour la génération et l'exploitation de la PI, empêchant ainsi le pays de récolter les bénéfices économiques de la PI. Ce manque a souligné la nécessité de développer la Politique de Propriété Intellectuelle pour le Botswana. La Politique de Propriété Intellectuelle du Botswana a été élaborée avec l'aide de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI).

L'objectif principal de la Politique est d'exploiter le potentiel de PI du Botswana pour une croissance et un développement économiques inclusifs et durables, apportant la prospérité à chaque citoyen du Botswana. Elle repose sur six piliers interdépendants : améliorer le cadre de gouvernance de la PI pour promouvoir la protection des droits de PI ; faciliter la disponibilité et l'accès au financement pour la génération, l'acquisition et la commercialisation de la PI ; promouvoir la sensibilisation, l'éducation et la formation en matière de PI ; négocier efficacement les accords de PI au profit du Botswana ; développer les capacités entrepreneuriales dans les secteurs sélectionnés axés sur la PI ; et créer des structures institutionnelles appropriées pour le développement de la PI.

La mise en œuvre réussie de cette Politique permettra au Botswana d'utiliser son potentiel en matière de PI pour devenir une Économie Basée sur la Connaissance (EBC) et diversifier l'économie du Botswana pour créer de la prospérité pour tous.

V. KENYA

Gestion de l'innovation

Système d'enregistrement des droits de propriété intellectuelle

Dans une démarche sans précédent, qui sera probablement largement copiée à travers l'Afrique, l'Autorité Anti-Contrefaçon du Kenya (ACA) a mis en place un Système d'Enregistrement des Droits de Propriété Intellectuelle. Ce système est conçu pour capturer des détails relatifs aux droits de propriété intellectuelle protégés, aux détenteurs/titulaires de droits de propriété intellectuelle et aux agents désignés dans une base de données électronique appelée AIMS. Ces informations seront utilisées par l'ACA pour lutter contre la contrefaçon en vérifiant le statut des droits de PI enregistrés et les personnes concernées à contacter en cas de suspicion d'infraction aux droits de PI. AIMS peut également être consulté par les agents de protection des frontières pour déterminer le statut d'enregistrement des marchandises devant être importées au Kenya. Étant donné que les Règlements de Modification Anti-Contrefaçon interdisent l'importation au Kenya de marchandises portant une marque de commerce, un nom commercial ou un droit d'auteur à des fins commerciales, sauf si le droit de PI est enregistré, les importateurs ont également la responsabilité de s'assurer que les droits de PI relatifs aux marchandises importées sont déclarés via le système d'enregistrement. Le non-respect de cette règle par les importateurs entraînera des poursuites, la saisie des marchandises importées non conformes, et leur confiscation pour destruction par l'ACA. De plus, en cas de condamnation, ils sont passibles d'une amende d'au moins trois à cinq fois la valeur du prix de vente au détail actuel des marchandises, et/ou d'une peine d'emprisonnement ne dépassant pas cinq à 15 ans.

E.N.

(Traduit de l'anglais par John-Pierce Ngombé)

Le Droit d'auteur à l'épreuve du droit à l'image dans l'exploitation des œuvres visuelles en République Démocratique du Congo

Par Thédore Nganzi-Ndoni
Docteur en Droit de l'Université de Kinshasa
Enseignant à l'Institut national des arts (Kinshasa)

Le droit d'auteur consacre un monopole limité par des exceptions strictement énumérées dans la loi. Or, la limite du droit à l'image n'est pas une exception au droit d'auteur au sens de la convention de Berne de 1886.

Le droit à l'image n'est pas défini en droit positif congolais. L'article 23.b[1] de l'ordonnance-loi N°86/033 du 05 avril 1986 portant protection du droit d'auteur et des droits voisins en République Démocratique du Congo[2] institue simplement le droit à l'image comme une limite au droit d'auteur. Cependant, nous pouvons considérer que ce droit fait partie intégrante du droit à la vie privée qui est protégé par la Constitution de la République Démocratique du Congo de 1986 en son article 31[3].

La loi pénale en vigueur réprime quelques atteintes à la vie privée, notamment la violation du domicile, la violation du secret de correspondance, la violation du secret professionnel[4]… On retrouve également la loi n°96-002 du 22 juin 1966 protégeant la liberté de presse spécialement aux dispositions qui régissent les délits de presse, notamment le droit de réponse, la réplique, la rectification[5] L'Ordonnance-Loi N°23-010 du 13 mars 2023 portant code du numérique réprime pénalement la diffusion du contenu tribaliste, raciste et xénophobe[6] ainsi que la pornographie infantile[7].

L'analyse de ces dispositions confirme l'absence d'une définition légale claire du droit à l'image en République Démocratique du Congo. Ainsi, pour combler cette lacune, nous pouvons proposer une définition du droit à l'image comme la prérogative

[1] L'article 23. B de la loi de la RDC de 1986 sur le droit d'auteur dispose que, lorsqu'il s'agit d'une œuvre plastique ou d'un portrait de commande, l'auteur ou le propriétaire d'un portrait ne peut le reproduire ou l'exposer en public sans l'assentiment de la personne y représentée. Cet article crée un conflit potentiel entre le droit d'auteur et le droit à l'image de la personne représentée dans le portrait.

[3] Cet article 31 de la constitution dispose : « toute personne a droit au respect de sa vie privée et au secret de sa correspondance, de la télécommunication ou de toute autre forme de communication. Il ne peut être porté atteinte à ce droit que dans les cas prévus par la loi ».

[4] Articles 69 à 75 du décret du 30 janvier 1940 portant Code pénal congolais toujours en vigueur.

[5] Articles 37-43, 67-75, 79 de la loi N° 96-002 du 22 juin 1966.

[6] Article 356 du Code Numérique dispose : « Quiconque aura, intentionnellement, Cree, télécharge, diffuse ou mis à la disposition du public par le biais d'un systèmes informatique des écrits, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées OU de théories, nature raciste, tribaliste ou xénophobe ou sous quelque-forme que ce au sens de la présente ordonnance-loi et conformément aux dispositions s ·c1e l'ordonnance-loi n° 66-342 du 07 juin 1966 portant répression du racisme et du tribalisme, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende d'un million a dix millions de francs congolais ou de l'une de ces peines seulement ».

[7] Article 357 du Code du Numérique dispose : « Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de rendre disponible, de vendre, de se procurer ou de procurer à autrui, de posséder tout matériel pornographique mettant en scène un enfant par le biais d'un système informatique ou d'un réseau de communication électronique, est puni de cinq à quinze ans de servitude pénale principale et d'une amende de deux mille à un million de Francs congolais ».

reconnue à toute personne physique d'autoriser que son visage ou tout son corps soit représenté ou reproduit dans les arts graphiques ou plastiques, par la photographie ou par une technique analogue[8].

Ce droit à l'image, dans la loi de la République Démocratique du Congo sur le droit d'auteur, crée simplement une limite[9] à l'exercice du droit d'auteur pour les créateurs des œuvres visuelles, principalement pour les portraits des personnes physiques et les photographies. En effet, un créateur d'une telle œuvre ne peut pas l'exploiter en public sans l'autorisation ou l'accord de la personne représentée dans le portrait ou dans la photographie.

Cette disposition légale est rare[10] en Afrique Francophone. Sur plus de 20 États francophones, seuls cinq États ont adopté cette règle. C'est ainsi que nous posons la question de l'opportunité d'une telle disposition dans la loi de la République Démocratique du Congo de 1986 sur le droit d'auteur. En effet, Le droit à l'image est un droit de la personnalité dont la violation relève normalement du droit pénal ou du droit civil des personnes[11]. Il s'agit d'un problème qui relève du droit commun de la responsabilité. Curieusement, le législateur de la loi de 1986 sur le droit d'auteur l'a inséré à son article23.b comme une limite à l'exercice du droit d'auteur. Cela risque de créer un conflit entre les deux droits (le droit d'auteur et le droit à l'image).

Ce conflit potentiel entre les créateurs des œuvres visuelles (les portraits des commandes ou des photographies) et les personnes y représentées est possible dans plusieurs hypothèses. En effet, il est possible que le droit à l'image empêche un auteur d'exploiter une photographie pour la simple raison qu'il n'a pas obtenu l'autorisation de la personne représentée dans la photo. Dans le sens inverse, un auteur peut interdire à l'acheteur d'un portrait de commande de l'exploiter pour des expositions au public. En revanche, les deux droits peuvent coexister pacifiquement lorsque l'un des titulaires des droits (droit d'auteur ou droit à l'image) obtient l'autorisation de l'autre.

C'est ainsi que nous allons examiner deux situations. La première concerne la coexistence du droit à l'image et du droit d'auteur (I). La deuxième situation concerne le conflit potentiel entre les deux droits (II).

I. La coexistence de deux droits

La coexistence de ces deux droits est possible dans deux cas. Le premier cas concerne la situation du titulaire du droit à l'image qui consent librement et expressément à l'exploitation de son image par l'auteur (A). Le deuxième cas vise le consentement de l'auteur pour l'exploitation de son œuvre par le titulaire du droit à l'image (B).

[8] Notre définition s'inspire du dictionnaire Larousse, édition 2012 qui définit l'image comme la représentation ou reproduction d'un objet ou d'une figure dans les arts graphiques et plastiques…

[9] Cette limite est une exception sui generis au droit d'auteur qui est différente de celles en vigueur dans la convention de Berne de 1886. Les articles 10 et 10bis de cette convention prévoient des limitations au droit d'auteur pour l'illustration dans l'enseignement et les informations d'actualité. La protection de l'image n'est pas concernée par ces limitations.

[10] On la retrouve dans les cinq lois suivantes : Loi de la République du Congo de 1982 (art.43); Loi du Gabon sur le droit d'auteur de 1987 (art.18); LOI de la Cote d'Ivoire n° 2016-555 du 26juillet 2016 (art.42); loi du Burkina-Faso de 1999 (art.29); Loi de la RDC de 1986 (art,23.b).

[11] L'article 258 du Code Civil Congolais Livre III sur les obligations dispose que tout fait quelconque de l'homme qui cause dommage à autrui oblige celui par la faute duquel il est arrivé à le réparer.

A. L'exploitation du droit d'auteur avec le consentement du titulaire du droit à l'image

Une personne physique qui passe commande d'un portrait, peut par la suite, autoriser le peintre ou le dessinateur de ce portrait à l'exploiter, par exemple, sous forme de reproduction en cartes postales. Dans ce cas, l'image de la personne concernée sera exploitée en public ou sur les lieux publics[12]. Aussi, une photo, prise avec le consentement du titulaire du droit à l'image, peut être exploitée dans un calendrier, dans les cartes postales et diffusée en public. Cela est conforme à l'article 23.b de la loi de la République Démocratique du Congo qui exige que l'auteur d'une œuvre visuelle requière l'autorisation de la personne représentée dans l'œuvre. Cependant, la situation peut devenir compliquée en cas des photographies des groupes des personnes se trouvant sur les lieux publics. Faudrait-il obtenir leur autorisation pour la prise de ces photos et pour leur diffusion ? En République Démocratique du Congo, il n'existe pas encore des décisions de justice sur ce cas.

Mais en France, Les avis sont partagés sur ce genre des photos. Une première opinion estime que les personnes se trouvant sur un lieu public s'exposent volontairement à la curiosité du public, donnant en quelque sorte une autorisation tacite à la diffusion de leur image[13].

Mais, une opinion divergente constante tend à affirmer que « le seul fait de se trouver dans un lieu public tel une rue, même une station fréquentée par des personnalités, ne peut valoir autorisation de reproduction de son image »[14]. Or, la loi de la loi de la République Démocratique du Congo sur le droit d'auteur est lacunaire sur cette question. D'où la nécessité d'enrichir cette loi pour encadrer la situation des photographies des groupes des personnes sur les lieux publics. Le consentement ne doit pas être nécessairement écrit. Mais il doit être spécial. L'autorisation donnée pour la prise de vue ne vaut pas nécessairement pour sa publication[15].

Le bénéficiaire du portrait ou de la photographie peut tolérer tacitement que son image soit communiquée au public lorsque cette communication est licite. Il peut s'agir d'un homme politique célèbre ou d'un artiste, qui ne trouve aucun inconvénient à ce que ses photos ou ses portraits soient largement diffusés en public. Cette large diffusion est souvent profitable aux hommes politiques et aux artistes célèbres même s'ils peuvent aussi tirer un profit économique dans l'exploitation publicitaire de leur image.

Ces diffusions sont licites lorsqu'elles se déroulent dans le cadre d'une information d'actualités. Il s'agit d'une exception légale prescrite à l'article 32 de la loi de la République Démocratique du Congo sur le droit d'auteur[16]. En effet, le droit à

[12] Un lieu public dont l'accès est libre et non soumis au consentement de la personne qui occupe ce lieu.
[13] CA Versailles, 31 janvier 2002, Juris-Data 2002-216790 cité par Thomas Livenais, Image et Droit pénal, mémoire de Master II, Droit des Affaires, Université de Toulouse I Capitole, Année académique, 2009-2010, p.25. N°64.
[14] TGI Nanterre, 20 mars 2009, Légipresse 2009, I, p56, cité par Thomas Livenais, op.cit p.26. N°67.
[15] Thomas Livenais, Idem, p.26, N°67.

[16] Cet article 32 dispose : « La presse écrite ou parlée peut reproduire un article publié dans un journal ou une revue, à la condition d'en indiquer la source, le titre et le nom de l'auteur, à moins que cet article ou le périodique dans lequel il est publié ne porte la mention que la reproduction en est interdite. Les nouvelles du jour et les faits divers qui ont caractère de simples informations de presse pourront être librement utilisées ». Cela signifie simplement que les journalistes qui publient les photos sans accord des personnes y représentées sont couverts par cette disposition légale.

l'information protégé par la Constitution de la République Démocratique du Congo[17], justifie, à nos jours, l'illustration photographique des faits reportés. Ce droit peut aussi entrer en conflit avec le droit à l'image lorsque la personne représentée par l'image estime que le reporter ou le journaliste devait recueillir son autorisation préalable.

Ce problème se pose lorsque la photographie porte atteinte à la personne y représentée. Une certaine doctrine estime que le photographe, qui n'a pas obtenu l'accord explicite de la victime, peut être poursuivi en justice lorsque cette atteinte à la dignité de la victime est intolérable[18]. Mais, il s'agit d'une précision pour éviter des actions judiciaires intempestives contre les photographes pour les vues prises dans les groupes des personnes sur les lieux publics. D'où l'intérêt de circonscrire la notion du consentement tacite dont la preuve peut poser problème.

La preuve du consentement tacite est difficile à établir lorsque le droit à l'image est menacé. Il n'existe aucune disposition légale en République Démocratique du Congo qui justifie un tel consentement tacite. Nous pourrons évoquer simplement l'adage « qui ne dit mot consent ». Or, cet adage ne présente aucune sécurité juridique susceptible de protéger l'auteur d'une photo des groupes des personnes sur les lieux publics. La solution pour couvrir le photographe, c'est de recourir à l'exception des événements d'actualités. Dans ce cas, la publication de la photo doit correspondre à une date proche de la prise de vue (un ou deux jours). Mais lorsque la photo est publiée plusieurs mois après, elle perd l'actualité[19]. En résumé, cette question du consentement du titulaire du droit à l'image limite l'exercice du droit d'auteur s'il n'est pas circonscrit par des conditions strictes.

En effet, l'atteinte au droit à l'image ne peut être réprimée que si cette atteinte est intolérable[20]. C'est le cas par exemple, lorsque la dignité ou la vie privée de la personne représentée dans la photo ou dans le portrait est menacée. Mais une autorisation généralisée pour l'exercice du droit d'auteur nous parait exagérée. En plus, les atteintes au droit à l'image relèvent plus du droit commun de la responsabilité tandis que le droit d'auteur est une question spéciale. D'où l'intérêt de privilégier la loi spéciale par rapport à la loi générale. Donc, l'autorisation du titulaire du droit à l'image n'a pas de place dans la loi sur le droit d'auteur.

B. L'exploitation d'une photo ou d'un portrait avec le consentement de l'auteur.

L'auteur d'une œuvre de l'esprit jouit, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous[21]. Cela signifie que l'objet corporel (photo ou portrait de commande) qui porte l'image de la personne qui l'a commandé ne peut pas être exploité en public sans l'accord de l'auteur. Donc, pour éviter tout conflit, le propriétaire

Dans ce cas, ils n'auront pas besoin de l'autorisation des titulaires du droit à l'image.

[17] Article 24 de la Constitution de la RDC du 18 février 1986,

[18] Thomas Livenais, Image et Droit pénal, mémoire de Master II, Droit des Affaires, Université de Toulouse I Capitole, Année académique, 2009-2010, p.21. N°54.

[19] Par exemple, il n'est pas possible de publier une photographie représentant deux personnes participant à une manifestation de soutien prise dix mois auparavant. En revanche, a été jugée licite la photographie reproduisant les traits de personnes manifestant contre le PACS et illustrant un article paru quelques jours après. Thomas Livenais, op.cit, p.27, N°69.

[20] Cependant, pour être protégée, l'image doit être individualisée, permanente, reconnaissable et requérir l'autorisation de la personne représentée. Marc Lesgour, le droit à l'image, 2eme Ed. Larcier, p.140.

[21] Article 1 de l'ordonnance-loi N°86-033 du 05 avril 1986 portant protection du droit d'auteur et des droits voisins en République Démocratique du Congo.

de l'objet matériel, doit demander l'autorisation de l'auteur avant de l'exploiter en public pour une reproduction ou une édition en plusieurs exemplaires. Si le titulaire du droit à l'image ne le fait pas, il commet une contrefaçon et s'expose à des sanctions civiles ou pénales même si c'est son image qui est représentée dans l'œuvre. En effet, le droit de propriété incorporelle est indépendant du droit de propriété corporelle sur le support de l'œuvre.

En République Démocratique du Congo, La nécessité d'obtenir l'autorisation des auteurs des portraits s'est manifesté dans un cas pratique dans la ville de Lubumbashi. En effet, dans cette ville, un prêtre belge, Léon Verbeek, agé de plus de 90 ans, avait acheté auprès des personnes physiques des portraits de commande et des photos puisque ces personnes devaient quitter la ville de Lubumbashi en 1993 précipitamment à cause d'un conflit communautaire entre kasaiens et katangais. Se sentant épuisé par l'âge, Père Léon Verbeek a décidé de céder ces objets au musée de Lubumbashi en 2023 mais il n'avait que l'accord des propriétaires des portraits et non celui des auteurs. Pour résoudre ce problème, l'association Waza Asbl qui fait la promotion de cette collection, a proposé de contacter le président de l'association des peintres de Lubumbashi pour identifier les auteurs ou leurs héritiers en vue d'obtenir leur autorisation.

Waza Asbl a aussi proposé une autre solution préventive : celle d'obtenir une autorisation globale de l'organisme national de gestion collective du droit d'auteur de la République Démocratique du Congo au nom des auteurs pour éviter tout conflit potentiel sur ces œuvres, même si certaines n'étaient pas signées par leurs auteurs (œuvres anonymes)[22]. Cette affaire Léon Verbeek démontre clairement combien le consentement de l'auteur est obligatoire même si les propriétaires des portraits de commande et des photographies avaient déjà donné leur accord. Ce consentement de l'auteur permet de créer une coexistence pacifique entre le droit d'auteur et le droit à l'image. Sinon, c'est la porte ouverte vers un conflit entre les deux droits.

II. Le confit potentiel entre les deux droits

Nous examinons d'une part le conflit lié à la primauté du droit à l'image (A) et d'autre part le conflit lié à la primauté du droit d'auteur (B).

A. La primauté du droit à l'image

Le droit de l'auteur d'un portrait ou d'une photo peut être paralysé par l'absence de l'autorisation de la personne représentée dans le portrait ou la photo. C'est le problème de la primauté du droit à l'image sur le droit d'auteur qui se pose. Est-ce qu'un auteur peut ignorer l'autorisation du titulaire du droit à l'image et publier ou diffuser des portraits ou des photos? En droit positif congolais, l'auteur est lié par l'autorisation du titulaire du droit à l'image conformément à l'article 23.b de la loi sur le droit d'auteur de 1986. Donc, sans autorisation du titulaire du droit à l'image, l'auteur peut être bloqué dans l'exercice de son droit.

En effet, l'expression artistique de la photographie ne peut justifier l'atteinte au droit à la vie privée qu'elle comporte. Le droit d'un artiste de faire connaitre son œuvre n'est pas absolu et ne saurait comprendre le droit

[22] Ce dossier est géré actuellement par l'association culturelle Waza Abl de Lubumbashi, qui a organisé un atelier à Lubumbashi, du 05 au 09 janvier 2023, pour régler ces différentes questions de cession des droits avec Père Léon Verbeeck, l'association des auteurs peintres et le musée de Lubumbashi.

de porter atteinte sans justification aucune, à un droit fondamental du sujet dont l'œuvre dévoile l'image[23]. Or, il arrive des situations pour lesquelles l'autorisation du titulaire du droit à l'image est difficile à obtenir pour plusieurs raisons : les personnes introuvables ou décédées, inconnues ou anonymes dans la photo…Comment contourner cette difficulté?

Si la photo a été prise dans le cadre d'un reportage, sa publication simultanée peut se justifier par l'exception des informations d'actualités[24]. Mais en dehors de cette hypothèse, la question qui se pose est celle de savoir si l'auteur du portrait peut se couvrir derrière l'exception de la caricature ou encore sur les photos générales des groupes. En droit positif congolais, l'exception de la caricature n'existe pas dans la loi de 1986 sur le droit d'auteur. Par conséquent, le titulaire du droit à l'image peut valablement poursuivre l'auteur pour atteinte au droit à l'image. Et pourtant, dans les autres États africains, cette exception existe déjà dans les lois et met à l'abri l'auteur contre toute poursuite judiciaire[25]. En plus, la loi de la République Démocratique du Congo ne fixe aucune règle susceptible de couvrir l'auteur pour les photos des groupes prises sur les lieux publics. Quelles seraient les solutions idoines pour limiter la responsabilité du photographe ou de l'auteur du portrait contre le titulaire du droit à l'image? Cinq solutions peuvent aider à limiter la responsabilité de l'auteur contre toute poursuite judiciaire.

La première solution, c'est d'instituer l'exception de caricature ou de parodie pour couvrir l'auteur contre toute poursuite judicaire. Le principe constitutionnel de la liberté d'expression[26] pourrait ainsi justifier une telle exception dans la loi sur le droit d'auteur. En effet, la liberté d'expression ne peut être remise en cause par le droit à l'image qui n'est pas constitutionnel. En vertu du principe de la hiérarchie des normes, le droit à l'image ne peut affronter la liberté d'expression qu'en cas d'atteinte à l'ordre public ou aux bonnes mœurs (le respect de la vie privée ou de la dignité humaine).

Une deuxième solution, c'est de supprimer simplement l'incise de l'article 23.b de la loi congolaise sur le droit d'auteur relatif au respect par l'auteur du droit à l'image puisque cette question est déjà réglée par le droit commun de la responsabilité civile qui oblige toute personne fautive à réparer le dommage qu'il cause à autrui[27]. Le droit à l'image ne peut pas dominer le droit d'auteur au nom du principe de la liberté d'expression.

La troisième solution, c'est de limiter strictement la durée pour l'exercice de l'action judiciaire du titulaire du droit à l'image dans les lois de procédure civile ou pénale. Ainsi, le législateur national pourra instituer un délai de prescription très court (cinq ans par exemple) pour l'exercice de l'action contre les atteintes au droit à l'image. Une telle prescription ne concernerait pas le droit à

[23] Marc Isgour, *Droit à l'image et création artistique*, Etudes Théatrales, p. 52 à 64, L'Harmattan, 2015.

[24] Article 26 de l'ordonnance-loi N°86-033 du 05 avril 1986 portant protection du droit d'auteur et des droits voisins en République Démocratique du Congo

[25] Art. 43. de la loi du Sénégal de 2008 dispose : « l'auteur ne peut interdire la reproduction ou la communication de l'œuvre à titre de parodie, compte tenu des lois du genre. Cette disposition légale du Sénégal n'émet aucune limite quant au droit à l'image. Ainsi, nous pouvons conclure qu'aucune restriction légale n'existe quant à ce droit à l'image.

[26] La liberté d'expression, en RDC, est protégée par l'article 23 de la Constitution qui dispose : « toute personne a droit à la liberté d'expression. Ce droit implique la liberté d'exprimer ses opinions ou ses convictions, notamment par la parole, l'écrit et l'image, sous réserve du respect de la loi, de l'ordre public et de bonnes mœurs.

[27] Article 258 du Code Civil livre III de la République Démocratique du Congo sur la responsabilité civile.

l'image, droit de personnalité imprescriptible[28], mais plutôt l'exercice de l'action judiciaire.

Cette solution de la réduction du délai de prescription de l'action judiciaire existe déjà dans le Code du travail de la République Démocratique du Congo. Par exemple, en matière du travail, le délai de prescription de l'action judiciaire est de trois ans[29] à compter de la réalisation de la faute (licenciement abusif ou révocation). La finalité, c'est d'éviter de créer une insécurité juridique permanente contre l'employeur. C'est un moyen de protéger l'employeur contre des actions judiciaires intempestives permanentes. La même logique peut prévaloir contre le titulaire du droit à l'image. Il ne peut pas conserver cette possibilité judicaire, de manière permanente, au risque de paralyser, à tout moment, le droit de l'auteur ou le droit à l'information.

La quatrième solution, c'est de règlementer des photos des groupes prises sur les lieux publics. En effet, selon une certaine opinion, des photos des groupes des personnes sur les lieux publics peuvent être publiées librement sauf si la personne représentée a été cadrée individuellement. Dans ce cas, l'auteur aura besoin de son autorisation avant de publier la photo. En plus, les prises des vues doivent être générales et non cadrées[30]. Ainsi, lorsqu'une personne est identifiable dans un groupe, il n'y aura pas atteinte. Mais, lorsque l'image de la personne victime est ciblée et cadrée, son autorisation sera requise. Sinon, on risque de tomber dans une atteinte au droit à l'image.

La réglementation stricte des photos prises sur les lieux publics peut valablement se justifier dans le système juridique congolais puisqu'elle prend en compte l'équilibre entre le droit à l'image et le droit à l'information. Or, le droit à l'information étant constitutionnel, il prime sur le droit à l'image. Par conséquent, l'autorisation du titulaire de ce droit à l'image ne peut valoir que lorsque l'auteur de la photographie du groupe des personnes est allé au-delà du droit à l'information, soit en causant une atteinte intolérable à l'auteur de l'image ou en publiant la photographie après que l'information ait perdu son actualité.

La cinquième solution est de s'inspirer de la loi du Cameroun de 2000 qui prévoit un transfert des droits patrimoniaux au profit de la personne qui a commandé l'œuvre sauf s'il y a une stipulation contractuelle contraire[31]. Ainsi, si l'auteur veut réserver ses droits patrimoniaux, il le manifestera dans le contrat avec le commanditaire; à défaut il y aura un transfert automatique des droits patrimoniaux au profit du commanditaire. En d'autres termes, en l'absence d'une stipulation contractuelle contraire, le propriétaire d'un

[28] S'agissant de la durée du droit à l'image, Thomas Livenais estime ce droit peut s'éteindre au décès de la personne victime de l'atteinte. Cependant, l'héritier pourra tout de même s'opposer à la reproduction de l'image du défunt, mais à condition de subir un préjudice personnel, déduit le cas échéant d'une atteinte à la mémoire et au respect dû aux morts. Livenais. Thomas, « Image et droit pénal », Mémoire de Master II, Droit des Affaires, Université de Toulouse I Capitole, Année académique, 2009-2010, p.27, N°68.

[29] Article 317 de la Loi N°015/2002 du 16 octobre 2002 portant Code du Travail en république Démocratique du Congo, *Journal officiel*, Numéro spécial du 25 octobre 2002.

[30] Idem, p. 25.

[31] L'article 12. 1 de la Loi du Cameroun n° 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins dispose : « Dans le cas d'une œuvre de commande, l'auteur est le premier titulaire du droit d'auteur. Toutefois, sauf disposition contractuelle, les droits patrimoniaux sur ladite œuvre sont considérés comme transférés au commanditaire qui les exerce dans les limites convenues ».

portrait de commande pourra devenir titulaire des droits patrimoniaux de l'auteur. C'est une règle efficace pour résoudre ce conflit entre l'auteur et le bénéficiaire d'un portrait de commande. Cette solution camerounaise, pourtant salutaire, entre en contradiction avec l'article 1.3 de la loi de la République Démocratique du Congo de 1986 sur le droit d'auteur qui permet à l'auteur de conserver son droit, même en présence d'un contrat de louage d'ouvrage ou de services [32]. En effet, cette disposition légale de la République Démocratique du Congo crée un risque de conflit entre l'auteur et la personne qui passe la commande d'un portrait par exemple. L'auteur peut le poursuivre en cas d'exploitation non autorisée du portrait.

Le législateur de la République Démocratique du Congo peut s'inspirer de cette solution du Cameroun qui prévoit, dans un contrat de commande, un transfert automatique des droits patrimoniaux au profit du commanditaire sauf stipulation contractuelle contraire. Cela peut contribuer à supprimer, en partie, le risque de conflit entre le droit d'auteur et le droit à l'image.

Malgré ces pistes des solutions, le conflit lié à la primauté du droit d'auteur peut persister.

B. La primauté du droit d'auteur

Ce conflit concerne les situations pour lesquelles le titulaire du droit à l'image ou ses ayants droit n'ont obtenu aucun consentement de l'auteur avant d'exploiter l'œuvre en public. Cela est possible pendant la durée de protection des œuvres. En principe, le titulaire du droit à l'image doit obtenir l'autorisation écrite de l'auteur conformément à l'article 34 de l'ordonnance-loi 1986 portant protection du droit d'auteur en République Démocratique du Congo. Sinon, le titulaire du droit à l'image tombe dans la contrefaçon.

Pour ce qui concerne l'exploitation des œuvres visuelles pendant leur durée de protection, la loi a consacré deux durées de protection différentes selon les catégories des œuvres.

Pour les œuvres photographiques, la durée de protection est de 25 ans[33]. Elle commence à courir à partir de la première année qui suit celle de la publication de l'œuvre. Dans ce cas, le conflit potentiel entre le titulaire du droit à l'image n'est possible que pendant cette durée de 25 ans. A son expiration, le risque de conflit disparait puisque le monopole de l'auteur cesse. Cependant, le droit à l'image, étant perpétuel, il persiste après l'expiration de la durée du droit patrimonial de l'auteur sur une œuvre photographique. Le droit à l'image est valide jusqu'au décès de la personne représentée dans l'image.

Cette courte durée de protection des œuvres photographiques défavorise leur auteur qui ne pourra plus prétendre à un droit exclusif et opposable à tous sur ses œuvres photographiques. Par conséquent, il est souhaitable que le législateur national rallonge cette durée de protection en l'alignant au minimum de 50 ans tel que prescrit par le traité de l'OMPI sur le droit d'auteur de 1996[34].

[32] Article 1.3 de la loi de la République Démocratique du Congo de 1986 sur le droit d'auteur dispose : « L'existence ou la conclusion d'un contrat de louage d'ouvrage ou de service par l'auteur d'une œuvre de l'esprit n'emporte aucune restriction à la jouissance du droit moral et patrimonial reconnu à l'auteur à l'alinéa premier du présent article ».

[33] Article 77 de la loi de la République Démocratique du Congo de1986 sur le droit d'auteur et les droits voisins.

[34] Article 9 du Traité de l'Organisation Mondiale de la Propriété Intellectuelle de décembre 1996 qui supprime l'article 7.4 de la convention de Berne. En effet, l'article 7.4 de la convention de berne de 1886

En revanche, pour les œuvres graphiques et plastiques, la durée de protection est de 50 ans. Elle commence à courir à partir de l'année du décès de l'auteur. Dans cas, si le titulaire du droit à l'image publie un portrait sans l'accord de l'auteur, le risque de conflit entre les deux parties peut perdurer pendant longtemps.

Après l'expiration de la durée de protection, le risque de conflit entre l'auteur et le titulaire du droit à l'image disparait puisque l'œuvre tombe dans le domaine public dont l'exploitation est libre. Le titulaire du droit à l'image devient alors le seul acteur sur le terrain. Le titulaire du droit à l'image ou ses héritiers seront les seuls acteurs disposant d'un droit personnel sur l'œuvre : le droit à l'image.

Cependant, le conflit peut aussi surgir lorsque le titulaire du droit à l'image, pendant la durée de protection de l'œuvre, refuse de mettre à la disposition de l'auteur, l'objet matériel qui contient ou qui soutient l'œuvre pour une exploitation du droit d'auteur. C'est le cas lorsque le bénéficiaire ou l'héritier d'un portrait de commande refuse de le remettre à l'auteur pour une reproduction ou une exposition au public. La loi de la République Démocratique du Congo de 1986 n'offre pas de solution pour résoudre ce conflit.

La solution peut aussi venir du droit comparé avec la loi du droit d'auteur du Sénégal de 2008 qui propose, en son article 4.4 que le titulaire du droit d'auteur puisse être autorisé par le tribunal, aux conditions que celui-ci détermine, à accéder à l'objet matériel dans la mesure nécessaire à l'exercice de ses droits. En d'autres termes, nous pouvons affirmer que le titulaire du droit à l'image ne peut pas paralyser l'exercice du droit d'auteur. L'auteur peut récupérer l'objet matériel, par la voie judiciaire, en vue d'exploiter son droit d'auteur (par exemple pour une reproduction ou une exposition pour le public) à condition qu'il restitue l'objet matériel à son propriétaire et qu'il ne cause pas une atteinte intolérable à la dignité et à la vie privée du titulaire du droit à l'image. Donc, le législateur congolais peut, dans le cadre de la réforme de sa loi nationale, adopter cette solution sénégalaise pour régler ce conflit potentiel pour consacrer la primauté du droit d'auteur.

Conclusion

L'analyse de l'article 23.b de l'ordonnance-loi N°86-033 du 05 avril 1986 portant protection du droit d'auteur et des droits voisins en République Démocratique du Congo démontre que c'est une disposition légale rare et inefficace qui risque de gêner l'exercice du droit d'auteur pour les œuvres visuelles en République Démocratique du Congo. L'auteur d'une œuvre visuelle peut l'exploiter librement au nom de la liberté d'expression qui est un principe constitutionnel en République Démocratique du Congo. La loi sur le droit d'auteur est une loi spéciale qui n'a pas vocation à régler les questions générales de responsabilité. Par conséquent, nous proposons que cette disposition légale (article 23.b) soit supprimée de la loi en vigueur sur le droit d'auteur en République Démocratique du Congo.

Enfin, le législateur de la République Démocratique du Congo peut s'inspirer de la loi du Cameroun qui prévoit que dans un contrat de commande, un transfert

avait créé une discrimination contre les œuvres photographiques à leur accordant une durée de protection de 25 ans pendant que les autres œuvres s bénéficiaient d'une durée de cinquante années à dater du décès de l'auteur (art. 7.1 de la convention de Berne).

automatique des droits patrimoniaux au profit du commanditaire sauf stipulation contractuelle contraire. Cela peut contribuer à supprimer, en partie, le risque de conflit entre le droit d'auteur et le droit à l'image. Dans ces conditions, le conflit est résolu par la stipulation contractuelle qui peut réserver les droits patrimoniaux à l'auteur. Sinon, C'est le bénéficiaire du portrait de commande qui acquiert automatiquement les droits patrimoniaux par l'effet de la loi.

T.N.N

Fiche pays : Côte d'Ivoire

Par Firmin Kouadio
Juriste-écrivain
Secrétaire éditorial de la RSPIA

I. INSTITUTIONS DE LA PROPRIETE INTELLECTUELLE EN COTE D'IVOIRE

Pour la propriété industrielle : OIPI

- Année de création : *2005*
- Texte institutionnel (originel) : *Décret n°2005-112 du 24 février 2005 portant création, organisation et fonctionnement d'un établissement public à caractère administratif Office ivoirien de la Propriété intellectuelle*
- Texte institutionnel révisé (en vigueur) : *Décret n°2015-241 du 8 avril 2015 déterminant les attributions, l'organisation et le fonctionnement de l'Office ivoirien de la Propriété intellectuelle, publié au JORCI du 29 juin 2015*
- Siège et adresse : Abidjan, Rue des Jardins – Ilot 204 – Quartier II Plateaux (Email: info@oipi.ci / oipi@aviso.ci)
- Statut : *Structure Nationale de Liaison (SNL), EPA*
- Mission : *cf. art. 4 du Décret n°2015-112 du 24 février 2015 [En général, il réceptionne et transmet les demandes de dépôt de titres de propriété intellectuelle à l'OAPI en vue de leur délivrance.]*
- Directeur Général (actuel) : *Dr Paul Koffi ASSANDE*
- Directeur Général (précédent, 2017-2022) : *Dr Jacques Roger Claude EKRA*

Pour la propriété littéraire et artistique : BURIDA

- Année de création : 1981
- Texte institutionnel (originel) : *Décret n°81-232 du 15 avril 1981 fixant les attributions, l'organisation et le fonctionnement du Bureau Ivoirien du Droit d'Auteur*
- Texte institutionnel (en vigueur) : *Décret n°2015-271 du 22 avril 2015 fixant les attributions, l'organisation et le fonctionnement du Bureau Ivoirien du Droit d'Auteur*
- Siège et adresse : Abidjan, II Plateaux-Vallon, Cocody – BP V 258 Abidjan (Email : info@buridaci.com)
- Statut : Organisme de Gestion Collective (OGC), Société civile de type particulier, placé sous la tutelle du Ministère de la Culture et de la Francophonie
- Mission : *cf. art. 7 du Décret n°2015-271 du 22 avril 2015 [En général, il se charge de collecter et reverser les redevances au titre de l'exploitation des œuvres.]*
- Directeur Général (actuel, décret n°2020-103 du 15 janvier 2020) : M. Karim OUATTARA
- Directeur Général (le tout premier, en 1981) : M. Serge RAIFF
- Directeur des affaires juridiques (actuel) : M. Jean-Claude KOUADIO

➢ **Autres structures** : *Autorité de Régulation des Télécommunications en Côte d'Ivoire* (*ARTCI*), ayant pour mission la gestion des noms de domaines et des adresses internet [email : courrier@artci.ci) ; *Comité National de Lutte contre la Contrefaçon* (*CNLC*), ayant pour mission de centraliser la lutte contre la contrefaçon, en synergie avec la douane et la police notamment [email : contact@cnlc-ci.info).

II. TEXTES DE LOI ADOPTES DEPUIS L'INDEPENDANCE

Rappel de textes applicables avant l'indépendance :

- **En propriété industrielle** : loi du 5 juillet 1844 pour les brevets d'invention, modifiée par celles des 31 mai 1856 et 7 avril 1902 ; loi du 23 juin 1857 sur les marques de fabrique et de commerce ; loi du 14 juillet 1909 sur les dessins et modèles
- **En propriété littéraire et artistique** : loi n°57-298 du 11 mars 1957 sur la propriété littéraire et artistique

Le Code pénal de 2019 et la propriété intellectuelle :

- Contrefaçons en matière commerciale : art. 343
- Concurrence déloyale : art. 344-345
- Abrogation des dispositions (art. 346 à 349) relatives à la propriété littéraire et artistique par l'art. 8 de la loi n°2021-893

du 21 décembre 2021 modifiant la loi n°2019-574 du 26 juin 2019 portant Code pénal

➢ **Texte actuellement applicable en matière de propriété industrielle** : L'Acte de Bamako du 14 décembre 2015, nouvel Accord de Bangui, entré en vigueur depuis le 14 novembre 2020, deux mois après le dépôt des instruments de ratification par deux tiers des Etats signataires.

➢ **Textes adoptés en matière de propriété littéraire et artistique :**

- Loi n°78-634 du 28 juillet 1978 portant protection des œuvres de l'esprit
- Loi n°87-806 du 28 juillet 1987 portant protection du patrimoine culturelle
- Loi n°96-564 du 25 juillet 1996 relative à la protection des œuvres de l'esprit et aux droits des auteurs, des artistes-interprètes et des producteurs de phonogrammes et vidéogrammes
- Loi n°2004-644 du 9 décembre 2004 portant régime juridique de la communication audiovisuelle
- Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité
- Loi n°2013-865 du 23 décembre 2013 relative à la lutte contre la contrefaçon et le piratage, et à la protection des droits de propriété intellectuelle dans les opérations d'importation, d'exportation et de commercialisation de biens et services
- Loi n°2016-555 du 26 juillet 2016 relative au droit d'auteur et aux droits voisins, publiée au JORCI n°84 du jeudi 20 octobre 2016 (texte en vigueur)

III. ADHESIONS, RATIFICATIONS DE TRAITES ET CONVENTIONS

- ***Convention de Paris du 20 mars 1883 pour la protection de la propriété industrielle, telle que révisée à Stockholm le 14 juillet 1967*** : dépôt d'instrument de ratification le 1er février 1974, entrée en vigueur le 4 mai 1974
- ***Convention de Berne du 9 septembre 1886 pour la protection des œuvres littéraires et artistiques, telle que révisée à Paris le 24 juillet 1971*** : dépôt d'instrument de ratification le 1er février 1974, entrée en vigueur le 4 mai 1974
- ***Traités administrés par l'OMPI*** : adhésion le 8 juillet 1961, en vigueur le 1er janvier 1962
- ***Accord de Libreville du 13 septembre 1962 portant création de l'Office Africain et Malgache de la Propriété Industrielle (OAMPI)*** : signé le 13 septembre 1962 par 12 Etats membres dont la Côte d'Ivoire
- ***Accord de Bangui du 2 mars 1977 portant création de l'OAPI, constituant révision de l'Accord de Libreville de 1962*** : ratifié par le 8 février 1982
- ***Accord de Bangui Révisé du 24 février 1999*** : ratifié par le moyen de l'Ordonnance n°2000-388 du 24 mai 2000, entré en vigueur le 28 février 2002
- ***Accord sur les ADPIC du 15 avril 1994*** : adhésion des Etats de l'OAPI par le biais de l'Accord signé à Genève le 22 décembre 1995
- ***Acte de Genève de l'Arrangement de Lisbonne sur les appellations d'origine et les indications géographiques*** : dépôt d'instrument d'adhésion le 28 septembre 2018 auprès du Directeur général de l'OMPI
- ***Acte de Bamako du 14 décembre 2015*** : dépôt d'instrument de ratification le 28 juin 2019 au Siège de l'OAPI auprès du Directeur général.

IV. ETAT DE LA DOCTRINE EN PROPRIETE INTELLECTUELLE

De plus en plus, on peut remarquer que la matière de la propriété intellectuelle intéresse tant les théoriciens que les praticiens ; à savoir les enseignants-chercheurs, les auteurs d'œuvres artistiques ou littéraires, les inventeurs, les propriétaires d'entreprises, les avocats, les magistrats... Ci-dessous quelques auteurs qui, à notre connaissance, s'intéressent à la matière :

- **Prof. OUATTARA Aboudramane :** Professeur titulaire, Avocat
  - *La preuve électronique : Etude de droit comparé Afrique, Europe, Canada*, Presses Universitaires d'Aix-Marseille, Collection Horizons Juridiques Jeunes Africaines, 2011, thèse, sous la direction du Prof ISSA-SAYEGH Joseph, Université de Cocody, 2003
  - « Données à caractère personnel et cybersécurité : des liaisons dangereuses », in *Enjeux du droit du numérique en Afrique*, table ronde du 24 septembre 2021
  - « Les mesures d'urgence dans la lutte contre la contrefaçon en droit d'auteur (blocage, etc.) », in *Colloque international sur le Droit de la propriété intellectuelle à l'heure du numérique* : les apports de l'Acte de Bamako, les 28 et 29 mars 2022 à Lomé

- **Prof. ALLA Koffi Etienne :** Agrégé des facultés de Droit, Avocat
  - *Subjectivisme et objectivisme dans le droit sur l'invention des médicaments*, thèse, sous la direction de Jacqueline Lohoues-Oble et de Jean-Marie Crouzatier, Toulouse 1, 2012
  - « L'équilibre des parties dans le contrat APA », in *Colloque international sur le thème Innovation, ressources biologiques et connaissances traditionnelles en Afrique de l'Ouest et centrale*, du 29 novembre 2019, à Yaoundé
  - *Droit de Propriété intellectuelle*, Abidjan, éd. ABC, 2021

- **Dr. BOHOUSSOU Dénis :** Enseignant-chercheur, Directeur Général de l'OAPI
  - *L'obligation de garantie dans les contrats relatifs à l'informatique*, thèse, sous la direction de Christian le Stanc, Montpellier 1, 1993
  - « L'Organisation Africaine de la Propriété intellectuelle et le protocole de Nagoya », in *Colloque international sur le thème Innovation, ressources biologiques et connaissances traditionnelles en Afrique de l'Ouest et centrale, du 29 novembre 2019, à Yaoundé*
  - « L'évolution de la législation de la propriété intellectuelle dans l'espace OAPI », intervention au CEIPI, le 31 mars 2022 dans le cadre du cycle de conférences « Droit comparé de la propriété intellectuelle »

- **Dr. ASSOKO Héraclès Mayé :** Enseignant-chercheur, Avocat
  - *La régulation de réseaux numériques par le contrat*, thèse, sous la direction de Jacques Larrieu, Toulouse 1, 2006
  - *Droit de Propriété intellectuelle*, Abidjan, éd. ABC, 2020

- **Dr. OUATTARA Simplice :** Mandataire agréé OAPI
  - *La contrefaçon de médicaments dans l'espace U.E.M.O.A.*, thèse, sous la direction de Stéphanie Carre, CEIPI, Université de Strasbourg, 2021

- **Dr. KPOLO Christian :** Enseignant-chercheur, Avocat
  - *Les présomptions en droit de la propriété intellectuelle, analyse à la lumière du droit commun*, thèse, sous la direction de Prof Patrick Tafforeau, Université de Loraine, 2019
  - Collaboration à l'ouvrage « *Droit de la propriété intellectuelle* » de Patrick TAFFOREAU, éd. Gualino, 2015
  - « L'élaboration de la norme juridique à partir des présomptions : exemple en droit de la propriété intellectuelle », in RRJ-2021

F.K.

ECHOS DE L'APIA

▪ LE BALAFON, *PODCAST DE L'APIA*

Dans l'élan de son ambition qui est de promouvoir la propriété intellectuelle en Afrique, l'APIA a franchi un pas en mettant en place un Podcast dédié : « Le Balafon ».

Le Balafon, Podcast de l'APIA est une lucarne d'échange et de réflexion vivante et interactive qui aborde tous les sujets relatifs à la propriété intellectuelle…et au-delà.

Du propre aveu de l'équipe éditoriale de cette œuvre de l'esprit à part entière, *« au fil des épisodes de ce podcast, les différents intervenants proposent une présentation synthétique et didactique d'un ou plusieurs sujets relatifs à la propriété intellectuelle afin d'en comprendre les contours, les enjeux et les éventuelles controverses ».*

La première saison s'est ouverte le 1er mars 2023 par un épisode intitulé « Plagiat, musique et droit d'auteur » dont l'invité n'est autre que Maitre Yvon Ngombé, Président de l'APIA.

Le ton était donné : aborder des sujets qui suscitent débats, voire controverses, dans un propos volontairement assumé mais qui admet la contradiction et la réflexion.

Le propos est assumé certes, mais bien plus, le format l'est tout autant. Chaque épisode du *Balafon* n'excède pas 15 minutes. L'idée étant de faire le tour de la question tout en envisageant que les débats se poursuivent lors des autres activités de l'APIA que sont entre autres *L'arbre à Palabre, La journée de la recherche scientifique* ou *La journée d'actualité jurisprudentielle.*

En fait de lucarne *Le Balafon* est un véritable terrain d'analyse subdivisée en plusieurs compartiments complémentaires. Ainsi, en plus des épisodes consacrés à la réflexion de sujets « évidents » sur le droit de la propriété intellectuelle et qui ont accueilli d'éminents spécialistes du domaine, *Le Balafon* consacre des épisodes à des sujets d'actualité mais également des épisodes à la présentation d'un sujet de thèse soutenu ainsi qu'un hors-série qui essaie de sortir du cadre.

C'est ainsi qu'au titre des sujets généraux, le podcast de Soel Ngaba, juriste et Conseil en propriété industrielle, qui a présenté successivement deux épisodes sur le précontentieux et le contentieux en matière de marque dans l'OAPI.

Les sujets d'actualité ont été présentés aux épisodes 7 et 8 respectivement par Jeanine Tano-Bian et Laurent Escriva.

Au jeu des souvenirs de soutenance de thèse, le podcast, dans ses épisodes intitulés ***Par(en)thèse***, a eu l'immense privilège de recevoir les docteurs Jeanine Tano-Bian et Théodore Nganzi Ndoni qui ont présenté leurs travaux et saisi l'occasion pour adresser de précieux conseils aux futurs impétrants.

Quant au Hors-Série, il a été consacré à quelques chapitres du livre *Rumbissimo : Rumba, Droit et Business* écrit par Yvon Laurier Ngombé.

Il y aurait tellement à dire sur les **12 épisodes** de cette première saison, mais la meilleure manière de le faire serait de laisser chaque lecture de la *RSPIA* se faire sa propre idée… en attendant la prochaine saison prévue en janvier 2024 ! Longue vie à *Le Balafon !!!*

Le Bureau de l'APIA

Le Balafon
Podcast de l'APIA
#1
Plagiat, musique et droit d'auteur
Invité
Maître Yvon Laurier Ngombé
Avocat au Barreau de Paris

Le Balafon
Podcast de l'APIA
#7
Rétrospective sur la célébration des 10 ans de la Loi ivoirienne sur la protection des données à caractère personnel
Invitée
Jeanine Tano-Bian
Docteure en droit - Consultante en cybersécurité
Enseignante-Chercheur à l'UFHB Abidjan

Le Balafon
Podcast de l'APIA
#5
La saisie-contrefaçon de marques OAPI
Invité
Soel Ngaba
Conseil en propriété industrielle OAPI

Le Balafon
Podcast de l'APIA
#8
Le consommateur moyen en droit de la publicité et en droit des marques
Invité
Laurent Escriva
Formateur

LE BALAFON
HORS - SÉRIE
RUMBISSIMO
RUM BISS IMO
RUMBA, DROIT ET BUSINESS
YVON L. NGOMBÉ
Chapitre 1 - Chez Faignon [Prélude]

Le Balafon
Podcast de l'APIA
Par(en)thèse #2
Le droit d'auteur à l'épreuve du numérique en droit comparé congolais, camerounais, ivoirien et sénégalais
Invité
Dr. Théodore Nganzi Ndoni

▪ LA 2E JOURNEE DE LA RECHERCHE SCIENTIFIQUE DE L'APIA

Invitées : Jeanine Tano-Bian, Andrée Glancia Madinda et Lynda Ngo Nkot

Pour sa deuxième journée de la recherche scientifique, l'APIA a tenu à inviter trois chercheures en Droit de la propriété intellectuelle et du numérique. Les femmes étant à l'honneur, cette journée leur a été consacrée. Deux doctorantes, Mesdames Ngo Kot et Madinda ainsi qu'une enseignante, Madame Tano-Bian ont respectivement présenté brièvement leurs travaux relatifs au Nom de domaine dans l'espace OAPI, au Contrat d'auteur dans l'espace OAPI et à la cybersécurité dans l'espace OHADA.

La modération de cette riche journée a été assurée par Maître Nilce Ekandzi, Docteur en droit et chercheur associé au CEIPI.

Les synthèses des interventions des trois conférencière paraitront prochainement dans le RSPIA.

Le Bureau de l'APIA

PANORAMA DE JURISPRUDENCE

Par Christian Kpolo, *Avocat*

Affaire Adjin Adimi c. Imprimerie Tropicale et autres, Tribunal de commerce de Cotonou, 26 décembre 2019, Jugement n° 154/2019/ CJ /SIII/TCC

Affaire Attouh, Cour d'appel de commerce d'Abidjan, RG N° 308/2018, 14 février 2019

Affaire Heden Golf Hôtel c. Uniwax, Tribunal de commerce Abidjan, 27 juin 2019, RG n° 263/2019, *inédit*

Affaire Safaricom PLC c. MultiChoice Kenya Limited et autres, Court of Appeal of Kenya at Nairobi, Civil Application n° E376 Civil of 2020, 19 mars 2021

Al Atheed General Trading LLC cColombina S.A, décision n° 007/22/OAPI/CSR, 18 mars 2022

Big Pictures Entertainment Limited, Adeyemi Adeuson et 27 autres c. Burida et MTN, Cour d'appel de commerce d'Abidjan, 12 janvier 2022, 4e ch., RG n° 768/2021

BURIDA c. *Gnacadja Nouyeton Sophie,* tribunal d'instance Abidjan, RG n° 707/2018, jugement civil n° 375 du 11 avril 2019

Cité Nazareth SARL c. M. Agomon Komlan, Tribunal de commerce de Lomé, 19 janvier 2022, n° 0043/2022

CSR, 17 juin 2022, n° 0039/22/OAPI/CSR, LEGENDS

CSR, 18 mars 2022, n° 007/22/OAPI/CSR, AMAZON + Logo

Dabé Zohora Bertin c. *La société Nouvelle Parfumerie Gandour*, Cour d'appel de commerce d'Abidjan, 1re ch., Côte d'Ivoire, arrêt no 28/2019 du 21 mars 2019

Ets AB PLAST c. Atikpohoun et Mahamadou, Tribunal de commerce de Lomé, 30 décembre 2020, n° 0687/2020

Ghandour Cosmetics Ltd c. El Paradis Cosmetics, décision n°0048/22/OAPI/CSR, 17 juin 2022

Lacoste SA c. Maxi Skf, décision *041/22/OAPI/CSR*, 17 juin 2022

Lords Healthcare Limited v Cipla Limited & another, High Court of Nairobi, Milimani Commercial Courts, 22 décembre 2022, Commercial Case 305 of 2015

Magdalena Lamwaka c. Mukono Bookshop Printing and publishing Co., High Court of Uganda, Civil Division, Civil Suit n° 326 of 2014, 25 février 2019

MASSOKHNA KANE et huit (8) autres c. *État du Sénégal*, Cour suprême, 13 juin 2019, arrêt n° 20

Mercy Munee Kingoo et Lydia Nyva Kingai c. *Safaricom Ltd. et Procureur général,* High Court of Kenya at Malindi, Constitutional Petition n° 5 of 2016, eKLR Report 2019

Mhg Ip Holding Pte Ltd c. directeur général de l'OAPI, décision n° 0038/22/0API/CSR, 17 juillet 2022

MultiChoice Africa Holding BV and SuperSport International (PTY) Limited c. Intelvision Limited,

Cour suprême des Seychelles, (CS 46/2020 [2021] SCSC 10 (7 avril 2021)

Nairobi Map Services Limited v. Airtel Network Kenya ans 2 others, 7th of June 2019, Cour of Appeal at Nairobi, Civil Appeal n° 125 of 2016

Natural Valley Ltd c/ Farily Bottling Ltd et Autres, Supreme Court of Zambia, Civil Jurisdiction, 13 January 2022, appeal n° 61/2016

ONG Action de Solidarité Islamique c. Pharmacie Nationale d'Approvisionnement et Imprimerie NOUROU PUB, Cour suprême du Sénégal le 18 avril 2016

Saic-Gm-Wuling Automobile Co. Ltd, LLC c. Deng Ming, Tribunal de commerce de Cotonou, Jgt. n° 105/22/CJ1/SII/TCC, 8 sept. 2022, RG BJ/e-TCC/2022/044

Sanitam Services (E.A.) Limited v. *Rentokil (K.) Limited Et Kentainers (K.) Limited*, High Court of Kenya at Nairobi (Milimani Law Courts – Commercial, Admirality & Tax Division), 25 avril 2019, Civil case no 338

SARL Application Agro-Industrielles Côte d'Ivoire c. SARL Castor, Cour d'appel de commerce Abidjan, 17 février 2022

Société DO MEDIA LIMITED c. Bureau Ivoirien du droit d'auteur dit BURIDA, Cour d'appel de commerce d'Abidjan, 4e ch., RG n° 883/2019 du 26 février 2020

Société Wm. Wrigley Jr c. Directeur Général de l'OAPI, CSR, OAPI, 7 septembre 2021

Société Xyleco inc. c. Directeur Général de l'OAPI, CSR, décision n° 00221/OAPI/CSR du 28 avril 2017

Suzhou Dake Machinery c. Total SA, décision n° 0051/22/0API/CSR, 17 juillet 2022

The Gb Foods Africa Holding Company, Slu SA c. Sté Xino SARL et a., Tribunal de commerce de Cotonou, 10 novembre 2022

Questions de compétence relatives aux litiges portant sur la propriété de la marque

A propos de l'affaire « *Elsafeer Falcon Pack Egypt Industries c/ Falcon Pack et al.* »

Par Yasser OMAR AMINE
Avocat au barreau du Caire
Docteur en droit
Chercheur associé au CECOJI-UP (EA 7353) - Université de Poitiers
Formateur agréé par l'OMPI

Dans cette affaire importante, la chambre civile et commerciale de la Cour de cassation égyptienne a été amenée à se prononcer, dans un arrêt en date du 14 mars 2019[35], sur les questions de compétence relatives aux litiges portant sur la propriété de la marque. La question à laquelle devait répondre la Cour de cassation était de savoir quelle est la juridiction compétente pour connaître le contentieux mettant en jeu la validité ou la nullité d'une marque enregistrée ? Ces questions dépendent-elles de la compétence des juridictions de l'ordre judiciaire, en l'occurrence, des Cours économiques qui sont compétentes de façon exclusive pour connaître les affaires et les litiges relatifs à l'application du Code égyptien de la propriété intellectuelle[36] (ci-après « CPI égyptien ») depuis la promulgation de la loi n° 120 de 2008 portant création des Cours économiques (modifiée par la loi n° 146 de 2019)[37] ou bien relèvent-elles, au contraire, de la compétence des juridictions de l'ordre administratif du Conseil d'État ? En effet, la question posée est dans la pratique bien plus complexe qu'il n'y paraît au premier abord.

Rappelons les faits. En l'espèce, une société émiratie *Falcon Pack* est titulaire de la marque « Falcon » enregistrée dans plusieurs pays arabes pour désigner des produits relevant des classes 3, 5, 6, 16, 21 qui les commercialisent sur le marché égyptien par le biais de son agent *Al Safier Company For Import & Export S.A.E.* Après avoir constaté que cette dernière a changé sa dénomination sociale pour devenir *Elsafeer Falcon Pack Egypt Industries* et a procédé au dépôt frauduleux de trois marques intitulées « Falcon », en Arabe et en Anglais respectivement sous les n° 148270, 187217 et 187218, pour désigner des produits en classe 3, 16, 35, la société émiratie *Falcon Pack* qui faisait valoir une antériorité d'usage l'a assigné devant la Cour économique du Caire (aff. n° 510/6e A.J.), notamment en nullité et en radiation des deux marques enregistrées de mauvaise foi sous les n° 148270 et 187217.

Or, la chambre d'appel de la Cour économique du Caire, par un arrêt du 16 décembre 2014, s'était déclarée incompétente pour connaître du litige au profit du Tribunal du contentieux administratif au Conseil d'État au visa de l'article 82 du CPI

[35] Cass. ch. civ. et com., 14 mars 2019, pourvoi n° 2707/85e Année Judiciaire (ci-après « A.J. »). Il convient de noter qu'il existe d'autres affaires opposant les deux parties qui ont fait l'objet de pourvois devant la Cour de cassation : Cass. ch. civ. et com., 26 mars 2017, pourvoi n° 2726/85e A.J. ; Cass. ch. com. et éco., 13 févr. 2018, pourvoi n° 11414/85e A.J. ; Cass. com., 23 févr. 2020, pourvoi n° 4838/89e A.J.

[36] Promulgué par la loi n° 82 de 2002 sur la protection des droits de propriété intellectuelle (*JO* du 2 juin 2002, n° 22 *bis*).

[37] Art. 4 et 6 de la loi n° 146 de 2019.

égyptien qui prévoit la compétence du Tribunal du contentieux administratif pour examiner les recours formés à l'encontre des décisions de l'Office sur l'opposition, et ce, conformément aux procédures et aux délais prescrits par la loi du Conseil d'État.

C'est dans ces conditions qu'un pourvoi en cassation s'ensuit. Sur le moyen unique du pourvoi, la partie demanderesse faisait grief à l'arrêt attaqué d'avoir fondé sa décision sur l'article 82 qui permet de faire recours contre les décisions de l'Office portant enregistrement, annulation et radiation des marques devant le Tribunal du contentieux administratif compétent, alors que le litige en question n'impliquait pas l'État ou des autres personnes morales de droit public pour qu'il puisse être considéré comme un litige administratif mais le litige se cristallisait plutôt sur la propriété de la marque litigieuse, opposant la société émiratie *Falcon Pack* à la société égyptienne *Elsafeer Falcon Pack Egypt Industries*, qui relève par conséquent de la compétence des tribunaux ordinaires.

Par un arrêt du 14 mars 2019, la chambre civile et commerciale de la Cour de cassation accueille le pourvoi et casse l'arrêt de la Cour économique du Caire, pour violation de la loi et sa fausse application, au motif que l'action de la société émiratie était fondée sur sa propriété de la marque « Falcon » ainsi que sur la radiation de ladite marque enregistrée de mauvaise foi au nom de la société égyptienne dans la mesure où Falcon Pack bénéficiait d'une antériorité d'usage, de sorte que le litige portait ainsi sur la propriété de la marque qui relève de la compétence des tribunaux ordinaires à l'exclusion du Tribunal du contentieux administratif.

Pour déterminer le périmètre de la compétence exclusive du Tribunal du contentieux administratif, la Cour de cassation a pris soin, tout d'abord, de qualifier la nature de l'action en nullité. La Haute juridiction rappelle, qu'aux termes des articles 80, 81, et 82 du CPI égyptien relatifs à la procédure d'opposition, que la compétence impartie au Tribunal du contentieux administratif implique que le litige entre les parties porte soit sur leur précipitation conjointe pour enregistrer une marque, soit sur la contestation de l'une des questions relatives à la procédure d'enregistrement ou, dans la limite, soit sur le recours contre la décision de l'autorité portant acceptation ou refus d'enregistrement de la marque. Elle en a déduit, à bon droit, que le litige portant sur la propriété de la marque ou sur l'annulation de l'enregistrement au vu d'une antériorité d'usage relevait par conséquent de la compétence des tribunaux ordinaires au détriment de la juridiction administrative.

A vrai dire, il semble que l'arrêt attaqué de la Cour économique du Caire ait confondu entre la nature de l'action en nullité portant sur une marque qui n'est pas en réalité un recours contre la décision administrative et la procédure d'opposition à la décision portant délivrance du titre qui est de nature administrative. Si le Tribunal du contentieux administratif n'est compétent en la matière que pour connaître les affaires et les litiges relatifs à la procédure d'opposition prévues aux articles 80, 81 et 82 précités, y compris le recours contre la décision de l'autorité portant acceptation ou refus d'enregistrement de la marque, les juridictions ordinaires sont, en revanche, compétentes pour trancher les actions et demandes mettant en jeu la contrefaçon et la validité ou la nullité de marques. Il en résulte que la demande d'invalidation de l'enregistrement fondée sur

la mauvaise foi ou le non-usage de la marque[38] ne peut être intentée que devant un tribunal civil. Il est clair que le législateur ait entendu, par dérogation aux litiges et aux affaires qui relèvent de la compétence du Conseil d'État, faire relever de la compétence des tribunaux de l'ordre judiciaire toutes les contestations relatives à la propriété et à la nullité de la marque s'inscrivant dans le cadre de l'article 65 du CPI égyptien.

En matière de brevets, la Haute Cour administrative égyptienne, avait déjà clarifié la nature de l'action en nullité, dans un célèbre arrêt riche d'enseignements qui date du 14 mai 1966[39], aux termes duquel : « *L'action en nullité d'un brevet d'invention n'est pas en réalité un recours contre la décision administrative, qui l'a émis, mais elle porte sur le monopole d'exploitation assuré par la loi à son titulaire, et elle implique une contestation au sujet de l'existence ou de la propriété de l'invention,* entre le titulaire du brevet, et celui qui lui conteste ses droits à l'invention, ou qui nie son existence, et partant une telle action n'est soumise à aucun délai de recours en nullité, conformément à la loi du Conseil d'État. […] »[40]. Cette qualification qui est bel et bien transposable au droit des marques s'explique par le fait que c'est la marque elle-même qui est annulée, et partant, le monopole y attaché.

Enfin, il convient de rappeler que la solution de la Cour de cassation, au regard de l'affaire qui lui était soumise, s'inscrit résolument dans la lignée de sa jurisprudence bien établie. Dans son arrêt du 22 mars 2011[41], la Haute juridiction avait déjà eu l'occasion de se prononcer sur les règles de compétence en matière de marques notamment dans l'affaire opposant la société *Al Doha Company For Food Stuff* à la société *El Kawafel El Misria For Food Stuff Ltd. et al.* Dans ses conclusions déposées, le ministère public soulevait, en l'espèce, l'incompétence de la Cour économique saisi au profit du Tribunal du contentieux administratif. Or, la Cour de cassation, rejetant cette exception d'incompétence, relève qu'en dépit de la compétence du Tribunal du contentieux administratif pour connaître les litiges relatifs à la procédure d'opposition prévues aux articles 80, 81 et 82 précités, néanmoins les litiges portant sur la propriété de la marque ou l'annulation de son enregistrement fondée sur l'antériorité d'usage ne relèvent pas du champ de la compétence de la juridiction administrative mais ils relèvent, au contraire, de la compétence des tribunaux ordinaires.

En somme, l'intérêt de cette décision commentée est double, puisqu'elle se prononce, non seulement sur la qualification de l'action en nullité de marque, mais également sur la délimitation des compétences respectives du Tribunal du contentieux administratif et de la Cour économique en matière de marques dont les contours sont parfois un peu flous.

Y.O.A

---

[38] La radiation de l'enregistrement d'une marque pour non-usage doit faire l'objet d'une demande auprès du tribunal compétent (art. 91 du CPI égyptien).

[39] Recours n° 1582/7e A.J., inédit, aff. *Abdel Moneim Ibrahim Saleh*. V. Dans le même sens : Trib. Adm., 29 nov. 1966, Aff. *El Assas*, recours n° 117/18e A.J. (inédit).

[40] V. Y. OMAR AMINE, « De l'insécurité juridique induite par les incohérences pratiques de l'action en nullité des brevets d'invention en Égypte : une analyse comparatiste à la lumière du droit arabe de la propriété industrielle », *Revue Francophone de la Propriété Intellectuelle* (RFPI), sept. 2015, n° 1, p. 30.

[41] Cass. com., 22 mars 2011, pourvoi n° 6286/79e A.J. Il en va de même sous l'empire de l'ancienne loi n° 57 de 1939 sur les marques de fabrique et de commerce et les désignations industrielles et commerciales : Cass., 15 mars 1956, pourvoi n° 342/22e A.J., *Rec.*, année 7, p. 341.

Marques antérieures déposées	Marques déposées de manière frauduleuse

Marque – Propriété de la marque – Nullité – Juridiction compétente – Juridiction administrative (non) – Juridiction ordinaire (oui) – Cours économiques (oui)

▪ CYBERSECURITE ET E-SANTE

La responsabilité des prestataires d'infogérance des établissements de santé en cas de vulnérabilités informatiques : étude de droit français (1ère partie)

Par Christian Kpolo
Avocat au Barreau de Paris
Docteur en droit - Chercheur Associé
Université de Lorraine et Université d'Abidjan

Introduction

L'évolution rapide de la technologie dans le domaine de la santé a conduit les acteurs de santé, au nombre desquels se trouvent les établissements de santé[42], à externaliser la gestion de leurs infrastructures informatiques et de leurs données à des prestataires d'infogérance spécialisés. Cette externalisation offre de nombreux avantages, notamment une expertise technique accrue, une gestion plus efficace des systèmes et une réduction des coûts opérationnels. Cependant, cette collaboration avec des prestataires d'infogérance soulève des questions fondamentales concernant la responsabilité en cas de vulnérabilités informatiques.

Les vulnérabilités informatiques, telles que les cyberattaques, les fuites de données ou les défaillances techniques, peuvent entraîner des conséquences graves pour les établissements de santé[43]. Non seulement elles peuvent perturber les opérations médicales essentielles, mais elles peuvent également compromettre la confidentialité des dossiers médicaux des patients, leur intégrité et leur disponibilité.

Or, il s'agit là, d'obligations légales, et de principes fondamentaux en matière protection des données à caractère personnelle ; en l'occurrence le principe d'intégrité et de confidentialité. Aux termes de l'article 5-1-f du Règlement Général sur la Protection des Données (RGPD) : *« Les données à caractère personnel doivent être […] traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ».*

En cas de vulnérabilité informatique, il devient alors crucial de déterminer où réside la responsabilité : du prestataire d'infogérance, de l'établissement de santé lui-même ou d'une combinaison des deux. D'ailleurs, le critère de la responsabilité est inhérent à tout traitement de données à caractère personnel comme le précise l'article 5-2 du RGPD qui prévoit que : *« Le responsable du traitement est responsable du respect du paragraphe 1 [fixant les principaux fondamentaux de la protection des données] et est en mesure de démontrer que celui- ci est respecté (responsabilité) ».*

[42] A. Laude, J.-L. Mouralis, J.-M. Pontier, L. Louvel (ss. Dir.), *Revue Lamy droit de la santé,* Éditions Lamy Liaisons, n° 205-7 : *« on peut qualifier d'établissement de santé, la structure matérielle de soins et de prévention qui assure des missions légalement définies aux articles L. 6111-1 du Code de la santé publique et exercées, dans le respect d'un certain nombre de principes fondamentaux par des personnes publiques ou privées ».*

[43] https://www.lemondeinformatique.fr/actualites/lire-cyberattaque-contre-le-pole-sante-leonard-de-vinci-a-chambray-les-tours-85367.html sur les cyberattaques dont ont été victimes les établissements de santé ; consulté le 9 mai 2023.

Du point de vue juridique, et au-delà de ce qui est prévu par notamment l'article 5 et les articles 24 et suivants du RGPD, la responsabilité des prestataires d'infogérance en matière de vulnérabilités informatiques est souvent définie par les termes du contrat entre les deux parties. Les contrats devraient spécifier clairement les obligations et les responsabilités de chacun en matière de sécurité des données et des systèmes.

De manière très pragmatique et en raison de statut très complexe du sous-traitant, du point de vue du traitement des données à caractère personnel, le RGPD institue un ensemble d'obligations concernant la sous-traitance en fixant une liste non exhaustive d'éléments qui doivent figurer dans le contrat de sous-traitance. A ce effet, et à titre d'exemple, l'article 28-3 du RGPD précise que : *« Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement ».*

Cependant, les problèmes peuvent survenir lorsque les termes du contrat sont vagues ou mal définis, laissant place à des interprétations différentes en cas de problème. Mais, là encore, la Commission Nationale de l'Informatique et des Libertés (CNIL) propose exemple de clauses contractuelles de sous-traitance en annexe de son Guide du Sous-traitant[44].

D'un point de vue éthique, la protection des données médicales des patients est une préoccupation primordiale. Les prestataires d'infogérance doivent faire preuve de diligence et de responsabilité dans la mise en œuvre de mesures de sécurité adéquates pour prévenir les vulnérabilités informatiques. Cela implique d'investir dans des technologies de sécurité de pointe, de former leur personnel et de mettre en place des processus rigoureux pour détecter et répondre rapidement aux menaces potentielles.

En outre, la question de la responsabilité soulève également des préoccupations en matière de conformité aux réglementations en vigueur, notamment en ce qui concerne la protection des données personnelles des patients. Avec l'entrée en vigueur du RGPD, les établissements de santé et leurs prestataires d'infogérance sont soumis à des obligations strictes en matière de protection des données. Tout manquement à ces obligations peut entraîner des sanctions financières importantes[45] et des dommages à la réputation.

Cette externalisation permet à l'organisation de se concentrer sur son cœur de métier, tout en bénéficiant d'un service informatique performant, sécurisé et adapté à ses besoins. Les établissements de santé sont confrontés à des enjeux majeurs liés à la transformation numérique, à la réglementation, à la qualité des soins, à la satisfaction des patients, à la maîtrise des coûts, etc. L'infogérance peut leur apporter des solutions efficaces pour relever ces défis, notamment :

---

[44] CNIL, *Guide du sous-traitant – Edition septembre 2017 : https://www.cnil.fr/sites/cnil/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf* consulté le 15 août 2023.

[45] Art. 83-4 RGPD : *« amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu » ;* art. 83-4 RGPD : *«'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ».*

- La réduction des coûts : en externalisant leur système d'information, les établissements de santé peuvent réaliser des économies sur les investissements matériels, logiciels, humains et de formation. Ils peuvent également bénéficier d'une tarification adaptée à leur consommation réelle et optimiser leur budget informatique.
- La sécurité et la conformité : le prestataire d'infogérance s'engage à respecter les normes et les réglementations en vigueur dans le secteur de la santé, notamment en matière de protection des données personnelles, de confidentialité, de traçabilité, etc. Il assure également la sauvegarde, la restauration et la disponibilité des données en cas de sinistre ou de panne.
- La performance et l'innovation : le prestataire d'infogérance dispose d'une expertise et d'une veille technologique qui lui permettent de proposer aux établissements de santé des solutions adaptées à leurs besoins spécifiques, tels que la télémédecine, le dossier médical partagé, le big data, l'intelligence artificielle, etc. Il assure également la maintenance préventive et corrective du système d'information, ainsi que son évolution permanente.
- La qualité de service et la satisfaction : le prestataire d'infogérance offre aux établissements de santé un service personnalisé et réactif, avec un interlocuteur unique et dédié. Il garantit un niveau de service optimal, mesuré par des indicateurs clairs et transparents[46] dans les aspects RGPD afin de respecter le droit des personnes concernées[47], car

[46] Art. 5-1-a RGPD : *« Les données à caractère personnel doivent être… traitées de manière licite, loyale et transparente au regard de la personne concernée »*. Comme le précise la CNIL, *« la transparence permet aux personnes concernées de connaître la raison de la collecte des différentes données les concernant ; de comprendre le traitement qui sera fait de leurs données ; d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits »* https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence consulté le 15 août 2023. La CEPD indique dans ses lignes directrices que *« Le responsable du traitement doit faire preuve de clarté et d'ouverture à l'égard de la personne concernée et lui expliquer comment il entend collecter, utiliser et partager les données à caractère personnel la concernant. La transparence vise à permettre aux personnes concernées de comprendre leurs droits établis aux articles 15 à 22 et, si nécessaire, d'en faire usage. […] En ce qui concerne le principe de transparence, on peut citer parmi les éléments clés de protection des données dès la conception et par défaut : • Clarté - Les informations doivent être formulées en des termes clairs et simples, concis et compréhensibles. • Sémantique - La communication doit avoir une signification claire pour le public concerné. • Accessibilité - Les informations doivent être aisément accessibles pour la personne concernée. • Contextualité - Les informations doivent être fournies au moment opportun et sous la forme appropriée. • Pertinence - Les informations doivent être pertinentes et applicables à la personne concernée spécifique. • Conception universelle – Les informations doivent être accessibles à toutes les personnes concernées et inclure l'utilisation de langages lisibles par machine pour faciliter et automatiser la lisibilité et la clarté. • Compréhensibilité - Les personnes concernées doivent avoir une juste compréhension de ce qu'elles peuvent attendre en ce qui concerne le traitement de leurs données à caractère personnel, en particulier lorsqu'il s'agit d'enfants ou d'autres groupes vulnérables. • Canaux multiples - Les informations devraient être fournies par différents canaux et médias, au-delà du texte, afin d'accroître la probabilité que les informations parviennent effectivement à la personne concernée. • Structuration par couches – Les informations devraient être structurées par couches de manière à résoudre la tension entre l'exhaustivité et la compréhension, tout en tenant compte des attentes raisonnables des personnes concernées »*. CEPD, *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut*, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf consulté le 15 aout 2023. Voir également, Groupe de travail « Article 29 » Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 – Version révisée et adoptée le 11 avril 2018, p. 6 s. https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf consulté le 15 août 2023.

[47] Art. 12, 13 et 14 RGPD. L'article 12 du RGPD impose aux responsables du traitement de fournir des informations claires et compréhensibles à la personne concernée concernant le traitement de ses données personnelles. L'article 13 précise les informations à communiquer lors de la collecte de données personnelles, notamment l'identité du responsable, les finalités du traitement et les destinataires potentiels. Enfin, l'article 14 concerne les cas où les données ne

« un des objectifs du législateur dans le cadre de [la réforme RGPD] était les droits des personnes concernées et de leur rendre le contrôle de leurs données »[48]. Le prestataire d'infogérance contribue ainsi à améliorer la qualité des soins et la satisfaction des patients.

Dans le cadre du RGPD, en raison de leur rôle de responsable du traitement des données les établissements de santé ont la responsabilité de s'assurer que les prestataires d'infogérance traitent les données personnelles conformément aux exigences légales.

En effet, aux termes de l'article 4-7 du RGPD, le « responsable du traitement *[est] la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».* Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité et la confidentialité des données, ainsi que pour prévenir les violations de données. Un établissement de santé est une organisation qui offre des soins médicaux, chirurgicaux ou paramédicaux aux patients.

Les établissements de santé peuvent être publics ou privés et peuvent inclure des hôpitaux, des cliniques, des centres de santé, des maisons de retraite, des centres de soins à domicile, des centres de soins palliatifs et d'autres structures médicales[49]. Dans son activité quotidienne et dans ses missions, il effectue un traitement massif de données. Et cela se répercute systématique dans ses relations avec le prestataire d'infogérance à qui il sous-traitent la gestion de son système d'information. L'article 4-8 du RGPD présente le « sous-traitant » comme : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».*

En raison des risques de cette opération de sous-traitance (aussi bien technique que juridique du traitement des informations sensibles) d'infogérance, il est nécessaire de conclure des accords de traitement de données avec les prestataires, définissant clairement les responsabilités en matière de protection des données et les obligations de signalement en cas notamment de violation de données, d'atteinte à la confidentialité ou à l'intégrité des données.

Le cadre de notre analyse est ici très restrictif en termes d'entité dans la mesure ne seront pas prise en considération un certain nombre d'établissements intervenant dans le domaine de santé. Ce sera notamment le cas des établissements pharmaceutiques.

Dans un contexte où les attaques informatiques et les diverses violations de données à caractères personnelles, conformément à l'article 4-12 du RGPD)[50],

---

sont pas obtenues directement de la personne concernée, en imposant des informations à fournir, y compris l'origine des données.

[48] A. Banck, *RGPD : la protection des données à caractère personnel, 20 fiches pour réussir et maintenir votre conformité*, coll. « Droit en poche », Gualino-Lextenso, 2023, p. 59.

[49] Art. L. 611-1 s. CSP.

[50] Aux termes de l'art. 4-12 du RGPD, la violation de données à caractère personnel est *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».* Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles : https://www.cnil.fr/fr/definition/violation-de-donnees

continuent de constituer une menace croissante pour le secteur de la santé, la responsabilité des prestataires d'infogérance devient d'autant plus critique. En tant que gardiens des données et des systèmes informatiques des établissements de santé, ces prestataires ont le devoir de mettre en œuvre des mesures de sécurité robustes pour prévenir, détecter et contrer les cybermenaces.

Dans le cadre des systèmes d'information, l'infogérance est définie *« comme le résultat de l'intégration d'un ensemble de services élémentaires, visant à confier à un prestataire spécialisé tout ou partie d'une fonction de l'entreprise dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de service et une durée définis (AFNOR Z 67 801-1). Le terme infogérance désigne des services d'externalisation dans le domaine des systèmes d'information »*[51].

Les vulnérabilités informatiques sont des failles ou des faiblesses dans un système informatique qui peuvent être exploitées par des attaquants pour accéder à des données sensibles, endommager ou perturber le fonctionnement du système. Les vulnérabilités informatiques peuvent résulter de problèmes de configuration, de logiciels malveillants, de faiblesses dans les mots de passe, d'erreurs humaines ou d'autres facteurs[52]. Les vulnérabilités informatiques peuvent être regroupées en trois grands groupes : *« les vulnérabilités matérielles ou logicielles qui nécessitent l'installation d'un correctif ou d'un contournement ; les vulnérabilités applicatives qui nécessitent une correction dans le code source de l'application ; les erreurs de configuration qui nécessitent la modification de paramètres, comme les services inutiles qui nécessitent la suppression ou la désactivation de composants inutiles ou obsolètes »*[53].

La responsabilité est l'obligation morale, juridique ou contractuelle de répondre de ses actes ou de ses négligences. En cas de problème, la responsabilité implique de prendre les mesures nécessaires pour réparer les dommages causés et pour éviter que le même problème ne se reproduise à l'avenir[54]. Dans cette perspective il apparait légitime de se demander de quelle manière pourrait-on évaluer la responsabilité du prestataire d'infogérance d'un établissement de santé en cas de vulnérabilités informatiques, en prenant en compte les risques liés à l'activité d'infogérance ou à l'externalisation des systèmes d'information des établissements de santé, les obligations légales et contractuelles des parties, ainsi que les mesures de sécurité à mettre en place pour éviter ces vulnérabilités.

L'objectif est de contribuer à une meilleure compréhension de la responsabilité du prestataire d'infogérance en cas de vulnérabilités informatiques et de violations de données de santé, ainsi qu'à l'amélioration de la sécurité informatique et de la protection des données de santé dans les établissements de santé. A titre préliminaire, il convient de préciser que l'article 4-15 du RGPD définit les données concernant la santé comme *« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y*

[51] ASIP – ANAP, *Mutualisation et Externalisation des SI de santé : Éclairage pour le décideur*, consulté le 9 mai 2023 sur le site https://www.afexis.com/wp-content/uploads/2016/10/Mutualisation-et-externalisation-SI.pdf p. 6.

[52] CLUSIF, *Gestion des vulnérabilités informatiques : vers une meilleure gestion des risques opérationnels [Valeur et caractère indispensable de la gestion des vulnérabilités]*, tome 1, Mai 2014, p. 10.

[53] CLUSIF, *Gestion des vulnérabilités informatiques Vers une meilleure gestion des risques opérationnels*, tome 2, 2015, p. 9-10.

[54] Responsabilité civile : Code civil art. 1231 s., 1240 s., anc. art. 1146 s., 1382 s. ; Responsabilité pénale : Code pénal art. 121-1 et 121-2 ; Responsabilité médicale : Code de la Santé Publique art. L. 1111-2, L. 1142-1 s.

compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

Pour atteindre cet objectif, il conviendra de mener les démarches suivantes :

- Analyser les obligations légales et réglementaires applicables aux prestataires d'infogérance en matière de sécurité informatique et de protection des données de santé dans le contexte des établissements de santé. Cette analyse devra prendre en compte le Règlement Général sur la Protection des Données (RGPD)[55], la Loi Informatique et Libertés (LIL)[56], ainsi que les normes professionnelles et les recommandations émises par les autorités compétentes ;
- Examiner les obligations contractuelles entre les établissements de santé et les prestataires d'infogérance en matière de sécurité informatique et de protection des données de santé. Cette analyse devra prendre en compte les clauses contractuelles types et les clauses spécifiques négociées entre les parties ;
- Examiner les pratiques courantes en matière de sécurité informatique et de protection des données de santé dans les établissements de santé et chez les prestataires d'infogérance. Cette analyse permettra d'identifier les bonnes pratiques à suivre et les pratiques à éviter pour minimiser les risques de vulnérabilités informatiques et de violations de données de santé ;
- Proposer des recommandations pratiques pour les établissements de santé et les prestataires d'infogérance afin de minimiser les risques de responsabilité en matière de sécurité informatique et de protection des données de santé. Ces recommandations pourront porter sur les aspects contractuels, organisationnels, techniques et humains de la sécurité informatique et de la protection des données de santé.

L'hypothèse envisagée est que la responsabilité du prestataire d'infogérance d'un établissement de santé en cas de vulnérabilités informatiques est complexe et dépend de nombreux facteurs, tels que la nature de la vulnérabilité, les termes du contrat de service, les politiques de sécurité et les mesures de prévention mises en place par le prestataire et l'établissement de santé. La recherche approfondie des facteurs influençant la responsabilité des prestataires d'infogérance dans le contexte de la gestion des systèmes d'information des établissements de santé peut aider à mieux comprendre les risques associés à l'externalisation et à l'infogérance de ces systèmes, et à proposer des recommandations pour améliorer les pratiques de sécurité et les contrats de service dans ce domaine.

Malheureusement, force est d'envisager que cette perspective devra faire face à un certain nombre de limites :

- La disponibilité des données : Il est possible que les données disponibles sur les incidents de sécurité informatique impliquant des prestataires d'infogérance dans les établissements de santé soient limitées, ce qui peut affecter la qualité et la quantité des résultats de la recherche ;

[55] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[56] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- La disponibilité des acteurs concernés : La recherche peut nécessiter la participation d'acteurs clés tels que les prestataires d'infogérance et les établissements de santé. Leur disponibilité pour participer à des entretiens ou à des enquêtes peut être limitée en raison de contraintes de temps ou de ressources ;
- La complexité du cadre réglementaire : Le cadre réglementaire entourant la gestion de la sécurité des données de santé peut être complexe et varier selon les juridictions. Il peut être difficile de prendre en compte toutes les nuances et les différences entre les différents cadres réglementaires dans la recherche.

Pour répondre aux problématiques relevées nous analyserons les facteurs de risques liés à l'opération d'infogérance (I) avant d'étudier le régime de traitement desdits facteurs (II).

I. Les facteurs de risques liés à l'infogérance des établissements de santé

Comme nous l'avons évoqué dans les premières lignes de notre analyse, le recours à l'externalisation de la gestion du système informatique des établissements de santé répond à un besoin avéré. Comme le précise l'Agence nationale de la sécurité des systèmes d'information (ANSSI), *« l'externalisation (en anglais « outsourcing ») est une démarche consistant à confier à un tiers tout ou partie d'une activité qui jusqu'alors était réalisée en interne »*[57]. Pour sa part, l'infogérance correspond *à « l'externalisation appliquée au domaine des systèmes d'information »*[58]. Dans une approche plus affinée, La gérance de l'informatique (communément dénommée *Facilities management* ou encore infogérance), dénomination de l'externalisation en matière de systèmes d'information, est officiellement définie comme la *« prise en charge contractuelle de tout ou partie de la gestion d'un système d'information d'un organisme par un prestataire extérieur »*[59].

Au-delà des avantages évidents que présentent cette démarche, il n'en demeure pas moins, qu'elle implique des risques particulièrement importants qui sont susceptibles de constituer des éléments déclencheur de la responsabilité des prestataires d'infogérance et par ricochet de portée atteinte aux données de santé[60]. En effet, l'externalisation correspond au transfert d'activités d'un organisme vers un prestataire externe. L'externalisation des données (parfois chez plusieurs prestataires en chaîne) peut provoquer des failles dans la protection de la confidentialité des données.

Dans la mesure où l'infogérance est une opération technique fondées sur des bases contractuelles et donc juridiques, il serait opportun d'analyser les facteurs de risques opérationnels (A) avant d'envisager les facteurs de risques juridiques (B).

A. Les facteurs de risques opérationnels

L'infogérance des établissements de santé peut présenter des avantages, mais aussi des risques qu'il convient d'évaluer avant de

[57] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 6.

[58] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 6.

[59] *Vocabulaire de l'informatique* : JO 20 avril 2007, p. 7078.

[60] Système national des données de santé, *Référentiel de sécurité : guide d'accompagnement*, consulté le 9 mai 2023 sur le site https://www.snds.gouv.fr/download/Guide_accompagnement.pdf, p. 11.

prendre la décision de l'intégrer dans son processus de gestion des données de santé. Les risques en matière de sécurité des systèmes d'information peuvent être liés au contexte de l'opération d'externalisation mais aussi à des spécifications contractuelles déficientes ou incomplètes.

L'Agence nationale de la sécurité des systèmes d'information a rédigé un guide[61] pour aider les décideurs informatiques à prendre conscience des risques en matière de sécurité des systèmes d'information (SSI) liés à toute opération d'externalisation et pour fournir une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation. C'est donc sur la base de ces éléments que l'analyse sera réalisée ; et il sera analysé successivement, sans que ces points ne soient exhaustifs, la perte de maîtrise du système d'information (1), l'intervention à distance (2), l'hébergement mutualisé des données de santé (3), ensemble de facteurs inhérents parfois au recours à l'informatique en nuage.

1. *La perte de maîtrise du système d'information*

La perte de maîtrise du système d'information est un risque à prendre en considération lorsque l'établissement de santé décide de travailler en infogérance. Cette menace peut être liée à la sous-traitance, à la localisation des données, à la nature particulière des données santé ainsi qu'aux choix techniques opérés par le prestataire. En effet, la responsabilité du sous-traitant, en vertu de l'article 82-2 du RGPD[62], sera établie sur la base la matérialité du dommage subit par les personnes concernées et plus spécifiquement s'il est établi que ce dommage lui est imputable. Cela sera notamment le cas si le dommage résulte d'un défaut du respect des obligations qui lui incombent en application du RGPD et si le dommage résulte de l'inobservation des instructions licites du responsable du traitement, à savoir l'établissement de santé.

A ce stade de l'analyse, les facteurs de risques techniques doivent être considérés aussi bien sous l'angle de l'activité de l'établissement de santé que sous celui du prestataire d'infogérance.

De prime abord, il faut considérer que l'établissement de santé risque de perdre la maîtrise de son propre système d'information si elle délègue trop la maîtrise d'ouvrage à un prestataire extérieure.

Pour situer le contexte, il faut savoir que dans le cadre d'une entreprise la maîtrise des systèmes informatiques comporte trois volets essentiels que sont : la maîtrise de l'exploitation qui est gérée par le Directeur de l'Informatique (DI) ou par le Responsable de la Sécurité des Systèmes d'Information (RSSI), la maîtrise du développement des nouvelles applications informatiques qui relève du domaine de prédilection du Directeur de l'Informatique, la maîtrise de la maintenance (entretien, adaptation, amélioration des applications existantes)[63].

---

[61] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance,* consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, *passim.*

[62] Art. 82-2 RGPD : *« Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci ».*

[63] J. des Courières, « Au-delà de la maîtrise des systèmes d'information la maîtrise de l'entreprise », *Lettre d'ADELI* n°39 – Avril 2000, p. 27.

La perte de maîtrise du système d'information soulève de réels problèmes dans le cadre de la gestion des données à caractère personnel et plus spécifiquement des données dans la mesure où, du point de vue de la règlementation en matière de données à caractère personnel, l'établissement de santé reste le responsable de traitement.

En effet, l'article 4-7 du RGPD précise que le *« responsable du traitement [est] la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».*

Le responsable du traitement est donc bien, en règle générale, le client (ici l'établissement de santé) et non son prestataire (à savoir le prestataire d'infogérance). La jurisprudence française a pu préciser que *« la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable du traitement de la responsabilité qui lui incombe de préserver la sécurité des données, sans que soit ainsi méconnu le principe constitutionnel de responsabilité personnelle, dès lors que ces sous-traitants agissent sur instruction du responsable de traitement »*[64].

La perte de maitrise du système d'information liée à la sous-traitance est une menace qui se présente dans le cadre du recours à l'infogérance. Il faut avant tout préciser que la sous-traitance est une *« opération par laquelle un entrepreneur, dit entrepreneur principal, confie par une convention appelée sous-traité ou contrat de sous-traitance, à une autre personne nommée sous-traitant, l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maître d'ouvrage, le recours à la sous-traitance impliquant, pour l'entrepreneur principal, l'obligation de faire accepter les sous-traitants par le maître d'ouvrage »*[65].

En pratique, l'établissement de santé intéressé par la sous-traitance, peut se présenter seul, au sein d'un groupement avec une ou plusieurs entités, ou encore recourir à la sous-traitance. Et c'est à ce moment que la sous-traitance peut devenir un risque notamment lorsque la prestation d"infogérance est sous-traitée à un fournisseur tiers par le prestataire principal ; c'est le cas de figure typique de la sous-traitance ultérieure prévue par l'article 28-4 du RGPD.

Dans ce type de situation, l'établissement de santé, en tant que responsable du traitement, peut se retrouver indirectement dépendant du prestataire principal pour la gestion de son système d'information. Cela peut compliquer la communication et la prise de décision directe en cas d'incident ou de problème ; d'autant plus qu'il n'a aucune garantie que la finalité et les moyens d'un traitement qu'il aura établit avec le sous-traitant soit répercuté par le sous-traitant ultérieur.

A cela s'ajoute le fait que l'établissement de santé peut perdre de la visibilité sur les opérations quotidiennes et sur les pratiques mises en place par le sous-traitant. Cela peut rendre plus difficile l'évaluation de la qualité des services rendus et l'identification des problèmes potentiels et le respect des principes fondamentaux en matière de protection des données de santé.

[64] CE, 30 décembre 2015 : *JurisData* n° 2015-029454.

[65] G. Cornu, *Vocabulaire juridique,* PUF, 13e éd., 2020, *v° « Sous-traitance ».*

La dégradation de la qualité du service peut être un facteur de risque lié à la sous-traitance en raison du fait que le prestataire principal peut parfois sous-traiter à un sous-traitant pour des raisons de coûts. Cela peut entraîner une dégradation de la qualité des services fournis, car le sous-traitant (ultérieur) peut ne pas avoir le même niveau d'expertise et d'engagement envers l'établissement de santé. Très concrètement, en cas de violation de la sécurité des données ou d'incident informatique, la gestion de la réponse peut être complexe si l'établissement de santé fait face à une chaîne de sous-traitance. La coordination entre le prestataire principal, les sous-traitants et l'établissement de santé peut entraîner des retards dans la prise de décision et la résolution du problème, ce qui augmente le risque de dommages.

Dans tous les cas, le recours généralisé à la sous-traitance complexifie la gestion des fuites de données par le responsable de traitement. L'article 82 du RGPD établit la responsabilité du responsable de traitement dès lors qu'il a participé au traitement ayant causé un dommage. Dès lors, le responsable de traitement se doit de gérer les fuites de données du sous-traitant avant, pendant et après son occurrence[66]. Il convient également d'établir un parallèle avec l'article 28 du RGPD qui pose le cadre de la responsabilité indirecte. Les articles 28 et 82 du RGPD distinguent la responsabilité du responsable du traitement et celle du sous-traitant en fonction de leur rôle et de leur implication dans le traitement.

Le responsable du traitement est responsable de tout dommage causé par le traitement qui constitue une violation du RGPD, sauf s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable. Le sous-traitant n'est tenu pour responsable que s'il n'a pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci. Ces deux articles prévoient que le responsable du traitement ou le sous-traitant doit aider l'autre partie à s'acquitter de ses obligations en matière de protection des données, notamment en cas de violation de données, d'analyse d'impact relative à la protection des données, de consultation préalable ou de respect des droits des personnes concernées.
A ce premier palier de risque lié au recours à l'infogérance, il faut aussi ajouter le risque lié à la perte de maîtrise liée à la localisation des données avec le problème principal du traitement transfrontalier.

L'hébergement externalisé n'est pas en soi une mauvaise chose. En effet, l'informatique en nuage (cloud computing) est une évolution de la fourniture d'applications hébergées. Il s'agit d'un *« mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire »*[67]. Il est précisé que c'est *« une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients »*[68].

Ces modes de fourniture de service informatique à distance permettent donc une externalisation informatique[69] de l'entreprise. Ils présentent un avantage certain en termes de coûts : l'établissement de santé qui est ici

[66] K. Bouslimani, « Fuite de données émanant d'un sous-traitant : comment gérer ? », publié le 17 mai 2022 sur le site https://www.village-justice.com/articles/fuite-donnees-emanant-sous-traitant,42216.html, consulté le 24 juillet 2023.

[67] *Vocabulaire de l'informatique,* JO 6 juin 2010, p. 10453.
[68] *Idem.*
[69] Le terme d'« outsourcing » est souvent utilisé.

le client n'a pas à se soucier de l'achat d'un matériel particulier pour l'utilisation du progiciel, et voit le coût du logiciel utilisé payé sur la durée de son utilisation, contrairement à la licence de progiciel[70], où bien souvent le prix est forfaitaire et payé intégralement à la conclusion du contrat. En outre, ce mode de fonctionnement autorise une grande souplesse, les services pouvant être souscrits en fonction des besoins réels du client[71].

Le propre de l'informatique en nuage est de reposer sur des infrastructures réparties, en conséquence d'atomiser les fichiers de données. Contrairement à un service d'externalisation classique fourni par un prestataire dont la localisation du centre de données (datacenter) est connue, le service de cloud implique une localisation dans plusieurs endroits simultanément. De telles solutions *« constituent souvent un facteur d'aggravation des risques d'atteinte à la confidentialité des données »*[72]. Un pan plus vicieux de ce processus réside dans le fait que les données peuvent être hébergés sur des serveurs situé dans pays ayant une législation en matière de protection de données à caractère personnel qui soit laxiste voire moins rigoureuse que le cadre posé par le RGPD, et notamment par l'article 4-23 du RGPD qui définit le traitement transfrontalier.

Pour sa part, l'article 44 du RGPD précise que : *« un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale ».*

Cette situation est de nature à accentuer le risque de violation des données personnelles. Il s'agit d'éléments juridiques avec des implications pratiques concrètes.

La question de la sécurité des données se pose d'un point de vue technique dans la mesure où l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des établissements de santé.

De plus, l'ANSSI précise qu'une localisation de données non maîtrisée peut comporter d'autres risques : difficulté à exercer un droit de regard et de contrôle sur les personnels du prestataire ; difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente ; difficulté à répondre à d'éventuelles injonctions de la justice, pour des raisons fiscales par exemple, ou d'autres raisons d'ordre juridique[73]. A cela il convient d'ajouter les aspects tenant au respect des

[70] Un progiciel : *« est, selon le vocabulaire officiel de l'informatique, un « ensemble complet et documenté de programmes conçu pour être fourni à plusieurs utilisateurs en vue d'une même application ou d'une même fonction » (Journal Officiel du 17 janvier 1982). Les progiciels constituent donc une catégorie parmi les logiciels : ce sont des logiciels standards conçus pour répondre aux besoins communs de nombreux utilisateurs / clients, par opposition aux « logiciels spécifiques » qui sont développés spécialement pour une entreprise (soit par ses informaticiens, soit le plus souvent par un prestataire informatique externe) pour répondre aux besoins propres de cette entreprise »* cf. https://www.dictionnaire-juridique.com/definition/progiciel.php consulté le 17 août 2023.

[71] F. Macrez, « Contrats d'externalisation informatique – Infogérance, fourniture d'application hébergée, informatique en nuage », JurisClasseur Communication, n° 815, 1er septembre 2022.

[72] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf , p. 8.

[73] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf , p. 8.

obligations imposées par le RGPD notamment l'obligation de transparence et de traçabilité qui prend la forme d'une mise à la disposition du responsable de traitement, par le sous-traitant, de toutes les informations nécessaires pour démontrer le respect de ses obligations, dans la lignée de ce prévoit l'article 28 du RGPD. Par exemple, le sous-traitant doit veiller *« à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité »*[74].

D'ailleurs, vu la complexité et la particularité de cette opération d'externalisation, il paraît difficile de faire peser sur le prestataire l'intégralité de la responsabilité de la confidentialité et de la sécurité des données : les responsabilités respectives de chaque cocontractant doivent être réfléchies et stipulées. La question est appréhendée sur le plan juridique par une règlementation très spécifique[75].

Le cas typique de ce type de risque est perceptible dans l'affaire DEDALUS concernant une fuite de donnée de santé massive[76]. En effet, pour évoquer le contexte de cette affaire, le 23 février 2021, une fuite de données massive concernant près de 500 000 personnes a été révélée dans la presse, qui mettait en cause la société DEDALUS. Les nom, prénom, numéro de sécurité sociale, nom du médecin prescripteur, date de l'examen mais aussi et surtout des informations médicales (VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques) de ces personnes ont ainsi été diffusés sur internet. Dès le 24 février 2021, la CNIL a effectué plusieurs contrôles, notamment auprès de la société DEDALUS BIOLOGIE qui commercialise des solutions logicielles pour des laboratoires d'analyse médicale. En parallèle, la CNIL a saisi le tribunal judiciaire de Paris qui a bloqué l'accès au site sur lequel étaient publiées les données ayant fuité. Cette décision du 4 mars 2021 a permis de limiter les conséquences pour les personnes. Sur la base des constatations effectuées lors des contrôles, la formation restreinte de la CNIL[77] a considéré que la société avait manqué à plusieurs obligations prévues par le RGPD, en particulier à l'obligation d'assurer la sécurité des données personnelles. La formation restreinte a ainsi prononcé une amende de 1,5 million d'euros et a décidé de rendre publique sa décision. Le montant de cette amende a été décidé au regard de la gravité des manquements retenus mais également en prenant en compte le chiffre d'affaires de la société DEDALUS BIOLOGIE[78].

---

[74] Art. 28-3-b du RGPD.

[75] Notamment l'article L. 1111-8 du Code de la santé publique : « Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article. L'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. La prestation d'hébergement de données de santé à caractère personnel fait l'objet d'un contrat ».

[76] Délibération de la formation restreinte n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE.

[77] La formation restreinte de la CNIL est l'organe chargé de prononcer les sanctions. « *Elle est composée de 5 membres et d'un Président distinct du Président de la CNIL. Elle peut prononcer diverses sanctions à l'égard des responsables de traitement qui ne respecteraient pas la loi* ». Cf. https://www.cnil.fr/fr/definition/formation-restreinte

[78] https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie

Un autre facteur de risque lié au choix du prestataire peut consister dans le fait que le prestataire peut être responsable des mises à jour, des correctifs de sécurité et des améliorations du système d'information. Si ces mises à jour ne sont pas effectuées correctement ou en temps opportun, cela peut entraîner des vulnérabilités de sécurité et une dégradation des performances.

Par ailleurs, si le prestataire d'infogérance ne suit pas de près l'évolution des technologies et des besoins de l'établissement de santé, cela peut entraîner des retards dans l'adoption de nouvelles fonctionnalités ou des opportunités manquées pour améliorer le système d'information. En toutes circonstances, les applications employées devraient idéalement être interopérables, garantissant au minimum une compatibilité avec les systèmes d'exploitation et les bases de données les plus largement utilisés.

Il convient également d'envisager les risques qui sont inhérent à l'intervention à distance, dans la mesure où cela correspond à l'opération technique adoptée.

2. L'intervention à distance

L'externalisation en générale, et plus spécifiquement l'infogérance peuvent impliquer des interventions à distance, où les prestataires de services gèrent et maintiennent les systèmes informatiques de l'établissement de santé à distance, sans être physiquement présents sur site. Les interventions à distance sont une partie importante de l'infogérance. Elles permettent aux prestataires d'intervenir sur les systèmes informatiques des clients sans avoir à se déplacer sur place.

Cela présente de nombreux avantages, tels qu'une plus grande rapidité d'intervention et une meilleure disponibilité des systèmes informatiques et par ricochet des données personnelles comme le prévoit l'article 32-1-b et 32-1-c du RGPD en vertu desquels *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins […] des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement […] des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ».*

L'Agence Nationale de la Sécurité des Systèmes d'Information a publié deux documents couvrant certains aspects des interventions à distance :

- Le guide *« Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information »*[79] ;
- La note technique *« Recommandations de sécurité relatives à la téléassistance »*[80].

Le guide ANSSI couvre les prestations informatiques ou de télécommunication confiées à des tiers, quelle que soit leur nature. Il traite en particulier le cas des prestations effectuées à distance. Pour ces dernières, il indique les vulnérabilités fréquemment rencontrées, souligne les risques principaux d'intrusion et d'abus de privilège d'accès et émet des recommandations. Quant à la note technique,

[79]https://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-dessystemes-d-information-un-guide-pour-maitriser.html

[80]https://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-la-tele-assistance.html

elle concerne la sécurité de la téléassistance et en particulier de la prise de main à distance sur un poste de travail. Elle précise les risques associés et donne des recommandations minimales à respecter.

Les principales recommandations de ces deux documents ont été reprises dans le document intitulé : *« Règles pour les interventions à distance sur les systèmes d'information de santé Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Avril 2014 »*[81]. Ce document définit les règles et les recommandations de sécurité relatives aux interventions effectuées à distance dans un Système d'Information de Santé (SIS). Il fait partie des guides spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)[82].

Ce guide donne une certaine définition de ce que recouvre les interventions à distance qui concernent les Systèmes d'Information de Santé, et il évoque notamment : la télésurveillance, la télémaintenance et la téléassistance.

Il les définit[83] comme suit :

- ***La télésurveillance*** désigne le processus de collecte et d'analyse à distance d'informations liées au fonctionnement technique d'un Système d'Information de Santé (SIS), dans le but de surveiller son fonctionnement, d'anticiper les tendances à venir et de repérer d'éventuelles irrégularités. Par exemple, cela peut englober le suivi des paramètres de charge d'un ensemble d'appareils ou l'exécution régulière de tests d'une application pour garantir sa disponibilité permanente.

- ***La télémaintenance*** englobe les actions entreprises à distance pour ajuster les paramètres et configurer les logiciels d'une partie ou de l'intégralité d'un Système d'Information de Santé, dans le but de maintenir son fonctionnement optimal ou de le faire évoluer. Cela peut inclure des activités telles que l'exploitation et la gestion technique, la résolution d'incidents techniques et la mise à jour logicielle.

- ***La téléassistance*** implique de fournir de l'aide depuis une station distante où les interfaces d'accès de la personne aidée sont reproduites fidèlement. Dans certaines situations, la seule interface reproduite est l'affichage à l'écran, et l'intervenant a la capacité d'observer uniquement ce que la personne assistée voit ou fait. Des exemples concrets incluent le dépannage logique d'un utilisateur sur son poste de travail ou la fourniture directe d'expertise par un

[81] ASIP Santé/DSSIS : Règles d'intervention à distance – Avril 2014 - V0.3

[82] La PGSSI-S regroupe des référentiels thématiques (identification électronique des acteurs, force probante des documents de santé, imputabilité des actions…) et des guides pratiques, qui rappellent aux différents acteurs des systèmes d'information de santé les bonnes pratiques pour être en conformité avec la réglementation en vigueur. L'Etat a confié à l'Agence du Numérique en Santé (ANS) l'élaboration et la publication de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), cadre devant être respecté par tous les acteurs de la santé, du social et du médico-social pour sécuriser les systèmes d'information de santé (SIS). L'article L. 1470-5 du code de la santé publique prévoit en effet que l'ANS élabore, en concertation avec l'écosystème, des référentiels visant à garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel par les services numériques en santé. cf. : https://esante.gouv.fr/sites/default/files/media_entity/documents/180528_PGSSI-S_0.pdf

[83] ASIP Santé/DSSIS : *Règles d'intervention à distance* – Avril 2014 - V0.3, p. 6.

administrateur sur la console d'un serveur.

Force est de constater que la sécurité n'est pas toujours bien appréhendée pour réaliser ce type d'intervention alors que les solutions utilisées apportent des vulnérabilités et octroient aux intervenants des droits importants. Par nature, un outil de téléassistance donne un accès très large aux ressources disponibles sur le poste de travail d'un utilisateur. Ainsi, tout individu accédant à distance à un poste de travail lors d'une opération de téléassistance peut prendre connaissance de l'ensemble des informations stockées sur la machine dont les données personnelles, utiliser différents périphériques qui y sont connectés (microphone, webcam etc.) voire employer les différentes applications installées en lieu et place des personnes se connectant localement.

Se posent alors des problèmes de protection et de préservation de la confidentialité des informations contenues dans le poste de travail, de traçabilité des opérations réalisées et du contrôle par l'utilisateur des opérations effectuées sur sa machine.

Appréhendé sous le volet protection des données personnelles, il faut relever que les risques liés à l'accès à distance des données personnelles par un sous-traitant comprennent plusieurs aspects. L'accès à distance pourrait augmenter le risque de violation de la sécurité des données, car les connexions à distance pourraient être vulnérables aux attaques informatiques et aux intrusions non autorisées. Également, si le sous-traitant se trouve dans un pays en dehors de l'Espace Économique Européen (EEE) ou d'un pays reconnu comme ayant un niveau adéquat de protection des données, le transfert international de données pourrait être effectué sans garanties appropriées, ce qui serait une violation du RGPD. Par ailleurs, lorsque les sous-traitants ont un accès distant aux données personnelles, le contrôle sur la manière dont ces données sont traitées peut devenir plus difficile à exercer par l'établissement de santé responsable du traitement desdites données.

Sur le volet cybersécurité, plusieurs menaces sont induites par les interventions à distance et sont des facteurs de risques dans le cadre de la prestation d'infogérance des Systèmes d'Information des établissements de santé. Entre autres cas, nous pouvons citer, pour reprendre les cas évoqués par le Guide de l'ASPI Santé/DSSIS[84] :

- Si le responsable du SIS ne maîtrise pas la sécurité de l'environnement organisationnel dans lequel s'exécute la prestation, les menaces à l'encontre du Système d'information sont notamment : défauts d'exécution ou de qualité de la prestation, conduisant à des indisponibilités du SIS, des pertes de confidentialité ou d'intégrité des données. Divulgation de données de la prestation vers des entités du fournisseur ou des organismes tiers (en cas de sous-traitance notamment), susceptible d'entraîner la violation d'obligations légales ou réglementaires ou l'incapacité çà répondre à des injonctions des institutions judiciaires. Accès logique au SIS par du personnel non autorisé du fournisseur.
- Si le responsable du SIS ne maîtrise pas la sécurité de l'environnement technique dans lequel s'exécute la prestation : les

[84] ASIP Santé/DSSIS : *Règles d'intervention à distance* – Avril 2014 - V0.3, p. 6.

menaces à l'encontre du Système d'information sont notamment : propagation d'incidents de sécurité dans le SIS parla plateforme du fournisseur : codes malveillants, attaques logiques de la plateforme. Accès logique illicite à des données du SIS par les utilisateurs de la plateforme.

- Si le responsable du SIS ne maîtrise pas la sécurité de l'environnement physique dans lequel s'exécute la prestation, les menaces à l'encontre du Système d'information sont notamment : Capture physique de données de la prestation dans l'environnement de la plateforme du fournisseur, observation du personnel, vol de support de stockage. Destruction de la plateforme, entraînant l'incapacité à assurer la prestation.

En dehors de modalités de traitement des données à distance évoquées, il est également utile d'envisager une autre approche qui consiste dans l'hébergement mutualisé des données de santé et qui présente un intérêt indéniable pour appréhender les critères de risques en matière d'infogérance.

3. L'hébergement mutualisé des données de santé

L'activité d'hébergement de données de santé consiste à héberger les données de santé à caractère personnel pour le compte de personnes physiques ou morales qui sont à l'origine de la production ou du recueil de ces données[85]. Quant à l'hébergement mutualisé, il consiste à héberger plusieurs services sur un seul et même serveur, afin de rationaliser les ressources. Dans la majorité des cas, les services concernés sont des sites Web, des services de messagerie ou des bases de données. Dans ce cas de figure, les clients (les établissements de santé) n'ont pas accès directement aux serveurs ou aux ressources mutualisées en tant qu'administrateurs. La configuration est réalisée puis gérée par l'hébergeur ou une société tierce[86].

De manière plus spécifique, l'hébergement mutualisé des données de santé et l'infogérance sont deux concepts liés à la gestion des systèmes informatiques dans le domaine de la santé. L'hébergement mutualisé implique de stocker les données de santé de plusieurs établissements de santé sur une même infrastructure informatique partagée. Cela permet aux établissements de partager les ressources informatiques, ce qui peut réduire les coûts d'infrastructure. Cependant, cela signifie également que les données de plusieurs établissements sont conservées dans un environnement partagé, ce qui soulève des questions de confidentialité et de sécurité.

Le recours au *Cloud,* par exemple, place l'établissement de santé en situation de dépendance technologique vis-à-vis du fournisseur qui dispose de la maîtrise des moyens de traitement et des données, et qui peut être tenté, par conséquent, de faire obstacle à leur accès par l'utilisateur au cours ou en fin de contrat. Or, ce dernier peut avoir de bonnes raisons de vouloir accéder à ses données : en cours de contrat par exemple, afin de répondre à des obligations légales (comme le droit d'accès ou le droit à la portabilité) ou bien pour s'assurer de la bonne exécution du contrat ; à l'issue de celui-ci, afin d'assurer la réversibilité (en cas de réinternalisation), ainsi que la transférabilité

[85] Articles R.1111-8-8 et R.1111-9 du Code de santé publique.

[86] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulté le 9 mai 2023 sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 13.

(en cas de poursuite de l'externalisation auprès d'un autre fournisseur) des prestations.

L'infogérance peut inclure la gestion des serveurs, la maintenance du réseau, la sécurité des données, le support technique, etc. L'infogérance permet aux établissements de santé de bénéficier de compétences techniques spécialisées sans avoir besoin de maintenir une équipe interne dédiée à ces tâches.

Lorsque l'hébergement mutualisé des données de santé est combiné avec l'infogérance, les établissements de santé peuvent choisir de confier la gestion de leur infrastructure informatique partagée à un prestataire d'infogérance externe. Cela permet aux établissements de bénéficier à la fois des avantages de l'hébergement mutualisé, tels que la réduction des coûts, et des avantages de l'infogérance, ainsi que l'accès à une expertise technique spécialisée.
Selon l'ANSSI, les risques proviennent du fait que le service hébergé est plus ou moins étroitement lié à d'autres services, certains étant plus vulnérables que les autres. D'autre part, les attaques ciblant une des ressources mutualisées (réseau, logiciel, matériel) pourront avoir des conséquences sur l'ensemble des services co-hébergés.

En effet, du point de vue de la sécurité des systèmes d'information, les principaux risques liés au co-hébergement et leurs répercussions sont les suivants, la perte de disponibilité ; perte d'intégrité et perte de confidentialité. Ces différents risques sont amplifiés lorsque le traitement des données intervient dans un environnement non maîtrisé.

En effet, bien que les prestataires d'infogérance mettent en place des mesures de sécurité pour protéger les données, il existe toujours un risque d'accès non autorisé par un personnel malveillant du prestataire d'infogérance. Cela peut être particulièrement préoccupant lorsque des données médicales par nature sensibles sont concernées.

A ce facteur de risque, s'ajoute la complexité de la gestion des autorisations qui peut intervenir lorsque plusieurs établissements partagent une infrastructure d'hébergement mutualisé. Pour que l'analyse soit complète, il est nécessaire d'aborder les facteurs de risques juridiques.

B. Les facteurs de risques juridiques

En plus des divers risques opérationnels que nous avons abordés précédemment, et qui semblent évidents lorsqu'il s'agit d'une opération d'externalisation, il convient d'ajouter des facteurs plus subtils et donc plus complexes liés à l'aspect juridique de l'infogérance des systèmes d'information de santé. Nous confronterons d'une part les éléments qui semblent être des risques, mais qui en réalité sont des sources de complexité pour l'opération, et qui sont issus de la nature juridique des données de santé (1). D'autre part, nous examinerons les contours de la relation contractuelle (2).

1. L'objet de l'atteinte : les données de santé

Même si cela peut paraître anodin, la nature particulière des données de santé[87], objet de l'opération d'infogérance, constitue en facteur de risque juridique que les co-

[87] A. Banck, *RGPD : la protection des données à caractère personnel, 20 fiches pour réussir et maintenir votre conformité*, coll. « Droit en poche », Gualino-Lextenso, 2023, p. 29.

contractants doivent prendre en considération. En effet, en raison de cette nature complexe et très encadrée, les données de santé ne doivent pas être gérées comme tous les autres types de données à caractère personnel dans le cadre de l'infogérance.

Selon l'article 4-15 du RGPD, les données de santé sont des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de soins de santé, qui révèlent des informations sur l'état de santé de cette personne[88]. Elles sont considérées comme des données sensibles, c'est-à-dire des données qui font l'objet d'une protection renforcée par le droit, car elles sont particulièrement intimes et susceptibles de porter atteinte à la vie privée ou aux droits fondamentaux des personnes[89].

L'article 4-15 du RGPD est au cœur d'un débat important concernant la définition de la donnée de santé et ses implications en matière de traitement des données à caractère personnel. La définition de la donnée de santé est cruciale car elle détermine si certaines informations relèvent de cette catégorie et, par conséquent, sont soumises à un traitement plus strict en vertu du RGPD. Le débat porte sur la clarté et l'étendue de cette définition, notamment sur ce qui constitue une "révélation d'informations sur l'état de santé".

L'article 9-1 du RGPD énonce une interdiction générale du traitement de données de santé, sauf si des exceptions s'appliquent. Ces exceptions incluent le consentement explicite de la personne concernée, l'exécution d'obligations légales dans le domaine de la santé, la protection des intérêts vitaux de la personne, etc.

Parmi les exceptions, le consentement explicite est souvent sujet à débat car il doit être libre, spécifique, éclairé et univoque. Dans le contexte médical, obtenir un consentement véritablement éclairé peut être complexe, en particulier lorsque la personne concernée n'a pas une pleine compréhension des implications.

Le champ d'application large de l'article 4-15 du RGPD englobe non seulement les données médicales traditionnelles, mais aussi les informations liées aux services de soins de santé. Cela peut inclure des données liées au suivi de la condition physique, aux habitudes alimentaires, etc. Cette large portée soulève des questions sur la vie privée et la sécurité des données. Le débat concernant les handicaps est important car certaines informations sur le handicap peuvent être interprétées comme des données de santé. Cela pourrait potentiellement poser des défis en termes de traitement de ces informations tout en respectant la confidentialité et la non-discrimination.

La nature juridique des données de santé dépend du contexte dans lequel elles sont collectées, traitées et utilisées ; mais repose également sur la multitude de textes qui encadre leur protection et qui sont susceptible de créer un flou juridique dans la manière dont de telles données seront appréhendées aussi bien par les établissements de santé que par les prestataires d'infogérance.

---

[88] CNIL : « qu'est-ce qu'une donnée de santé », https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante, consulté le 24 juillet 2023

[89] N. Martial-Braz, F. Jault-Seseke, « Données à caractère personnel – Cadre légal – Champ d'application matériel », *Répertoire IP/IT et Communication*, juillet 2019, n° 70 s. ; Ch. Féral-Schuhl, *Cyberdroit,* coll. « Praxis », Dalloz, 2021, n° 132.01 s.

Selon le Considérant 35 du RGPD : *« les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro ».*

La notion de données de santé donnée par la CNIL est désormais large[90]. Elle est à apprécier, au cas par cas, compte tenu de la nature des données recueillies et sur cette base les données de santé peuvent être classées en trois catégories :

- *« celles qui sont des données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.*
- *celles, qui du fait de leur croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la mesure de l'effort, etc.*
- *celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical »*[91].

La nature juridique des données de santé a des conséquences sur les conditions de leur traitement. En effet, le RGPD impose des obligations spécifiques aux responsables de traitement et aux sous-traitants qui traitent des données de santé, notamment en matière de base légale[92], de consentement[93], d'intégrité et de confidentialité[94], de droits des personnes concernées[95] et de transferts hors de l'Union européenne[96].

A cela s'ajoute les débats relatifs au principe d'interdiction de traitement des données sensibles[97] dont font partie les données de santé, prévu notamment par l'article 9-2 du RGPD, et ses dérogations aux contours encore flous et qui constituent des facteurs de risques juridiques dans le cadre de l'opération d'infogérance.

En effet, le RGPD prévoit sans équivoque que les traitements de données dites sensibles

[90] CNIL : « Qu'est-ce qu'une donnée de santé », https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante consulté le 24 juillet 2023.

[91] CNIL : « Qu'est-ce qu'une donnée de santé », https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante consulté le 24 juillet 2023.

[92] Art. 6-1 du RGPD. La CNIL précise que *« La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement ». https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales*

[93] Art. 6-1-a et art. 7 du RGPD.

[94] Art. 5-1-f et art. 32

[95] Droit à l'information (art. 13 et 14 du RGPD) ; Droit d'accès (art. 15 du RGPD) ; Droit de rectification (art. 16 du RGPD) ; Droit à l'oubli (art. 17 du RGPD) ; Droit à la limitation du traitement (art. 18 du RGPD) ; Droit à la portabilité des données (art. 20 du RGPD) ; Droit d'opposition (art. 21 du RGPD) ; Droit de ne pas faire l'objet d'une décision individuelle automatisée (art. 22 du RGPD)

[96] Art. 44 à 49 du RGPD.

[97] L. Maisnier-Boché, « Données de sante à caractère personnel. – Régime général », JurisClasseur Communication, Fascicule n° 945, 31 décembre 2019.

sont interdits. Cette interdiction se justifie notamment en raison de la nature de ces données et des risques potentiels sur la vie privée des personnes concernées. Cela repose sur le fait que les données dites sensibles sont des données éminemment personnelles qui sont susceptibles de conduire à des discriminations si elles sont révélées ou traitées pour des finalités ou selon des modalités ne garantissant pas à la personne concernée une protection de ses droits et libertés. C'est la raison pour laquelle le traitement de cette catégorie de données est par principe interdit[98].

Concernant les exceptions à ce principe d'interdiction de traitement des données sensibles, elles sont prévues aussi bien par le RGPD que par loi Informatique et libertés.
Le RGPD autorise le traitement des données sensibles dans des cas précis (RGPD, article 9, § 2)[99].

Quant à la loi Informatique et libertés, elle va au-delà de la liste des exceptions qui permettent de traiter des données sensibles, dans le cadre des marges de manœuvre laissées par le RGPD (L. n° 78-17, 10 janv. 1978, art. 44). Elle reprend bien sûr la liste des exceptions de l'article 9 du RGPD, mais y ajoute certains cas[100] :

A cette première liste de facteurs à risque, il faut ajouter les facteurs tenant au cadre dans lequel intervient l'exécution des obligations fixées par la loi ; à savoir le cadre contractuel.

2. Le cadre de l'atteinte : le contrat

La nature particulière du contrat d'infogérance est le point de départ d'un facteur de risque inhérent aux contours des délimitation contractuelles de l'intervention du prestataire d'infogérance, car en effet, il y a un lien direct et évident entre la manipulation des données de santé, la fraude informatique et la vulnérabilité du système dans la mesure où c'est le caractère illicite du traitement de cette donnée qui sera le point de départ de toute la réflexion.

La vulnérabilité est une *« faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser »*[101]. D'un point de vue de protection des données personnelles, la vulnérabilité est envisagée par le RGPD en ses articles 5-1-f (principe d'intégrité et de confidentialité)[102] ; article 32 (sécurité du traitement)[103], article 33 (notification des violations de données aux

[98] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulté le 24 juillet 2023.
[99] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulté le 24 juillet 2023.
[100] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulté le 24 juillet 2023.
[101] Glossaire de l'ANSSI : https://www.ssi.gouv.fr/entreprise/glossaire/v/ consulté le 24 juillet 2023.
[102] Ce principe stipule que les données à caractère personnel doivent être traitées de manière à garantir une sécurité appropriée. Il s'agit d'un principe fondamental en matière de protection des données qui souligne la nécessité de mettre en place des mesures techniques et organisationnelles pour prévenir le traitement non autorisé ou illicite, ainsi que la perte, la destruction ou les dégâts d'origine accidentelle des données. Cela permet de minimiser les risques de vulnérabilité en assurant que les données sont traitées avec une sécurité adéquate.
[103] Cet article détaille les mesures que les responsables du traitement et les sous-traitants doivent prendre pour garantir un niveau de sécurité approprié au traitement des données personnelles. Ces mesures comprennent, entre autres, la pseudonymisation, le chiffrement, la capacité à rétablir la disponibilité des données en cas d'incident, ainsi que des procédures régulières de test et d'évaluation de l'efficacité des mesures de sécurité. En mettant en œuvre ces mesures,

autorités de contrôle)[104] et article 34 (communication des violations de données aux personnes concernées)[105] déjà évoqués.

Le contrat d'infogérance est un contrat d'entreprise tel que prévu par l'article 1710 du Code civil[106] ; et en tant que tel il contient les germes de plusieurs facteurs à risque. Le premier étant la difficulté à délimiter strictement le cadre d'intervention du prestataire d'infogérance, et plus spécifique de son personnel. Il faut également préciser que ce type de contrat intervient à l'exclusion de tout pouvoir de représentation (c'est-à-dire qu'on ne saurait y voir un contrat de mandat). Si, classiquement, la prestation découlant d'un contrat d'entreprise concernait des actes matériels, il ne fait aujourd'hui aucune difficulté à considérer qu'elle puisse être intellectuelle *« les travaux d'ordre intellectuel ne sont pas exclus de la définition du contrat d'entreprise »*[107].

A cette disposition du Code civil relative à la portée générale du contrat de sous-traitance, il est primordial d'ajouter les obligations fixées par l'article 28 du RGPD. En effet, L'article 28 du RGPD traite de la relation entre les responsables du traitement (ceux qui déterminent les finalités et les moyens du traitement des données) et les sous-traitants (ceux qui traitent des données pour le compte des responsables du traitement). Cet article impose des obligations spécifiques aux sous-traitants en matière de protection des données personnelles. Les dispositions de cet article incluent la nécessité de conclure un contrat de traitement de données entre le responsable du traitement et le sous-traitant, qui doit contenir certaines clauses spécifiques pour garantir la sécurité et la protection des données personnelles.

La fraude informatique va consister en une intrusion non autorisée et dommageable dans le système informatique de l'établissement de santé. Cela signifie non seulement que l'intrusion ait été faite en dehors des termes du contrat, mais aussi qu'elle ait causé un dommage à l'établissement de santé et par ricochet aux personnes auprès vis-à-vis desquelles l'établissement de santé est considéré légalement comme le responsable du traitement des données.

Cet aspect permet d'opérer systématiquement une bascule sur les aspects pénaux d'une telle intrusion. En effet, et depuis très longtemps déjà, la loi du 5 janvier 1988[108] a été pionnière en matière d'infractions spécifiques aux technologies de l'information et ses dispositions forment encore le cœur de la matière. Les dispositions législatives de lutte contre les infractions liées aux technologies de l'information[109] répriment le fait :

---

les organisations réduisent considérablement la vulnérabilité des données aux menaces et aux risques.

[104] L'article 33 impose aux responsables du traitement de notifier les violations de données personnelles à l'autorité de contrôle compétente dans les 72 heures suivant la prise de connaissance de la violation, sauf si la violation n'est pas susceptible d'entraîner un risque pour les droits et libertés des personnes concernées. Cette disposition est cruciale pour atténuer les conséquences des violations de données et pour permettre aux autorités de prendre des mesures appropriées pour protéger les droits des personnes vulnérables dont les données ont été compromises.

[105] L'article 34 énonce que, dans certaines circonstances, les personnes concernées doivent également être informées des violations de données si ces violations risquent d'entraîner un risque élevé pour leurs droits et libertés. Cette communication permet aux personnes vulnérables de prendre des mesures pour se protéger contre les conséquences potentielles de la violation.

[106] Art. 1710 Code civil : « Le louage d'ouvrage est un contrat par lequel l'une des parties s'engage à faire quelque chose pour l'autre, moyennant un prix convenu entre elles ».

[107] Cass. 3e civ., 28 février 1984, n° 82-15.550 : *Bull. civ.* III, n° 51.

[108] L. n° 88-19, 5 janvier 1988 relative à la fraude informatique, JO 6 janv., p. 231.

[109] C. pén., art. 323-1 s.

- d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ;
- d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ;
- d'introduire frauduleusement des données dans un système de traitement automatisé ;
- d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient.

Ajouté à cela, il faut relever le fait que le contrat de sous-traitance informatique implique plusieurs obligations connexes qui rendent complexes la démarche de contractualisation.
Très concrètement il est pertinent d'évoquer les clauses de réversibilité, la clause d'audit obligatoire de l'article 28-3-h du RGPD. Les clauses de réversibilité sont des dispositions contractuelles qui visent à garantir que, en cas de fin de contrat ou de changement de sous-traitant, les données transférées au sous-traitant sont restituées ou transférées de manière sécurisée au responsable du traitement. Cela peut inclure des exigences concernant la remise des données, la suppression des données, la fourniture de copies des données, et ainsi de suite. Cependant, la mise en œuvre pratique des clauses de réversibilité peut être complexe, en particulier lorsque les données sont traitées sur plusieurs systèmes, dans différents formats, ou lorsqu'elles sont interconnectées avec d'autres données.

La réversibilité peut devenir problématique si le sous-traitant n'a pas une bonne documentation de l'emplacement des données, de leur format et des méthodes de traitement. Il peut également y avoir des coûts et des difficultés techniques associés à la migration ou à la restitution des données.

Par ailleurs, l'article 28-3-h du RGPD stipule que le contrat de traitement de données doit inclure une clause permettant au responsable du traitement de faire réaliser des audits par le sous-traitant ou par un auditeur tiers pour évaluer la conformité aux obligations du sous-traitant. Cela vise à garantir que le responsable du traitement puisse vérifier la conformité du sous-traitant aux exigences du RGPD. Cependant, l'application concrète de cette clause peut être complexe. Les audits peuvent exiger du temps, des ressources et une coordination étroite entre le responsable du traitement, le sous-traitant et l'auditeur tiers. De plus, il peut y avoir des préoccupations concernant la confidentialité des informations commerciales sensibles du sous-traitant. Néanmoins, cette clause est essentielle pour maintenir une surveillance adéquate et garantir que les données sont traitées conformément aux normes de sécurité des données.

S'agissant de l'Analyse d'Impact sur la Protection des Données (AIPD), il s'agit d'une évaluation des risques liés au traitement des données personnelles, exigée en vertu de l'article 35 du RGPD pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées. Dans le contexte de l'infogérance des systèmes d'information de santé, il est important de mener une AIPD pour identifier les risques liés aux données de santé et mettre en place des mesures pour les atténuer.

D'ailleurs, cette complexité aboutit à la difficulté de déterminer précisément la nature de l'obligation qui sera à la charge du prestataire d'infogérance. Comme le relève la doctrine juridique, la distinction des obligations de moyens et de résultat, *« plus*

maladroite que fausse »[110], n'a pas été consacrée par la réforme du droit des contrats. Elle continuera toutefois de jouer tout son rôle, notamment dans le contrat d'entreprise. Les éléments permettant d'aboutir à la solution sont l'activité, l'aléa, la volonté des parties et le rôle du client[111]. Dès lors que ces différents facteurs de risque ont été relevé, il apparait naturel d'analyser le régime de responsabilité lié à l'infogérance des établissements de santé.

[110] Ph. Malaurie, L. Aynès, Ph. Stoffel-Munck, *Droit des obligations*, LGDJ, 11e éd., 2020, n° 941.
[111] F. Labarthe, C. Noblot, « Le contrat d'entreprise », *JurisClasseur Contrats – Distribution*, Fascicule n° 425, 1er juillet 2021, n° 163 s.
[112] Cf. Riguidel Michel, ouvrage la sécurité des réseaux et des systèmes, 2006

Sécurité des réseaux dans les espaces OAPI et OHADA

Par Jeanine Tano-Bian
Docteure en droit, Consultante en cybersécurité
Enseignante-Chercheur Université d'Abidjan

Résumé

Partie intégrante du système d'informations, le réseau est à la fois un canal et un contenant. Il reçoit des données qu'il transporte. Il oblige dès lors à envisager la confiance des titulaires des droits attachés à ces données mais aussi leurs rapports à ce réseau. Il est aussi intéressant d'étudier les questions d'interaction des réseaux entre eux et par conséquent celle de l'interconnexion. Comment les Etats de l'OAPI parviennent-ils à assurer la sécurité des réseaux ? Quels outils technologiques et mécanismes juridiques sont prévus ? Les avancées technologiques invitent à passer en revue la sécurité des réseaux qui est fondamentale en termes de propriété intellectuelle. L'objectif de cette étude est de montrer les adaptations opérées par les Etats en matière de sécurité des réseaux grâce à des techniques liées à l'économie numérique.

Mots clés : Etats, OAPI, OHADA, réseaux, sécurité.

Introduction

La sécurité des réseaux est un domaine vaste et étendu qui implique la confidentialité, l'intégrité et la disponibilité. Selon la typologie de réseaux et de systèmes élaborée par Michel RIGUIDEL[112], il existe les réseaux informatiques[113], les réseaux de télécoms[114], les réseaux de diffusion de

[113] Les réseaux locaux d'entreprises, les réseaux de vidéosurveillance sur IP, Internet, les réseaux sans fil (WiMax, Wifi, Bluetooth), les réseaux passifs d'étiquettes intelligentes (RFID) ;
[114] Les réseaux satellites, les réseaux de localisation GPS ou Galiléo, les réseaux téléphoniques, les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, EDGE, UMTS)

télévision, les systèmes d'information de l'état, des institutions, des entreprises, des banques, des organisations, des réseaux à domicile (réseau domestique), de gestion des infrastructures critiques et du patrimoine numérique naissant des familles et des individus.

En appui de cette typologie, assurer la sécurité des réseaux c'est protéger un système d'information avec les activités qui s'y développent, la fonctionnalité dudit système ainsi que l'intégrité du réseau surtout celles des données qui y transitent par le biais des technologies matérielles et des technologies logicielles : les réseaux des systèmes d'information sont internes[115] et externes[116]. Dès lors, assurer la sécurité des systèmes d'information[117] exige de prévoir d'une part les attaques qui pourraient endommager lesdits systèmes et d'autre part de répondre aux attaques par des actes de défense et de réparation en cas de nécessité.
Les mécanismes mis en œuvre trouvent leur fondement dans des textes juridiques, élaborés la plupart du temps, à la suite des observations techniques. C'est dire qu'en la matière, l'appréhension technique de la sécurité, en d'autres termes l'action, précède l'encadrement de cette sécurité par les textes. L'activité technologique est en amont de l'élaboration des fondements qui encadrent les comportements préventifs et les conduites curatives à adopter. D'ailleurs, ce sont les attaques cybercriminelles récurrentes qui ont conduit les Etats à réfléchir sur des textes répressifs en la matière.

Le réseau, partie intégrante des systèmes d'information ne déroge pas à la règle. Plus précisément, la loi n°2017-20 portant code du numérique en République du Bénin[118] définit le réseau comme un ensemble connecté de systèmes informatiques, quel que soit leur mode de connexion. Les connexions peuvent être reliées à la terre, sans fil ou les deux. Il faut souligner qu'un réseau peut être géographiquement limité à une zone peu étendue ou couvrir une zone étendue et de tels réseaux peuvent eux-mêmes être interconnectés.

Comment la sécurité des réseaux est-elle envisagée par les Etats membres des espaces OAPI et de l'OHADA ?

Il peut apparaître audacieux d'étudier ces deux espaces ensemble mais à y regarder de près, ils s'entrecroisent et se recoupent : les Etats membres qui sont les mêmes 17 Etats membres de l'OAPI et de l'OHADA. Et il s'agit du Bénin, Burkina Faso, du Cameroun, de la Centrafrique, des Comores, de la République démocratique du Congo, de la Côte d'Ivoire, du Gabon, de la Guinée, de la Guinée Bissau, de la Guinée équatoriale, du Mali, de la Mauritanie, du Niger, du Sénégal, du Tchad et du Togo. C'est dans ce contexte que les Etats membres de l'Organisation Africaine pour la Protection de la Propriété

[115] Le réseau interne selon la loi béninoise est un réseau indépendant entièrement établi sur une même propriété, sans emprunter ni le domaine public y compris hertzien, ni l'espace atmosphérique, ni une propriété tierce.
[116] A l'instar de l'infogérance que l'Agence française de normalisation (AFNOR) définit comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définie.
[117] AKOKA Jacky, BRIOLAT, Dominique and COMYN-WATTIAU Isabelle (1998) "La Sécurité des réseaux : une approche de détection de malveillances," Systèmes d'Information et Management : Vol. 3 : Iss. 2, Article 2. Available at : http://aisel.aisnet.org/sim/vol3/iss2/2
[118] Loi disponible sur https://sgg.gouv.bj/doc/loi-2017-20/

intellectuelle sont au cœur des réflexions pour encadrer la sécurité des réseaux.

A la pratique, plusieurs textes[119] convergent en ce sens dans la mesure où l'activité de sécurisation des réseaux est multiforme et oblige les législateurs à prendre en compte tous les secteurs concernés.

Pour appréhender la sécurité des réseaux telle qu'elle est prévue par les Etats de l'OAPI sans trahir l'objectif fondamental de protection de la propriété intellectuelle, il convient de vérifier comment la sécurité des réseaux est assurée au point de vue de la prévention avant d'en apprécier l'effectivité structurelle. De cette approche il ressort que la sécurité des réseaux dans les espaces OAPI et OHADA tient compte de la technicité du domaine (I) qui semble l'exiger. En sus de cette technicité, les besoins structurels l'imposent *a posteriori* (II).

I- Une sécurité a priori exigée par la technicité du domaine

Dans l'élaboration des règles qui la régissent, la sécurité des réseaux semble emprunter un peu du droit international général tel que défini par COMBACAUD et SUR[120] dans le domaine répressif de la cybersécurité. La règlementation a surtout des aspects spécifiques propres au régionalisme comme le souligne TCHAMENI[121].Quel que soit le prisme choisi, la sécurité des réseaux implique la sécurité des accès au réseau. Ce qui renvoie à la sécurité des télécommunications dans leur disponibilité (1) et à la sécurité du transport de ces communication, qui elle suppose l'exploitation des réseaux. (2)

1. La disponibilité du réseau : un préalable indispensable

Le réseau est dit sécurisé dès lors qu'il est disponible. Cette disponibilité est assurée selon Solange GHERNAOUTI par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information[122]. L'accès au réseau est sécurisé grâce à la mise en place de mécanisme de *login* intégrant un identifiant et un mot de passe avec la précision de changer régulièrement ces mots de passe et en conserver la confidentialité. Cet aspect mêle à la fois la recherche de l'intégrité des informations tout en assurant leur caractère secret et in fine le caractère opérationnel d'un système qui fonctionne correctement sans faille.

Une des atteintes à la disponibilité est le déni de service. Il s'agit d'une attaque du système d'informations qui le bloque en empêchant les personnes d'y avoir accès ou encore en empêchant l'accès aux services offerts par le site ou l'interface consulté. Le fait que les Etats de l'OAPI prévoient des législations en vue d'incriminer et de punir ce genre de comportements répréhensibles portant atteinte à la disponibilité des réseaux constituent un gage de la sécurité de la disponibilité des réseaux.

[119] L'espace OAPI et OHADA seront mis en avant mais les textes convoqués pourraient être tirés notamment de code du numérique, de lois relatives à la cybersécurité, et non uniquement des textes de propriété intellectuelle et de droit des affaires. Ces derniers seront également convoqués mais en plus de textes plus spécifiques au domaine de la sécurité.

[120]Jean COMBACAUD et S. SUR, Droit international public, Paris Montchrestien 2012, P. 46

121 TCHAMENI, les évolutions du régionalisme africain, Paris, L'Harmattan, 2013, p.17 et s. voir également Dr. Abdulqawi A. YUSUF, Panafricanisme et droit international, édition Hague Academy Special, 2017.

[122] Cf. S. GHERNAOUTI, cybersécurité, analyser les risques, mettre en œuvre les solutions, 7e édition DUNOD

Un réseau est dit disponible dès lors que le service qu'il offre est opérationnel au cours d'une période précisée. En cela, Solange GHERNAOUTI souligne *qu'il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit (notion d'accessibilité). La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié et une certaine redondance ainsi que par une gestion opérationnelle et une maintenance efficace des ressources.*

En vue d'assurer la disponibilité des réseaux, la loi congolaise relative à la cybersécurité[123] en son article 1dispose qu'elle régit le cadre juridique national de sécurité des systèmes d'information et des réseaux de communications électroniques. A ce titre, elle vise notamment à organiser et coordonner la sécurité des systèmes d'information et des réseaux de communications électroniques. La suite des dispositions de cette loi prévoit un ensemble de mécanismes pour prévenir les risques éventuels et certains. En outre, l'article 27 de la loi congolaise relative à la cybersécurité dispose que « Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations ».

2. La sécurité de l'exploitation du réseau : contenu, corollaire nécessaire

L'exploitation des réseaux renvoie à son utilisation et par conséquent aux informations qu'il transporte, qui stocke, pour lesquelles il représente un canal. En effet, la sécurité de l'exploitation est relative, comme le souligne GHERNAOUTI, au *bon fonctionnement opérationnel des systèmes informatiques et des réseaux de télécommunication*. On y inclut la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.
Les contenus font appel aux applications et logiciels sollicités en vue de sécuriser les réseaux. Il apparaît à ce stade impérieux de se demander ce que prévoient les dispositions relatives à la propriété intellectuelle quant à ces outils de sécurité ? En effet, il est certes prévu de sécuriser un réseau mais les personnes productrices de ces outils de sécurité sont-elles assurées du point de vue de la propriété de leur invention ?

La protection des personnes ayant créé des outils de sécurité reste une question fondamentale pour garantir la sécurisation et éviter les risques de piratage ou de détournement. Cet aspect est relatif à la sécurité structurelle des réseaux qu'il convient d'aborder.

II. Une sécurité a posteriori structurelle

La sécurité des réseaux telle qu'appréhendée par les textes des Etats de l'OAPI ou de l'OHADA est structurelle dans la mesure où elle vise in fine des objectifs de compétitivité, de sécurité logique et de concurrence.

1. Des objectifs de sécurité pérennes et performants

Un réseau sécurisé est plus compétitif parce que plus attrayant. C'est pourquoi des sites

[123] Loi n°26-2020 du 5 juin 2020 relative à la cybersécurité publiée au JO 2020-23.

sécurisés seront plus productifs dans la mesure où les clients seront plus confiants par rapport aux propriétaires de ces sites offrant des espaces sans crainte. Ils seront certains de ne pas voir leurs informations dérobées notamment. La sécurité des réseaux s'érige en gage de confiance et devient un indicateur de mérite et d'excellence. Elle est de ce fait un avantage concurrentiel puisqu'elle représente désormais une force pour l'entreprise ou le site qui la garantit à ses visiteurs, clients ou simples prospects.

Etudier la force de la sécurité de ses réseaux passe par des indicateurs de performance. Le recours à des études comportementales des visiteurs de sites, de comptes ou de vitrines virtuelles permet de se rendre compte de l'importance de la sécurisation de la performance vendue sur toute la chaine de valeur.

La protection des logiciels et des bases de données[124] a connu une évolution relativement à son encadrement juridique. Cette protection juridique est assurée, dans l'espace OAPI par les droits d'auteurs et les droits voisins. Le texte de Bangui consacre la protection des bases de données et pose comme critère « le choix, la coordination ou la disposition des matières ». En termes de sécurité, il n'y a réellement pas de protection spécifique uniquement pour eux.[125]. La disposition des données et leur organisation dans la base indiquée plus haut est bel et bien la manifestation de l'originalité.

Outre cet exemple législatif ivoirien, le droit sénégalais envisage une protection à minima de la base de données. Mais, elle est restreinte à la structure et ne s'étend pas à la composition en tant que telle. Pour emboîter le pas à Elhadji Oumar Ndiaye[126]qui présente dans sa thèse la protection des bases de données en droit sénégalais, il est possible de regretter que le droit sénégalais n'ait pas saisi cette occasion pour protéger davantage le contenu des bases de données, qui en général sont le résultat de l'assemblage de critères qui leur donnent et leur confèrent une originalité Ce qui manque sans doute dans les lois africaines c'est une protection sui generis.

A cet effet, les critères varient selon les besoins pour lesquels les bases de données sont créées, ce qui explique qu'il n'est pas évident de retrouver les mêmes critères d'une base de données à l'autre. La composition en aurait dû être protégée valablement au même titre que sa structure.

En réalité, il faut noter que la protection est avant tout guidée par le transfert de

[124] Nathalie Mallet-Poujol, que « la base de données se trouve être, en effet, ou bien le simple réservoir de données, sur un support informatique, ou bien le réservoir de données ayant subi un travail d'indexation préliminaire ou encore le réservoir de fichiers de données, tout à fait structurés. C'est le "tout", c'est l'ensemble, l'entité "réservoir" qui caractérise la base de données » Nathalie Mallet-Poujol, « Protection des bases de données », JCL Propriété littéraire et artistique, Fasc. 6080, n° 20

[125] La jurisprudence acceptait déjà depuis longtemps de protéger la structure originale d'un recueil dont le contenu n'était pas protégé par le droit d'auteur. Il a été jugé en effet que « le fait de réunir ces données en un ensemble ordonné et complet, de les classer en diverses nomenclatures constitue une œuvre personnelle » 95. Plus récemment aussi, dans son jugement du 28 décembre 1998, le tribunal de grande instance de Lyon a considéré comme œuvre protégeable un recueil de conventions collectives au motif que « les arrangements, la présentation, la mise en page utilisée rendent la consultation du « Dictionnaire Permanent » (le recueil) plus simple et plus attractive que l'originale : pour des cas en France, voir Cass. 1re civ., 9 nov. 1983 : JurisData n° 1983-702217 ; JCP G 1984, II, 20189, note A. Françon. - Cass. ass. plén., 30 oct. 1987, n° 86-11.918 : JurisData n° 1987-001712 ; JCP G 1988, II, 20932, rapp. X. Nicot et note J. Huet ; JCP E 1988, II, 15093, obs. M. Vivant et A. Lucas ; D. 1988, p. 21, concl. J. Cabannes ; RTD com. 1988, p. 57, obs. A. Françon 95 CA Paris, 18 déc. 1924, Didot-Bottin, à propos de données compilées à partir de l'annuaire téléphonique.

[126] Elhadji Oumar Ndiaye, La protection des bases de données par le droit d'auteur : approche comparative entre le droit français et le droit sénégalais. Droit. Université Montpellier ; Université de Saint-Louis (Sénégal), 2017. Français.

compétences[127]. Sur la base du transfert de compétences technologiques, la répartition des droits d'auteur sur une base de données ou un logiciel dépendra du niveau de liberté du logiciel dont il est question[128]. Ainsi, s'agissant de la production ou la création des applications, plusieurs algorithmes préétablis ou créés par des firmes de renom disposant de brevet ou mettant à disposition des licences d'exploitation sont utilisés, en tant qu'emprunt à des créations antérieures. Ces créations antérieures selon qu'elle soit des logiciels libres ou duplicable auront une protection à minima. Cette considération ne facilite pas la protection spécifique des logiciels créés dans ce cadre.

S'agissant de la sécurité logique, elle fait référence à la protection des données et à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes et des services offerts. La qualité et la sécurité des développements logiciels et des tests de sécurité, une mise en œuvre adéquate de la cryptographie pour assurer intégrité et confidentialité des données. Des procédures de contrôle d'accès logique et d'authentification. L'ensemble de ces dérivés de la sécurité logique précisés par Solange GHERNAOUTI, permettent d'appliquer les dispositions relatives à la sécurité des réseaux et de manière spécifique facilitent l'atteinte des objectifs de sécurisation : elles garantissent la confidentialité des données et leur intégrité.
Pour que la sécurité structurelle soit complète, la définition des niveaux de responsabilité ainsi que l'identification des acteurs dans cette sécurisation des réseaux est réalisée par les Etats de l'OAPI.

2. Des acteurs à la responsabilité précisément définie : une responsabilité proportionnelle aux acteurs

En la matière, le Cameroun prévoit dans la loi de 2010 qui régit la sécurité des réseaux avec une politique générale de sécurité électronique. Sur le fondement de cette politique le Cameroun sépare l'Agence Nationale des Technologies de l'Information[129] et de la Communication de l'Agence de Régulation des Télécommunications.

Au Congo, le code du numérique distingue les parties prenantes principalement les autorités en charge de la sécurité des réseaux entre autorité de régulation du numérique, autorité nationale de certification électronique et conseil national du numérique. Elles ont chacune des missions coercitives ou consultatives. C'est à ce titre notamment qu'il est possible de mentionner que les réseaux sont assujettis à des exigences de surveillance des risques, ce sont des obligations contenues dans la loi congolaise portant cybersécurité[130]. A ce titre, elle prévoit par exemple en son article 12 que : « *Les systèmes d'information et les réseaux de communications électroniques relevant des divers organismes publics sont soumis à un régime d'audit obligatoire et périodique de la sécurité des systèmes d'information* ». Il faut souligner que l'audit

[127] Raoul EHODE ELAH Tourere ZENABOU Victorine Ghislaine Nzino MUNONGO, le droit de propriété intellectuelle et le transfert de technologie, *Revue* Valaque d'Etudes Economiques, *Volume 5(19) N °1. 2014*

[128] Saerens Patrick, Les créateurs, maillons faibles des Tic en Afrique ? N° 15/2B – Supplément 2014 Tic, industries culturelles et industries créatives : Appropriation sociale et diversité culturelle Communication & Changements sociaux en Afrique 3° Colloque international Douala, 10 au 12 avril 2014

[129] Loi N°2010-12 du 12 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

[130] Loi n°26-2020 du 5 juin 2020 relative à la cybersécurité (JO 2020-23)]

obligatoire et périodique de la sécurité des systèmes d'information est une technique de sécurité qui emprunte plusieurs formes notamment par des tests d'intrusion[131]. Elle est une obligation de sécurité mise à la charge des fournisseurs d'accès et des exploitants de système d'information.

Au Bénin, le code du numérique prévoit des dispositions transversales avec une sécurité de type 360 degré depuis la constitution du système jusqu' à ses usages et les atteintes : non seulement du fait des usagers mais aussi des interconnexions[132] et des atteintes venant de l'extérieur du réseau.

Le fait pour les législateurs africains[133] de prévoir des responsables en matière de sécurité est assorti de sanctions en cas de non-respect des obligations prévues. Ces exigences confèrent un caractère contraignant à la sécurisation des systèmes et par voie de conséquence des réseaux de télécommunications et des réseaux numériques.

Conclusion

La sécurité des réseaux dans les espaces de l'OAPI et de l'OHADA est assurée en termes de sécurité du réseau en amont par des législations en construction et en aval par des applications pratiques en chantier. Beaucoup des législations élaborées sont au stade de l'expérimentation à l'instar des technologies numériques.

L'encadrement juridique pour atteindre des objectifs de sécurité à la fois des systèmes d'information et de leurs composantes ainsi que des données qui transitent par ces réseaux forcent à observer et à assurer la disponibilité desdits réseaux. Pour corollaire, cette disponibilité à la confidentialité mais aussi l'intégrité des données ou informations transportées comme gage de sécurité.

Les Etats gagneraient à renforcer leur coopération dans la mesure où des instruments communautaires comme l'OAPI et l'OHADA permettent d'assurer la mutualisation des enjeux et des objectifs de sécurité. Parvenir à atteindre la sécurisation effective et totale pour endiguer la cybercriminalité et la haute criminalité numérique est une garantie qui couvre non seulement les économies nationales mais aussi les investissements dans le numérique en faveur de l'Afrique.

J.T.-B.

---

[131] Jonathan Tournier, François Lesueur, Frédéric Le Mouël, Laurent Guyon, Hicham Ben-Hassine. Audit d'un système IoT par test d'intrusion. RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, May 2018, Nancy, France. pp.1-3. ffhal-01937223f

[132] Cette notion est définie comme la liaison physique et logique des réseaux ouverts au public, exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou bien d'accéder aux services fournis par un autre opérateur, voir à ce sujet N. COLIN et al., « Économie numérique », in Notes du conseil d'analyse économique 2015/7 (n° 26), pp. 1-12. [Https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2015-7-page-1.htm] cité par Hervé Martial TCHABO SONTANG, in Les piliers juridiques du développement de l'économie numérique au Cameroun.

[133] Toutes les législations des Etats convoqués ont une partie réservée aux sanctions des opérateurs ou fournisseurs en cas de non-respect de leurs obligations.

Entrée en vigueur attendue : la convention sur la cybersécurité de Malabo

Par Jeanine Tano-Bian & Christian Kpolo
Docteurs en droit, Chercheurs, Université d'Abidjan

Depuis quelques semaines, les réseaux sociaux et forums d'information spécialisées scandent la ratification de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel. ENFIN ! est-on tenté de compléter. En effet, c'est le 27 juin 2014 que l'Union Africaine représentée par ses Etats membres a adopté ladite Convention à Malabo[134].

Il est reproché aux Etats africains de n'avoir pas de textes (uniformes ou harmonisés) régulant la sécurité du numérique. La sphère des scientifiques, des chercheurs et mêmes des professionnels se plaignent des insuffisances de décisions de justice en la matière ainsi que d'autres inconvénients liés à une relative lente prise de conscience des risques liés au tout digital.

Il faut le souligner, la ratification de la Convention de Malabo a mis un certain temps : presqu'une dizaine d'années. Le nombre de ratifications attendu, au niveau des Etats membres n'étant pas encore atteint jusqu'à récemment. Or, la Convention n'exigeait comme condition à sa ratification que la signature de quinze (15) pays[135]. Parmi celles-ci, il est traditionnellement prévu un nombre minimum de ratifications. Aucune autre condition n'était exigée. Pour plus de précisions, la Convention de Malabo s'appliquera dans les Etats suivants : Angola, Bénin, Cap-Vert, Côte-d'Ivoire, Ghana, Ile Maurice, Mauritanie, Mozambique, Namibie, Niger, République démocratique du Congo, Rwanda, Sénégal, Togo et Zambie.

En cette année 2023, il est permis de se réjouir de l'entrée en vigueur de cette Convention. Il faut également mentionner qu'adopter la Convention sur la cybersécurité est partie intégrante de l'agenda 2063 de l'Union Africaine[136].

Désormais, il est possible de faire cas d'un instrument régional africain de lutte contre la cybercriminalité dans la mesure où ce texte contient certes des dispositions pour la prévenir mais il est par ailleurs relatif à la sanction des actes cybercriminels et prévoit en outre la régulation de la protection des données à caractère personnel, terreau de toutes les exactions commises contre et via les réseaux numériques.

D'autres avantages comme la célérité des procédures pourront être cités en faveur de cette ratification de la Convention de Malabo. En outre, elle devient l'instrument régional africain qui facilitera la contextualisation non seulement des infractions qui surviendraient mais également celle d'une coopération judiciaire et juridique transfrontalière efficace. La question du nombre aussi peu élevé des Etats ayant ratifié la Convention conduit à s'interroger sur la place qu'occupe cette problématique de cybersécurité dans les gouvernances des Etats africains.

J.T.-B. & Ch.K.

---

[134] La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.

[135] L'article 36 de la convention dispose que : « la présente Convention entre en vigueur trente (30) jours après la réception, par le Président de la Commission de l'Union africaine, du quinzième (15ème) instrument de ratification ou d'adhésion ».

[136] Projets phares de l'agenda 2063 | Union africaine (au.int)

Les obligations de cybersécurité des acteurs : analyse des dispositions relatives à la cybersécurité dans la nouvelle loi de la République démocratique du Congo sur le numérique

Par Jeanine Tano-Bian & Christian Kpolo
Docteurs en droit, Chercheurs, Université d'Abidjan

La cybersécurité est l'ensemble des politiques, des mécanismes, des applications élaborées en vue d'atteindre un réel état de sécurité des systèmes d'information et des réseaux y affairant. Elle est devenue une norme de compétitivité, un gage de confiance dans le numérique et une valeur pour les économies mondiales. Les défis répressifs des Etats face à la cybercriminalité ne suffisent plus ; ces derniers doivent être de plus en plus avenants par des mécanismes d'anticipation et de prévention, et ce dans tous les secteurs d'activité. Dès lors, chaque Etat élabore une politique de sécurité de ses espaces de télécommunications et de transfert ou de transport de ces données.

Comment le Congo envisage-t-il la cybersécurité en intégrant toutes les parties dans son dispositif préventif et défensif ?

Cet espace dédié est l'occasion d'étudier à la lumière de la loi congolaise relative à la cybersécurité et de l'ordonnance-loi 23/10 du 13 mars 2023 portant code du numérique comment la République du Congo intègre ses parties prenantes au cœur de leurs activités respective à la cause de la cybersécurité.

La législation congolaise avec la loi n° 26-2020 du 5 juin 2020 relative à la cybersécurité s'est assignée pour rôle la mise en œuvre des actions garantissant la sécurité des réseaux et des systèmes d'information. Elle met des obligations à la charge de toutes les parties prenantes de la sphère économique et sociale.

La politique d'application de ces dispositions vise à éradiquer la cybercriminalité ainsi que tous les comportements répréhensibles ou en faveur de la criminalité numérique. Pour fil conducteur, la loi congolaise portant cybersécurité catégorise les parties prenantes d'une part et définit les niveaux de responsabilité en y associant des sanctions en cas de non-respect des obligations.

Ainsi, dans le texte relatif à la cybersécurité, la loi met en place des mécanismes pour prévenir les systèmes d'informations du phénomène criminel. Ce corpus de règles de prévention et d'anticipation propose des mesures en guise de réparation des failles créées par les attaques.

Les articles 4 et 5 de la loi congolaise de cybersécurité mettent à la charge de quiconque une obligation de sécurité, de prendre les mesures adéquates pour protéger et prévenir tout risque encouru par les tiers du fait de cet usage. Ces dispositions citent explicitement les entreprises en les qualifiant d'entité.

Il est possible d'analyser cette formulation au sein des personnes morales pouvant engager leur responsabilité au regard de l'étendue des risques envisagés par l'usage des canaux de communication et d'échange mis à disposition du public. L'anticipation des risques dans l'usage des systèmes et réseaux d'information est d'abord de la responsabilité de l'usager.

Ensuite, sa responsabilité pour détecter et répondre aux incidents de sécurité est également soulignée dans l'article 5 dès lors qu'il développe fournit, gère, maintient ou

utilise des systèmes et réseaux. A ce stade, la responsabilité est plus accentuée : il devient responsable et comptable (garant) de la sécurité et, est, par ailleurs tenu d'examiner et d'évaluer en permanence ses propres politiques, pratiques, mesures et techniques de manière à s'assurer qu'elles soient adaptées à ses différentes interfaces d'intervention. Il est donc responsable de la conformité de son système d'information. En d'autres termes, la conformité qui est une qualité supérieure attendue, renvoie à un ensemble de démarches responsabilisant les entreprises grâce à des obligations spécifiques à la fourniture, la gestion,

De ces dispositions, le législateur congolais entend encadrer les Comportements et précise ainsi les obligations à la charge des entreprises : les impératifs de sécurité sont pris en compte et on y entrevoit notamment le traitement des informations, et des données sont la disponibilité, la confidentialité et l'intégrité doivent être garanties et conservées. Par ailleurs, le respect des intérêts légitimes des autres usagers et détenteurs des systèmes et réseaux d'information est à assurer. Pour emprunter des analyses à la France, notamment à la Commission Nationale de l'Informatique et des Libertés (CNIL), l'intérêt est légitime si trois conditions cumulatives sont réunies : qu'il soit manifestement licite, déterminé de façon suffisamment claire et précise et qu'il soit réel pour l'organisme concerné, et non fictif.

Les mécanismes contenus dans la loi congolaise sont réalistes et techniques de sorte que cette loi est avant-gardiste et précise dans ses termes les préalables à la sécurité : elle traite de l'amont c'est-à-dire de la prévention des actes qui pourraient constituer des infractions.

Le législateur congolais est dans une logique concrète de culture de cybersécurité : elle opère une auto-régulation des acteurs. En ce sens, les entreprises et les pouvoirs publiques adoptent une gestion de sécurité axée sur l'évaluation des risques. Cette évaluation des risques concerne non seulement les niveaux des activités mais intervient également dans tous les aspects des opérations des entreprises et les pouvoirs publics.

Ils devront mettre en œuvre les moyens nécessaires en vue d'atteindre le degré de sécurité numérique souhaité en premier lieu grâce à l'autorégulation). Ce qui inclut, par anticipation, les réponses aux menaces identifiables ou prévisibles ainsi que la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit.

L'article 8 de la loi congolaise fait peser la responsabilité de cette évaluation des risques sur les entreprises et il tient compte des préjudices aux intérêts d'autrui ou causé par autrui, rendus possibles par l'interconnexion des systèmes d'information.

Fort de ces dispositions, il apparaît possible de se prémunir des actes de cybercriminalité, même si la réparation des dommages quand ils se produisent reste quasiment impossible.

J.T.-B. & Ch.K.

Les dispositions relatives à la responsabilité des intermédiaires techniques dans la nouvelle loi de la RDC sur le numérique

Par Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APIA

Dans ce texte, dense et foisonnant, le législateur de la RDC a régi les aspects numériques de l'économie. Le texte porte autant sur les données à caractère personnel[137], la cybersécurité, la cybercriminalité[138], les atteintes au droit de propriété intellectuelle que le commerce électronique. S'agissant du commerce électronique, la nouvelle loi congolaise porte sur la liberté de commerce, sur les contrats[139] et sur la responsabilité des acteurs du commerce électronique. Dans le cadre de la présente chronique, seules seront évoquées, brièvement, les dispositions relatives à la responsabilité des acteurs du commerce électronique.

C'est dans un titre consacré à la sécurité des systèmes informatiques que sont insérées les dispositions relatives à la responsabilité des acteurs du commerce électronique, plus précisément dans un chapitre intitulé obligations générales et spécifiques[140].

Tout d'abord, une section intitulée obligations générales énumère les obligations qui pèsent sur le fournisseurs d'accès à Internet et le fournisseur de services en ligne. On peut y constater une parenté avec la *Loi pour la confiance dans l'économie numérique* (France). En effet, le texte de la RDC prévoit qu'il ne pèse sur ces acteurs aucune obligation générale de surveillance (art.286) mais qu'ils doivent lutter contre certaines infractions spécifiques (art.287).

Les fournisseurs d'accès à Internet et les fournisseurs de services en ligne doivent, selon la loi de la RDC, observer une obligation d'identifier les utilisateurs de leurs services. Aux termes de l'article 284 de la loi de la RDC relative au numérique prévoit que le fournisseur d'accès à Internet et le fournisseur de services en ligne « *n'engagent pas leur responsabilité civile et/ou pénale du fait des activités ou des informations stockées à la demande d'un destinataire de leurs services, s'ils n'avaient pas effectivement connaissance de leur caractère illicite ou […] si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces données ou en rendre l'accès impossible* ». Ainsi, les fournisseurs d'accès à Internet et les fournisseurs de services ne sont a priori pas responsables des contenus qu'ils transportent. Ils ne peuvent voir leur responsabilité que si après en avoir été informés, ils ne retiraient pas promptement le contenu dont le caractère illicite leur a été notifié.

S'agissant de la notification du contenu illicite, le texte de la RDC s'éloigne aussi bien de la loi française que d'autres textes africains (Code béninois du numérique par exemple). En effet, alors que d'autres lois africaines, comme la loi française, citent des conditions

[137] V. la chronique de A. Ngoue et I. Randrianirina à paraître
[138] V. la chronique de Ch. Kpolo et J. Tano-Bian ci-dessus
[139] V. la chronique de R. Mabouana à paraître
[140] Loi de la RDC sur le numérique, art. 281 et s.

cumulatives permettant de présumer la connaissance du contenu illicite par le fournisseur d'accès à Internet (ou par le fournisseur d'hébergement), le texte de la RDC cite des conditions alternatives. On peut y lire : *« la connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il lui est notifié l'un des éléments suivants*[141] *: 1. la date de la notification […] ».* A titre de comparaison on relèvera, par exemple, que le Code béninois du numérique dispose[142] : *« la connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il lui est notifié les éléments suivants* [143].

La rédaction du texte de la RDC laisse perplexe car son application pourrait poser des problèmes pratiques. Comment, par exemple présumer qu'un intermédiaire technique est informé de la présence d'un contenu illicite au seul motif qu'il aurait reçu l'identité d'un titulaire des droits, y compris s'il n'a pas précisé le contenu qui doit être retiré. L'interprète est alors enclin à supposer qu'il s'agit d'un *lapsus calami.*

Après la section consacrée aux obligations générales, la loi de la RDC envisage des obligations spécifiques. Celles-ci concernent les fournisseurs de cache (art.290), les fournisseurs de liens hypertextes (art. 291), les fournisseurs de moteurs de recherche (art.292) et les fournisseurs d'hébergement (art. 293).

Concernant le fournisseur de cache, sa responsabilité est engagée s'il intervient sur le contenu ou si après avoir été informé de la présence d'un contenu, il ne le retire pas (promptement) ou ne le rend pas promptement inaccessible.

Le fournisseur de liens hypertextes, comme le fournisseur d'hébergement, engage sa responsabilité s'il ne supprime le contenu litigieux à la suite d'une injonction des autorités judiciaires ou administrative ou « *s'il n'a pas pris connaissance ou conscience d'informations illégales spécifiques stockées ou des activités illégales qu'exerceraient les destinataires de leurs services, autrement que par une injonction de l'autorité judiciaire* ». Le fournisseur de liens hypertextes ou l'hébergeur qui ne pouvait être au courant du caractère illicite d'un contenu ne peut en être responsable.

S'agissant spécifiquement du fournisseur de liens hypertextes, il n'est pas non plus responsable, précise le texte, s'il *« n'a pas informé rapidement les autorités judiciaires pour leur permettre d'évaluer la nature des informations ou des activités et, si nécessaire, d'ordonner le retrait du contenu ».* Le fournisseur de cache doit informer les autorités qui jugeront de l'opportunité du retrait du contenu signalé comme illicite. Cette obligation n'est pas reprise concernant les fournisseurs d'hébergement sans qu'on comprenne ce qui justifie sur ce point la différence entre la responsabilité des fournisseurs de liens hypertextes et celle des fournisseurs d'hébergement.

Le moteur de recherche est responsable, s'il est à l'origine de la transmission du contenu litigieux, ou s'il sélectionne les destinataires, ou encore s'il modifie le contenu en question. Dans l'ensemble, le législateur a fait le choix d'un régime particulièrement allégé de responsabilité des acteurs du commerce électronique. Il semble alors à contre-courant du mouvement de responsabilisation (qu'il faut relativiser) observé dans la législation de l'Union européenne.

Y.L.N.

[141] Nous soulignons
[142] Art. 498
[143] Nous soulignons

Revue de l'actualité des données à caractère personnel en Afrique

Par Aline Mbenoun-Ngoué
Juriste docteur en Droit privé et droit de la propriété intellectuelle
Conseil à l'OAPI et certifiée DPO (RNCP)
Chargée d'enseignement à l'Université de Lyon

Renforcement de la législation africaine en droit des données à caractère personnel

Nous saluons l'arrivée de deux nouvelles législations. Il s'agit de la Loi sur la Protection des Données Personnelles déjà publiée depuis 2022 et entrée en vigueur le 1er mai 2023 de la Tanzanie d'une part et de l'ordonnance-loi n°23/010 du 23 mars 2023 portant CODE DU NUMERIQUE en République Démocratique du Congo d'autre part. Néanmoins, seule l'Ordonnance -loi de la République Démocratique du Congo que nous présentons brièvement dans le cadre de cette publication.

C'est une approche globale qui est retenue dans ce nouveau dispositif législatif. Le législateur de la République Démocratique du Congo se rapproche ainsi du législateur Camerounais et se différencie par exemple du législateur Sénégalais (Voir la RSPIA avril 2023). Cette approche globale se caractérise par l'intégration de la protection des données à caractère personnel qu'elle désigne « Données Personnelles » dans un texte qui s'applique à plusieurs activités en lien avec le numérique. Néanmoins, dans le cadre de l'ordonnance -loi du 23 mars 2023, cette approche globale est plus forte car la protection des données à caractère personnel n'est pas expressément mentionnée dans le champ d'application du texte. Il est précisé dans le chapitre 1 article

1 que : « (…) la présente ordonnance -loi s'applique :
1.aux activités et services numériques ;
2.aux écrits, outils électroniques et prestataires de services de confiance ;
3.aux contenus numériques ;
4.à la sécurité et à la protection pénale des systèmes informatiques.

En outre, elle fixe le régime fiscal, parafiscal, douanier et de change applicable aux activités et services numériques en République Démocratique du Congo. »

C'est au chapitre 2 article 2 (intitulé Définitions) alinéa 30 que la notion de données personnelles intègre le texte par une définition. Il s'agit de : « toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement ». Cette définition se rapproche par exemple de celle de **L'Acte Additionnel A/SA.0/01/10/ du 16 février 2010 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.**

Dans ce texte régional la donnée à caractère personnel est **: «** : « toute information relative à une personne physique identifiée ou identifiable directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale, économique ». Certaines notions nouvelles sont prévues comme la notion de Donnée publique définie à l'article 2 alinéa 31 :« **Donnée publique** : donnée produite et stockée dans les registres publics de données sur le territoire de la

République Démocratique du Congo dans le cadre d'une mission de service public par l'Etat, les provinces, les entités territoriales, les services, établissements et organismes publics ainsi que les personnes morales de droit privé chargées d'une mission de service public ».

L'ensemble des dispositions relatives à la protection des Données personnelles est prévu de l'article 183 à l'article 270 du nouveau texte. Cette législation est assez complète car elle prévoit un cadre institutionnel complet avec la création d'une Autorité de la protection des données (APD) « (…) Une autorité administrative indépendante dotée de la personnalité juridique et jouissant d'une autonomie administrative et financière ». Cette Autorité de protection est dotée de compétences (article 262 et suivants) ; elle est par ailleurs constituée de trois organes avec des compétences précisées aux 'article 264 et suivants : « Les organes de l'Autorité de protection de données sont :
1. L'Assemblée planièdre ;
2. Le Bureau ;
3. Les Commissions permanentes (…) ».

La nouvelle législation de la République Démocratique du Congo prévoit des dispositions plus complètes que certaines lois nationales des pays africains. Elle présente en cela un grand intérêt. Une analyse de ce texte est prévue pour le prochain numéro de la RSPIA.

A.M.N.

ACTIVITES ACADEMIQUES

RECENSION DE TRAVAUX SCIENTIFIQUES

Par Ampah JOHNSON-ANSAH
Chef du Département de Droit Privé
Université de Lomé (Togo)

Éric MONTCHO-AGBASSA
Agrégé des Facultés de droit,
Université de Cotonou (Bénin)

Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APIA

AKPAH Ayélé Edwige

La ZLECAF et la libre circulation des biens intellectuels

Mémoire Master droit de l'entreprise, Institut supérieur de droit et d'interprétariat, Université de Douai, 2022

Madame AKPAH s'est donnée pour tâche d'entrevoir comment la libre circulation des biens intellectuels va s'opérationnaliser dans le nouvel espace africain formant une zone de libre-échange continental. La création d'un tel espace pourrait supposer une automaticité de la libre circulation des produits incorporant les droits de propriété intellectuelle. Toutefois, l'expérience européenne nous montre clairement que la mise en place d'un marché commun gouvernée par la libre circulation des biens, des personnes et des capitaux n'équivaut pas toujours mécaniquement à celle des biens intellectuels. Chacun sait que c'est le mécanisme de l'épuisement des droits qui peut se résumer en la distribution des biens intellectuels qui a permis de répondre à cette problématique d'une manière plus ou moins efficace. Cette question se posera dans des termes certainement différents en droit africain pour la simple raison que l'Afrique n'est pas encore un grand marché de biens intellectuels. C'est d'ailleurs l'un des axes de ce mémoire telle que l'a bien souligné Madame AKPAH.

En effet, selon l'auteur du mémoire, un gros bémol doit être mis sur l'automaticité de la libre circulation des biens incorporant les droits de propriété intellectuelle. Elle fait notamment appel à ce mécanisme de l'épuisement des droits de propriété intellectuelle comme pouvant permettre, en rapport avec celle de la ZLECAF, de nuancer cette automaticité de la libre circulation de ces droits. Et ceci en comparaison avec l'Europe où le marché commun a été institué dans les années 1950 sans qu'il n'y ait pour autant une libre circulation de ces produits spéciaux qui dérogent relativement au droit commun de la libre circulation. Au contraire, il a fallu un processus de lecture et e compréhension de l'objet spécifique et la fonction essentielle de chaque droit pour organiser la libre circulation à partir de l'épuisement intracommunautaire. La question se posera encore de fait de la permanence de la territorialité des droits de propriété intellectuelle et des modes non harmonisés de l'épuisement sur l'ensemble du continent.

Certains pays ont souscrit à un épuisement national, d'autres à un épuisement international qui constitue également une sorte de flexibilité à l'instar de l'OAPI depuis l'acte de Bamako de 2015. Cette impossibilité d'une libre circulation automatique peut entraîner une résistance des titulaires à l'épuisement de leurs droits. Il faudrait alors compter sur les juges africains pour la vaincre comme les juges européens qui ont conditionné la libre circulation des produits incorporant les droits de propriété intellectuelle à certaines exigences fondamentales telles que le consentement et la mise sur le marché des produits dans l'espace européen.

La ZLECAF ne doit pas ignorer cette philosophie dans la mise en œuvre de la libre circulation des biens intellectuels. Malgré le fait continental qui l'entoure, le mode d'épuisement souhaitable pour les biens intellectuels semble être l'épuisement international. Les marchandises de contrefaçon doivent être exclues du périmètre de l'épuisement et les contrôles aux frontières renforcées. On ne peut que souscrire à la conclusion de ce mémoire qui relève qu'« *une nouvelle ère s'ouvre pour le continent africain et il paraît important de mesurer les enjeux de cette forte initiative pour en tirer un maximum de profits dans l'intérêt des populations africaines* ».

A.J.A.

EKUE Foli Fabrice Crédus

Le droit pénal de la contrefaçon des droits de propriété industrielle dans l'espace OAPI

Mémoire de Master Droit Privé, Université de Lomé, 2021

Le mémoire de Monsieur Ekoué Folly Fabrice révèle le problème de la force dissuasive du droit pénal en droit de propriété intellectuelle. Ce constat est conforté par le renforcement des sanctions de la contrefaçon opéré par l'acte de Bamako, qui renouvelle l'expression de la force dissuasive du droit pénal de la contrefaçon. Il remet le droit pénal au cœur de la lutte anti-contrefaçon. À juste titre, l'auteur relève que la seule édiction de sanctions pénales est insuffisante. Il faut d'une part que les victimes recourent fréquemment au droit pénal de la contrefaçon et d'autre part, que les sanctions prévues soient réellement appliquées. Les victimes seraient ainsi encouragées par les résultats satisfaisants de la voie pénale.

En dehors du désintérêt des victimes, la rareté de la sanction pénale de la contrefaçon, dans le contexte africain résulte également de la faiblesse des moyens mis en œuvre pour faire respecter les droits de propriété industrielle. L'absence de moyens de mise en oeuvre des lois rend hypothétique le respect des droits des titulaires. Dans ce cas, l'auteur soutient que l'effectivité de la protection des droits de propriété industrielle a un enjeu économique fort : l'affluence d'investisseurs étrangers, très attentifs à l'environnement juridique et judiciaire des États. Il fait par ailleurs du juge un acteur décisif de la lutte. Il devrait relayer, à travers ses décisions, le message de fermeté du législateur vis-à-vis de la contrefaçon. Au-delà de l'amélioration du cadre institutionnel et juridique, il semble opportun d'adopter d'autres stratégies anti-contrefaçon. La lutte contre la contrefaçon ne peut prospérer sans une meilleure acceptation sociétale de la propriété industrielle. La population au sein de l'OAPI aurait une appréhension limitée de la dimension économique et même sociale des droits de propriété industrielle. Pour l'auteur, la précarité joue un rôle important dans la situation actuelle des pays de l'OAPI à l'égard de la contrefaçon.

Elle favoriserait le recours massif à des produits de contrefaçon dangereux pour la santé de l'homme, notamment les médicaments. Il faudrait donc procéder par des sensibilisations sur les dangers avérés de la contrefaçon pour l'économie, l'emploi, la sécurité des États et surtout la santé. Il en induit que la lutte contre la contrefaçon doit passer par la responsabilisation des différents acteurs impliqués dans le circuit de contrefaçon principalement relativement aux produits contrefaisants qui portent une atteinte directe à la vie humaine, notamment les médicaments. La responsabilisation apparaît donc comme un concept moralisateur, une responsabilité d'ordre moral qui consiste à faire prendre conscience aux acteurs du commerce de contrefaçon de la nécessité de préserver l'intérêt général.

Au-delà de cette sensibilisation qui a d'ailleurs peu de chose à avoir avec la propriété industrielle, il montre que la volonté du législateur de combattre la contrefaçon rencontre divers obstacles qui ne favorisent pas l'émergence de l'action pénale avant de conclure avec ce constat amer que « la contrefaçon, action hybride est frappée d'hémiplégie. Elle devient unijambiste car l'action pénale est pratiquement délaissée ». Espérons que le cri de détresse de l'auteur sera entendu par les

praticiens de la matière et qu'ils chercheront également la répression des actes de contrefaçon pour restaurer pleinement le champ pénal ainsi que les droits des titulaires et surtout afin que la contrefaçon soit véritablement prise au sérieux. Inscrit en doctorat avec un thème relatif aux contrats intelligents, nous espérons qu'il reviendra vite en droit de propriété intellectuelle. Il assure qu'il continue son aventure en droit de la propriété intellectuelle sous l'angle des nouvelles technologies, notamment de la blockchain au Canada.

A.J.A.

DOUTY Marléne

L'obligation d'exploitation du brevet d'invention dans l'OAPI

Mémoire de Master Droit Privé, Université de Lomé, 2019

Monsieur DOUTY Marléne a obtenu un master en droit privé avant de se lancer définitivement dans la carrière d'écrivain et artiste-interprète dans laquelle il se sent encore plus dans sa peau. Il a déjà à son actif près de cinq pièces de théâtre publiées et est l'initiateur du « Théâtre chez vous » se transportant avec son équipe dans les établissements scolaires, dans les lieux publics et même dans les maisons pour des représentations théâtrales. Dans son mémoire relatif à l'obligation d'exploitation du brevet d'invention, il évoque le rapport entre le développement industriel et le brevet d'invention à travers l'exclusion de l'importation des actes conférés au breveté tel qu'il se retrouve dans l'accord de 1977. Il souligne qu'à travers cette exclusion et l'exigence de l'obligation d'exploitation locale, l'objectif poursuivi par l'accord de Bangui de 1977 paraissait plus clair, le brevet occupant une place prépondérante. Sa mise en valeur est une source infinie de richesses.

Le législateur OAPI avait donc fait de l'exploitation locale du brevet un cheval de bataille, un principe sacro-saint. L'obligation d'exploitation joue alors un rôle de levier pour valoriser le brevet sur le plan socio-économique dans l'intérêt général des populations. En effet, l'exploitation du brevet crée un intérêt certain sur le plan économique mais aussi social. Au regard de tous ces intérêts qui s'avèrent d'ordre public, le législateur de l'espace OAPI a institué une obligation d'exploiter le brevet en sanctionnant sévèrement l'inexploitation par la licence obligatoire et d'autres mécanismes telles que le refus pour tout contrevenant à cette obligation du recours en justice pour contrefaçon, le non-renouvellement du brevet dont la durée légale d'exploitation tait de dix ans renouvelables une fois. Malheureusement, le même législateur va faire tomber ces remparts étanches qu'il a dressés.

L'auteur ne met pas véritablement l'accent sur l'échec des sanctions de la non-exploitation locale des inventions. Toutefois, il relève que l'Accord sur les ADPIC qui a été signé le 15 avril 1994 à Marrakech par les pays membres de l'OMC au nombre desquels on compte les pays de l'OAPI et l'OAPI même en tant qu'organisation, a contribué largement à cette désaffection à l'égard de ce mécanisme si important dans les dans la maîtrise des effets économique des brevets d'invention. Cet accord instaurerait un certain nombre de règles défavorables aux pays de l'OAPI à savoir la durée légale d'exploitation du brevet qui est de vingt ans et la standardisation des règles gouvernant l'ensemble des droits intellectuels. En même temps, le nouvel accord semble diluer considérablement la force de la licence obligatoire. L'auteur estime que dans ce cas l'obligation d'exploiter le brevet sur place a perdu de sa teneur et de sa vigueur. Elle serait même réduite en peau de chagrin avec l'admission de l'importation comme droits conférés.

En affaiblissant l'obligation d'exploiter, le législateur lui a ôté la possibilité de provoquer le développement industriel par la voie du transfert de technologie, et social par le canal de la création du bien-être des populations. Cependant, grâce à l'émulation autour de l'exploitation du brevet créée par la forte concurrence des entreprises, l'on peut constater que le brevet garde une certaine place

dans le développement de l'espace et que son exploitation dans l'espace reprend vigueur. Il s'agit là d'une forme de survie voire de renouveau de l'obligation d'exploiter sur place. Il nous semble pourtant que ce n'est que par une prise de conscience que l'Afrique pourrait développer sa culture de la propriété industrielle pour faire face à ses propres défis.

En outre, rien n'interdit au législateur OAPI d'imposer l'obligation d'exploitation surplace malgré l'Accord sur les ADPIC. L'auteur a conclu son mémoire en souhaitant que les Etats puissent tirer le plus grand profit de l'épuisement international adopté dans l'accord de 2015 afin compenser la perte de vigueur de l'obligation d'exploitation. Nous souhaitons le meilleur à Monsieur Douti Marléne afin que son inspiration ne s'épuise pas dans la voie d'artiste-interprète et auteur pour une exploitation radieuse de ses œuvres.

A.J.A.

ADZOH Oli-Sika

L'efficacité du brevet d'invention du droit de propriété intellectuelle dans l'espace OAPI : cas du brevet d'invention

Mémoire de Master Droit du procès, Université de Kara, 2019

S'il est un point très discuté en droit de propriété intellectuelle en Afrique, c'est bien celui de l'efficacité de ces droits qui rime à la fois avec leur effectivité, efficience et leur utilité pour un continent qui cherche et qui peine à se construire et à édifier sur ses fondations les bases d'une véritable culture de la propriété intellectuelle. La question a émergé dès les années 1970 et a persisté jusqu'en 1995 avec les ADPIC. Elle ne semble pas close. C'est ce que révèle le mémoire de Madame ADZO Oli-Sika.

L'auteur relève d'entrée que l'efficacité se manifeste au regard des finalités du droit des brevets et au regard de l'exercice du droit exclusif du breveté. Curieusement, il construit l'efficacité sur la seule existence de la législation relative au brevet. Ainsi, elle remarque qu'au regard des finalités du droit des brevets, on constate que le législateur OAPI se donne pour objectif de protéger efficacement les droits du breveté. Elle ajoute que la supranationalité est un facteur non négligeable dans l'appréciation de cette efficacité. Cette supranationalité se manifeste par la centralisation des procédures d'obtention du brevet d'invention. Elle relève surtout le caractère attractif du brevet africain. Ce caractère est inhérent à la quête d'efficience. En outre, la protection du breveté est renforcée par l'adhésion de l'OAPI aux conventions internationales. Cette adhésion aux conventions internationales est un gage de sécurité non seulement pour le breveté, mais aussi pour les investisseurs.

L'auteur n'a pas manqué de mettre en exergue les éternels problèmes du brevet africain du fait de la faiblesse de la culture africaine de la propriété intellectuelle. La fonction sociale serait mal en point du fait de l'extension du domaine des droits conférés à l'importation. La question de l'accès aux produits pharmaceutiques n'a pas manqué d'être mentionnée comme l'un des maillons faibles de la brevetabilité des médicaments.

Cependant, il y aurait une prise en compte, certes par intermittence, salvatrice de l'intérêt général. Cette prise en compte insuffisante de l'intérêt général est marquée par les flexibilités accordées par l'Accord ADPIC. Aussi, l'Acte de Bamako révisant l'Accord de Bangui de 1999 a-t-il pris en compte certaines flexibilité comme l'exception Bolar ou encore le report de la brevetabilité des produits pharmaceutique en 2031. L'efficacité du droit de brevet africain serait en outre compromise avec l'absence de l'exigence d'une exploitation sur place des brevets.

En conséquence, de nombreux étrangers obtiennent les brevets OAPI mais ne les exploitent pas dans l'OAPI faisant du brevet un instrument de monopole de commercialisation. Ils utilisent les

brevets OAPI pour contrôler le marché de l'importation et de vente de leurs produits brevetés. Cette situation produit un effet négatif sur l'ensemble des États membre de l'OAPI. L'efficacité se manifesterait aussi à travers l'exercice du droit exclusif par le breveté. Celui-ci jouit d'un monopole d'exploitation par lequel il peut exploiter son invention. L'exploitation peut aussi se faire par l'intermédiaire des tiers à travers les contrats de licence ou de cession.

C'est la preuve que seul le breveté a le droit d'exploiter son invention. L'exploitation par le tiers sans son autorisation est une contrefaçon. Cependant, le breveté peut être privé de ce droit s'il n'exploite pas son invention. Le mécanisme de l'obligation d'exploitation et de licence obligatoire contribue à limiter le droit exclusif du breveté. Toutefois son utilisation est très rare et son intérêt très relatif pour l'appréciation du droit exclusif. Le monopole de commercialisation, quant à lui, sera considérablement affecté avec l'Acte de Bamako de 2015 du fait de l'épuisement international adopté par cet accord.

Madame ADZOH affirme qu'il y aurait « un semblant d'efficacité qui est retrouvé avec l'amputation de la prérogative de la maîtrise absolue de la circulation des produits protégés pour le breveté » et incite les justiciables à faire recours aux Modes Alternatifs de Règlement des Conflits pour régler leurs litiges. Cette proposition pour une résolution efficace des différends doit faire plaisir au Centre d'arbitrage de l'OAPI.

A.J.A.

PORPORTY Aféké Comi

La protection des œuvres de salariés en droit OAPI

Mémoire de Master Droit Privé Fondamental, Université de Lomé, 2017

La spécificité de cette étude est qu'elle a eu lieu dans une période transition entre le droit OPAI de 1999 et celui de 2015 qui n'était pas entré en vigueur. L'auteur était malaisé entre le choix d'un droit prospectif ou d'un droit positif. Il a choisi d'approfondir le droit positif qui n'a jamais été véritablement étudié en droit togolais malgré le vieil âge de cette législation. L'analyse a consisté principalement à voir si, l'article 31 de l'annexe VII de l'Accord de Bangui du 24 février 1999 qui régit la propriété littéraire et artistique, protège efficacement le créateur salarié, considéré comme étant la partie la plus faible dans le rapport créateur-exploitant. D'entrée, l'auteur a relevé le réalisme du législateur OAPI.

En même temps, il fustige les faiblesses de cette législation dans sa conclusion. En effet, il remarque que le législateur n'a pas dérogé au principe de la reconnaissance de la titularité originaire des droits d'auteur à l'auteur salarié, mais a institué une cession légale de ses droits patrimoniaux au profit de l'employeur, tout en prohibant l'aliénation des droits moraux de l'auteur salarié. Ainsi, en dépit de la cession légale des droits patrimoniaux à l'employeur, l'auteur salarié conserve ses droits moraux sur l'œuvre qu'il a créé. Aussi pertinente qu'elle soit, cette option contient des faiblesses et des approximations qui ne font pas droit à la protection de l'auteur. On le comprend, c'est une volonté de partager les eaux de la prééminence des prérogatives économiques du *copyright* avec celles de la force intangible des prérogatives morales du droit d'auteur français. Pour l'auteur, la législation de 1999 ne résolvait pas toute la difficulté inhérente à la création salariée, mais crée subtilement une autre difficulté : celle de la détermination de l'activité habituelle de l'employeur.

Il se pose alors un problème relatif à la détermination de l'étendue, du moment et des modalités du transfert. Cela crée une insécurité juridique au préjudice de l'auteur salarié qui risque d'être soumis au pouvoir discrétionnaire de l'employeur parce que celui-ci est avant tout, le seul juge du choix économique de son entreprise. En outre, il serait possible que l'auteur salarié qui conserve ses prérogatives morales en dépit de la cession de ses prérogatives patrimoniales à

l'employeur, pourrait entraver l'exploitation des œuvres par ce dernier, d'autant plus qu'il est le seul à même de déterminer si ses intérêts intellectuels ont été atteints ou pas et que l'exercice des prérogatives morales est avant tout, discrétionnaire.

De même, l'exercice intempestif des droits moraux pourrait amener l'employeur à chercher à mettre en cause la responsabilité contractuelle de l'auteur salarié. En face de cette rencontre conflictuelle des diverses prérogatives en cause, l'auteur a essayé de chercher à concilier les exigences du droit d'auteur avec les prérogatives de l'employeur et les contraintes économiques de l'entreprise. M. Porporty propose alors une amélioration du mécanisme de la cession légale en raison des incertitudes qu'il contient ainsi qu'un encadrement de l'exercice des droits moraux pour que l'auteur salarié ne puisse pas au nom d'un droit moral dévoyé, compromettre les actes d'exploitation de l'employeur qui a investi dans la création et qui a pour ambition légitime, d'exploiter les œuvres de ses salariés.

Il est absolument vrai que le législateur OAPI a vu venir tous ces problèmes et a préféré un alignement des œuvres salariées sur les inventions de salariés du droit français. Reste à savoir si les pertinentes questions sur le droit moral ne subsisteront dans la mise en œuvre de la législation de 2015. Entré cette année à l'école nationale de la magistrature après admission sur concours, nous espérons que M. Porporty aura la chance en tant que juge de trancher des litiges et de trouver des solutions adéquates à ces conflits entre les intérêts divergents de l'entreprise et de l'auteur salarié à l'aune de l'Accord de Bangui de 2015.

A.J.A.

ALONYO Yawa Senyediva

Le risque de confusion dans la contrefaçon des marques

Mémoire de Master Droit Privé Fondamental, l'Université de Lomé, 2017

En choisissant de travailler sur le risque de confusion en droit des marques, Madame ALONYO Yawa Senyediva avait en fait choisi en réalité de prendre à bras le corps une question cruciale de la contrefaçon de la marque. Evidemment, la marque étant incontestablement un droit de la clientèle porté par le signe distinctif joue un rôle essentiel dans la régulation de la concurrence. Tout le droit de propriété étant focalisé sur ce signe, c'est sur le terrain de la confusion que se jouent la plupart des délits. C'est bien ce que révèle le mémoire de Madame Alonyo qui a malheureusement opté pour une thèse en droit bancaire.

Elle a d'abord objectivement noté un élargissement du risque de confusion Ainsi, celui-ci qui était exclusivement cantonné à la similitude entre les signes a désormais compétence même en cas d'identité. Le risque de confusion a ainsi évincé le critère de l'identité et on assiste à un recul voire à une rareté des cas de reproduction à l'identique. C'est la raison pour laquelle la preuve du risque de confusion est subordonnée à l'atteinte à la fonction essentielle de la marque. Ensuite, elle a retenu que l'appréciation du risque de confusion obéit à des règles bien ficelées et établies. Ces règles qui sont pour la plupart élaborées par la jurisprudence déterminent les critères et la méthode d'appréciation du risque de confusion. Les critères qui sont très rigides peuvent être regroupés en deux catégories. D'une part, il y a des critères dits objectifs qui se composent de la ressemblance entre les produits ou services et entre les signes. D'autre part, le critère subjectif qui s'articule autour de l'agent référent du risque de confusion encore appelé consommateur d'attention moyenne.

Ce constat rappelle d'ailleurs que le consommateur d'attention moyenne, tout comme l'homme de métier en droit des brevets ou l'internaute en droit d'auteur, constitue un référent comme une famille de la propriété intellectuelle. Il apparaît ainsi incontournable dans l'appréciation de la contrefaçon de marque. Or en droit OAPI, l'identification de consommateur d'attention

moyenne peut relever des spécificités régionales. L'intérêt de ce travail est d'avoir relevé cette particularité dans l'appréciation de ce consommateur du fait, à titre illustratif du niveau d'alphabétisation des populations ainsi que de leur niveau économique et social. Ayant conscience des difficultés que peut entraîner une telle voie, l'auteur souligne que « même si cette position a connu de vives critiques, il faut saluer cette innovation du droit africain qui cherche à se démarquer des conceptions occidentales ». Elle souligne le rapprochement probable du droit OAPI avec le droit français relativement à la méthode d'appréciation dite globale du risque de confusion puisque les différents critères sont interdépendants et même si elle n'a pas été ainsi nommée.

L'auteur a conclu son mémoire avec le rôle déterminant des juges dans l'appréciation du risque de confusion en matière de contrefaçon de marques avec le risque d'instrumentalisation de cet outil qui est malléable à merci. Toutefois, elle s'en remet à la sagesse et la prudence des juges qui doivent jouer leur rôle dans l'encadrement de cette notion aux contours ondoyants par une interprétation judicieuse de l'Accord de Bangui et faire échec à des excès préjudiciables aux parties. Nous souhaitons une belle continuation en thèse en droit bancaire à Madame Alonyo en espérant un retour à ses premiers amours… Il est heureux que le thème ait été repris par un doctorant qui nous livrera dans un avenir proche les résultats de sa recherche.

A.J.A.

KOSSADOUM Cédric

Les exceptions au droit d'auteur à l'épreuve de la justice dans l'espace OAPI et dans l'espace ARIPO

Mémoire de Master 2 Droit de la création et du Numérique, Université Paris-Saclay, septembre 2023

Ce mémoire de recherche analyse les exceptions au droit d'auteur dans l'espace OAPI et ARIPO éprouvée par la justice. Le juge de l'espace OAPI et celui de l'espace ARIPO rencontrent plusieurs difficultés dans l'interprétation des exceptions au droit d'auteur. Au nombre de ces difficultés l'auteur relève l'absence de juridiction permettant une interprétation harmonisée et effective des exceptions au sein dans les Etats-Membres de l'OAPI.

Par ailleurs, explique l'auteur, l'interprétation des exceptions au droit d'auteur diffère parfois selon qu'elles sont interprétées par le juge de l'espace OAPI ou de l'espace ARIPO. L'auteur considère qu'il y a nécessité d'interprétation commune des exceptions au droit d'auteur tant dans l'espace OAPI que dans l'espace ARIPO, et cela au regard du contexte Africain. A titre d'exemple, indique l'auteur, *« une interprétation différente des exceptions au droit d'auteur n'aurait pas lieu d'être, car la similitude entre ces deux espaces est le contexte Africain, par sa dimension culturelle, familiale et solidaire, mais aussi la nécessité de permettre aux Africains l'accès au savoir ».* L'auteur n'a pas pu exploiter l'ensemble des décisions pertinentes disponibles mais a néanmoins livré des analyses comparatives intéressantes qui pourront être approfondies par lui ou par d'autres.

Y.L.N

HONMINOU Edem Kokouvi

La marque au regard de l'Accord de Bangui Révisé, Acte du 14 décembre 2015, Mémoire de Master Droit privé fondamental soutenu, le mercredi 28 décembre 2022.

Face aux critiques à l'endroit de la marque en droit de l'Organisation Africaine de la Propriété Intellectuelle (OAPI) et de la nécessité de se conformer aux exigences des accords sur les Aspects des Droits de Propriété Intellectuelle qui touchent le Commerce (ADPIC), les Etats membres de l'OAPI ont révisé en 2015 l'Accord de Bangui. Dans un souci d'assurer plus de protection à la marque contre la contrefaçon, l'ABR a procédé à l'élargissement de l'assiette des marques sujettes à protection. Au-delà de l'élargissement de l'assiette,

l'ABR offre aux victimes des mesures suffisantes de preuve pour justifier toute contrefaçon de leur marque.

Que ce soit les mesures prises aux frontières ou la procédure de recherche d'informations, les victimes se retrouvent en possession de toutes les informations nécessaires pour la défense de leurs droits ; peuvent demander la réparation intégrale des préjudices subies et voir les contrefacteurs condamnés au paiement du quintuple de l'amende prévu en 1999. Toutes ces innovations apportées par l'AB de 2015 ont pour but de protéger et la marque et son propriétaire contre toute contrefaçon. Toutefois, pour une Afrique émergente ou l'on prône l'essor de la technologie, de l'industrie, n'est-il pas opportun pour l'OAPI d'admettre les marques tactiles, olfactives et gustatives dans l'assiette des marques à protéger ?

E.M.A.

SODJI Alexis

La contribution de la douane béninoise a la lutte contre la contrefaçon

Mémoire de Master Droit des Affaires et Fiscalités, Université d'Abomey-Calavi, soutenu le 11 octobre 2023

La douane contribue-t-elle efficacement à la lutte contre la contrefaçon ? Telle est la question qui sous-tend cette étude. Il s'est agi d'évaluer, à la lumière d'une lecture croisée entre le cadre légal et organique, la contribution des douanes dans la lutte contre la contrefaçon, tout en mettant en exergue les actions concrètes menées, mais aussi et surtout en relevant les insuffisances.

Le législateur a veillé à doter au fur et à mesure la douane de instruments juridiques lui permettant de mieux d'aborder la lutte contre la contrefaçon. De plus, plusieurs acteurs nationaux et étrangers interviennent dans cette lutte aux côtés de l'administration douanière.

A l'analyse, la douane béninoise est active sur le terrain de la lutte contre la contrefaçon. Elle a mené, seule ou sous l'égide de l'Organisation Mondiale de la Douane (OMD), diverses opérations (PANGEA, BIYELA, ACIM, VICE-GRIPS) qui ont permis d'arraisonner d'importantes quantités de médicaments contrefaisants et d'initier à l'encontre des auteurs de cette infraction des poursuites judiciaires adéquates.

Pour améliorer la contribution de la douane béninoise dans la lutte contre la contrefaçon, il est nécessaire de la renforcer dans ses attributions. Plus spécifiquement, la création d'une direction uniquement consacrée à la lutte est souhaitée.

E.M.A.

▪ ACTUALITE UNIVERSITAIRE

➢ Journée RGPD à Lyon

L'Association Française des Correspondants à la protection des Données à caractère Personnel (L'AFCDP) a organisé une journée RGPD le 13 septembre à Lyon avec pour objectif de donner une opportunité aux professionnels du secteur d'échanger autour du RGPD et des bonnes pratiques à adopter avec pour base de réflexion les décisions récentes de la CNIL notamment. Par ailleurs cette association produit une NEWSLETTER qui donne les actualités sur la règlementation, les activités et rencontres des professionnels du secteur.

- **Journée Sécurité & RGPD**

A l'initiative de Aline MBENOUN-NGOUE, l'institut de la communication de l'Université de Lyon 2 (ICOM) a organisé une demi-journée de RGPD sous le thème : Cybersécurité et conformité RGPD le 20 /03/2023.

Madame Aurèlie DUSONCHET, Experte Cybersécurité & RGPD, y est intervenue sur l'invitation de Mme Aline MBENOUN-NGOUE.

Ce projet a été mis en place pour les Master OPSIE (Organisation et protection des systèmes d'information dans les entreprises). L'objectif de cette première rencontre était de mettre en relief le lien entre la sécurité et le RGPD.

- **Journée 30 ans de Droit OHADA**

A l'occasion du trentième anniversaire de l'OHADA, l'Univesrité Catholique de de Lyon accueille le 23 novembre un colloque, sur le thème 30 ans d'application du droit uniforme des affaires OHADA sous la direction scientifique du Pr. Gérard Anou et du Dr Louis-Daniel Muka Tshibende.

L'APIA est fière de relever que deux de ses adhérents, Mme Mbenoun-Ngoue et M. Falilou Diop, y présideront des séances.

Par Aline Mbenoun-Ngoué

L'arbitrage et les procédures collectives en droit OHADA et marocain

Youssouf Adoum Youssouf
Juriste

Le chevauchement de l'arbitrage et des procédures collectives n'est pas une problématique récente. Plusieurs auteurs se sont attelés là-dessus. Toutefois, l'abondance des contentieux concernant le sujet, renouvelle son importance et accentue le débat déjà très riche sur l'arbitrage et les procédures collectives. Cela peut s'expliquer par le fait qu'il s'agit de concilier deux matières naturellement antagonistes. Amener deux justices, l'une privée (l'arbitrage) et l'autre étatique (procédures collectives) à se concilier, n'est pas pour autant une question aussi simple[144].Ce faisant, les spécificités de chaque procédure doivent être prises en compte d'une part et d'une autre.

En plus de leur nature contradictoire, l'arbitrage et les procédures collectives suivent des objectifs divergents.

L'arbitrage, étant une justice privée, est la consécration de la liberté contractuelle, de l'autonomie des volontés et de la force obligatoire, qui sont des principes sacro-saints du droit des contrats. Le législateur OHADA a sciemment omis de donner une définition à l'arbitrage. L'Acte uniforme relatif au droit de l'arbitrage de novembre 2017 ne mentionne aucune définition de l'arbitrage.

Devant une situation pareille, notre regard se tourne inéluctablement vers le législateur marocain, qui a consacré la définition de l'arbitrage à l'article 1er du dahir[145] n° 1-22-43 du 23 choual 1444(24 mai 2022) portant promulgation de la loi 95-17 relative à l'arbitrage et la médiation conventionnelle. Ledit article dispose que : « L'arbitrage a pour objet de faire trancher un litige par un tribunal arbitral qui reçoit des parties la mission de juger en vertu d'une convention d'arbitrage ». L'arbitrage constitue le mode de règlement de litiges de prédilection des acteurs du commerce interne et international. En effet, il devient monnaie courante dans le règlement des litiges découlant de contrats commerciaux[146].

Pour certains auteurs, l'arbitrage est aussi vieux que l'humanité. Il est plus qu'un phénomène international, mais parfois interculturel. L'arbitrage serait apparu en Grèce antique au VIème-Vème siècle avant Jésus-Christ. Cette époque aurait connu la naissance de l'arbitrage. L'on dénombre

[144] Julie Daniel, Nicolas Borga, Arbitrage et procédure collective : de l'art de coordonner les procédures, Recueil Dalloz, 2013, p2891.

[145] Au Maroc, le dahir est un décret qui émane de la juridiction du roi. Il désigne le sceau du roi apposé aux textes législatifs

[146] OSSAGOU Diane Loïca, Arbitrage et procédures collectives, Thèse, Université Toulouse 1 Capitole, 2017, p17.

plusieurs arbitrages qui avaient eu lieu entre cités grecques à partir du IVème siècle av J-C. Très tôt, Aristote l'a distingué de la justice étatique : « l'arbitre vise à l'équité, le juge à la loi. L'arbitrage a été inventé pour que l'équité soit appliquée ». De plus, l'histoire de l'arbitrage remonte aussi au Rome antique (VIIème- VIème av J-C) avec « l'arbitrium liti aestimandae » dont un arbitre se chargeait de fixer le montant de la réparation à payer par le coupable ayant succombé au procès. Par la suite, l'arbitrage est devenu monnaie courante. Pour Cicéron : « L'arbitrage est le moyen de ne pas gagner complètement un bon procès, ni de perdre un mauvais procès ».

Considérer l'arbitrage comme le seul apanage de la civilisation gréco-romaine, c'est prendre l'histoire sous un seul angle. Le livre saint de l'islam a déjà distingué entre l'arbitre (Hakam) et le juge (qadi). La Bible en fait aussi mention[147].

La consécration de l'arbitrage comme mode alternatif de règlement des différends contractuels en droit Ohada a été acté dès l'aube. Le Traité de Port-Louis du 17 octobre 1993 précise expressément à travers son préambule la volonté des Etats parties à promouvoir l'arbitrage comme instrument de règlement des litiges contractuels[148].L'article 1er dudit traité dispose que l'encouragement du recours à l'arbitrage est l'un des objectifs du traité. L'article 2 du même traité énumère le droit de l'arbitrage parmi les disciplines qui entrent dans le domaine du droit des affaires. De ce fait, le traité initial avait consacré un titre entier à l'arbitrage.

Nonobstant cette consécration, la notion d'arbitrage reste relativement exposée par ce texte. Il a fallu attendre quelques années afin que l'arbitrage jouisse d'un corpus autonome, qui approfondit cette notion. L'arbitrage, en tant que mode alternatif des règlements de litiges, a été renforcé en droit Ohada par l'Acte uniforme relatif au droit de l'arbitrage du 11 mars 1999. Ce dernier, fut révisé par l'acte uniforme relatif au droit d'arbitrage (AUA) du 23 novembre 2017[149].

Par contre, le doit marocain d'arbitrage a connu plusieurs évolutions. On est passé d'une loi reliée au code de procédure civile, à une loi autonome. Le code de procédure civile du 12 août 1913 a consacré un chapitre à l'arbitrage. Ce texte instaure le régime juridique de l'arbitrage au Royaume. Il fut modifié par le Dahir du 28 septembre 1974. La loi n° 08-05 de 2007 abrogeant et remplaçant le chapitre VIII du code de procédure civile, s'inscrit dans le cadre d'amélioration du climat d'affaires et la sécurisation juridique des investissements. Tout de même, bien que la loi n° 08-05 ait instauré pour la première fois des dispositifs régissant l'arbitrage international, elle n'a pas pu se prémunir contre les critiques des investisseurs et des professionnels[150]. C'est dans ce cadre qu'intervient le dahir n° 1-22-43 du 23 choual 1444(24 mai 2022) portant promulgation de la loi 95-17 relative à l'arbitrage et la médiation conventionnelle. Cette loi novatrice vient apporter des solutions aux lacunes tant décriées de l'ancienne loi n°08-05. Le formalisme lié au recours à l'arbitrage par l'Etat, les collectivités territoriales, entreprises publiques et établissements publics est assoupli.

[147] Charles Jarrosson, La notion d'arbitrage, Paris, LGDJ, 1987, p1 et suiv.

[148] Préambule du traité relatif à l'harmonisation du droit des affaires en Afrique.

[149] Gaston Kenfack Douajni, Droit de l'arbitrage Ohada, ERSUMA, 2010, p1.

[150] Abdallah Khial, L'Arbitrage en droit marocain, p1. Article disponible sur la page de la Cour internationale de médiation et d'arbitrage. https://www.cimeda.ch/

Dorénavant, les réunions et audiences peuvent se tenir par le moyen des nouvelles technologies de l'information et de communication. Cela va de soi également pour les échanges procéduraux, qui peuvent se faire par voie électronique[151].

A l'inverse de l'arbitrage, les procédures collectives, imprégnées des règles d'ordre public, cherchent à centraliser les litiges entre les mains du juge étatique, afin de remédier aux difficultés des entreprises.

Arbitrage et procédures collectives sont deux matières qui, parfois, se chevauchent dans la pratique. Leur traitement nécessite une vigilance sans précèdent aussi bien pour les juges étatiques que pour les arbitres[152].

Alors, deux questions fondamentales se posent : Les procédures collectives ne prévalent-elles pas sur l'arbitrage ? Peut-on parler d'une conciliation entre les deux procédures ? Pour répondre à ces interrogations, nous serons amenés à traiter dans une première partie (I) de la prédominance des procédures collectives sur l'arbitrage, et dans une deuxième partie (II), de la résistance de l'arbitrage face aux procédures collectives.

I- La prédominance des procédures collectives sur l'arbitrage

Bien que l'effet positif de la convention d'arbitrage exige que la procédure d'arbitrage prenne son cours, toutefois, cela ne devrait pas être pour les parties une aubaine afin de s'affranchir des règles d'ordre public des procédures collectives.

S'il s'est avéré aucun obstacle à l'arbitrabilité du litige, l'ordre public des procédures collectives apparait comme l'obstacle majeur à la procédure d'arbitrage. De ce fait, l'ordre public des procédures collectives a une influence non seulement sur le déroulement de l'instance arbitrale mais aussi sur les attributions de l'arbitre[153].

Dans ce cadre, doivent être préservées toutes les règles d'ordre public propres aux procédures collectives telles que : l'arrêt des poursuites individuelles et l'interdiction de payer les dettes antérieures. Ces règles s'imposent aux parties et aux arbitres à tel point que leur violation entraine l'annulation de la sentence arbitrale[154]. Par conséquent, l'arbitre doit veiller au respect de ces règles le long de la procédure. Toute négligence de la part de l'arbitre frappera la sentence d'incompatibilité avec l'ordre public des procédures collectives[155].

En effet, il s'avère primordial qu'il y ait des limites à l'instance arbitrale qui intervient en même temps qu'une procédure collective du débiteur ou ayant débuté avant le jugement d'ouverture. Comme il a été mentionné précédemment que les procédures collectives sont impérialistes, elles exercent une influence sur la procédure d'arbitrage(A). En outre, la possibilité de compromettre postérieurement(B) au jugement d'ouverture ne doit être perdu de vu.

---

[151] Kawtar Jalal, La loi 95-17 relative à l'arbitrage : un propulseur du Maroc comme place de rang de premier choix comme siège d'arbitrage-Avancées et lacunes, La lettre D'ARTEMIS, n° 23-2ème trimestre 2022, p39.

[152] Youssouf Adoum Youssouf, Arbitrage et procédure collective, Mémoire de fin d'études, Université Cadi Ayyad, Marrakech, 2022, p8.

[153] OSSAGOU Diane Loïca, op.cit, p31.

[154] Youssouf Adoum Youssouf, op.cit, p12.

[155] Thomas Clay, L'articulation harmonieuse de l'arbitrage et des procédures collectives, recueil Dalloz, 2004, p3184.

A- L'influence de l'ordre public des procédures collective sur l'arbitrage

En principe, rien n'interdit qu'une procédure d'arbitrage prévue par une clause compromissoire, établie avant le jugement d'ouverture soit actée à la survenance du litige. Arbitrage et procédures collectives peuvent se chevauchés en pratique. Dans ce cas de figure, le respect des règles des procédures collectives telles qu'édictées dans l'Acte uniforme organisant les procédures collectives d'apurement du passif (AUPC) doivent être respectées. La survenance d'une procédure collective n'est pas sans effet sur la procédure d'arbitrage.

Cette dernière se trouve automatiquement interrompue. Si rien n'empêche l'arbitre de conserver ses attributions et peut rendre une sentence arbitrale, tout de même, la procédure d'arbitrage se trouve quelque fois perturbée. Cette perturbation est justifiée par le caractère impérialiste de la procédure collective. Le respect de cette règle s'impose à l'arbitre. Au nom de ce principe, l'instance en cours est suspendue. Cependant, il s'impose à nous de soulever que la suspension de l'instance en cours n'est que temporaire.

Le temps que les créanciers déclarent leurs créances. Passée cette étape, l'instance peut reprendre normalement son cours[156].C'est dans cette optique que l'article 75, alinéa 4 de l'acte uniforme Ohada relatif aux procédures collectives d'apurement du passif dispose : « Les instances en cours sont interrompues jusqu'à ce que le créancier poursuivant ait produit sa créance. Elles sont alors reprises de plein droit, le syndic dûment appelé, mais tendent uniquement à la constatation des créances et à la fixation de leur montant ». Cette position légale est entérinée par la Cour Commune de Justice et d'Arbitrage (CCJA)[157].

En droit marocain, le législateur chérifien a opté pour la même logique que celle du promoteur de l'acte Ohada, à travers l'article 687 du Code de commerce. Il ressort de cet article que les instances sont temporairement suspendues et cela s'applique à toutes les instances en cours. Cette règle d'arrêt de poursuite est réconfortée par la haute juridiction marocaine. Dans un arrêt, la Cour de cassation décide que : « Le prononcé d'une décision de redressement judiciaire suspend les formalités d'exécution sur les meubles et immeubles appartenant à l'entreprise concernée »[158].

L'arrêt des poursuites individuelles ne se présente pas non seulement comme une règle d'ordre public interne dans les deux législations, mais également une règle d'ordre public international des procédures collectives. La sentence rendue en matière d'arbitrage international, amenée à être exécutée en zone Ohada ou au Maroc, doit être impérativement conforme à ce principe. En outre, les arbitres doivent veiller au respect du principe de l'interdiction de paiement des dettes antérieures, qui est également une règle d'ordre public interne et international des procédures collectives.

Exception faite aux créances salariales, le jugement ouvrant la procédure collective emporte de plein droit, interdiction de payer toute créance née antérieurement au jugement d'ouverture[159]. L'arbitre lors de la

[156] Pierre M. Lecorre, Droit des entreprises en difficulté, 8ème édition, Dalloz, p121.
[157] CCJA, 18 mai 2017, n° 128/2017.
[158] C. cass marocaine, chambre com.04 mars 2009, n° 335, dossier 203 /3/1/2007
[159] Article 690 du code de commerce marocain.

reprise de l'instance arbitrale, et lorsque l'action tend au paiement d'une somme d'argent devrait se remettre au respect de la règle d'égalité des créanciers. En vertu de ce principe, les instances en cours tendent uniquement à la constatation des créances et à la fixation de leur montant. Cette interdiction est valable également lorsque la procédure collective est ouverte avant l'instance arbitrale.

En présence d'une procédure collective, l'arbitre est dans l'impossibilité de condamner le débiteur qui est en procédure collective au paiement d'une somme d'argent. Lorsqu'une instance arbitrale est saisie, elle ne devrait pas demander par sentence au débiteur le paiement de sa dette antérieure. L'instance arbitrale se limitera alors à la vérification et l'évaluation du montant de la créance[160].

La sentence arbitrale qui condamne le débiteur au paiement d'une somme d'argent en présence d'une procédure collective, ne peut recevoir l'exéquatur en raison de la violation des règles d'ordre public des procédures collectives.

B- La possibilité de compromettre durant la procédure collective

S'il est moins compliqué de parler de la procédure d'arbitrage prévue antérieurement aux procédures collectives, il ne va pas de soi avec celle qui intervient durant la tenue de la procédure collective. Après l'ouverture d'une procédure collective, conclure une convention d'arbitrage est considéré comme un acte grave. L'ouverture d'une instance arbitrale pose des difficultés lorsqu'une procédure collective est préalablement ouverte. En effet, il est en principe légalement impossible d'ouvrir une instance arbitrale en cours de procédure collective. Toutefois, cette interdiction connait quelques dérogations.

L'ouverture d'une procédure collective a pour effet dans la plupart des cas, d'altérer les pouvoirs de gestion du débiteur. L'interdiction de compromettre se fonde à la fois sur des dispositions légales et sur la nature même du litige. Cette analyse tire son fondement en droit Ohada des procédures collectives, de l'article 75, al 1 de l'AUPC. Les dispositions du code de commerce marocain relatives aux procédures collectives interdissent également le recourir à l'arbitrage par le biais d'un compromis d'arbitrage[161].

Quand bien même que les dispositions de l'article 75, al 1 ne mentionnent expressément l'arbitrage, étant aussi une justice, l'arbitrage tombe dans le champ d'application de ces dispositions. Centraliser les litiges entre les mains du juge étatique semble être l'objectif recherché par les procédures collectives. Offrir l'opportunité aux créanciers de compromettre préjudiciera l'état de la trésorerie et porter indéniablement atteinte à l'égalité des créanciers[162].C'est dans ce sens que le professeur Philippe Fouchard affirme que compromettre après le jugement d'ouverture n'est pas une simple « opération de gestion »[163].

Une partie de la doctrine marocaine admet que : « Si la convention d'arbitrage est conclue après l'ouverture de la procédure collective, elle est frappée de nullité car ladite procédure concerne l'ordre public ainsi que des formalités substantielles dont la mise en œuvre a été dévolue par la législation moderne ,à la compétence exclusive des

[160] Ossagou Diane Loïca, op.cit, p235.
[161] Article 686 du code de commerce marocain.
[162] Thomas Clay, L'arbitre, 1ère édition, Dalloz, p175.
[163] Philippe Fouchard, op.cit, p493.

tribunaux nationaux ,la législation marocaine s'inscrivant parfaitement dans cette tendance en ayant octroyé aux juridictions commerciales la compétence pour connaitre des litiges relatifs aux procédures collectives »[164].Dans ce cadre, les litiges nés de l'effet des procédures collectives ou ayant un lien étroit avec celles-ci ne peuvent être soumis à l'arbitrage. A ce titre, ne sont pas arbitrables les contestations relatives au jugement d'ouverture, des périodes suspectes, de l'extension de procédure aux dirigeants sociaux etc.

Cependant, cette interdiction légale connait quelques atténuations. Le législateur a habilité le syndic de recourir à l'arbitrage malgré l'ouverture d'une procédure collective. Cette habilitation est soumise à l'autorisation du juge-commissaire, et le litige doit avoir une nature purement contractuelle.

Dans ce cadre, les législateurs Ohada et marocain accordent au juge-commissaire le pouvoir d'autoriser le syndic à compromettre en cours des procédures collectives. La possibilité de compromettre trouve une justification dans les articles 148 de l'AUPC et 594 du code de commerce marocain.

Par la possibilité de recourir à l'arbitrage malgré l'ouverture d'une procédure collective, le législateur veut favoriser l'essor de l'arbitrage, et démontrer que le recours à ce mode alternatif de règlement des différends ne peut être détérioré par la simple survenance d'une procédure collective.

Enfin, le litige objet du compromis doit impérativement être de nature contractuelle. Par conséquent, le litige ne doit avoir ni son origine, ni un lien avec la procédure collective. Peut faire à cet effet l'objet d'un compromis d'arbitrage, l'action contre une caution[165].

Néanmoins, l'ouverture de la future instance arbitrale sera affectée par les règles d'ordre public des procédures collectives. L'instance arbitrale ne peut s'ouvrir que lorsque le créancier demandeur ait déclaré sa créance[166].

II- La résistance de l'arbitrage face aux procédures collectives

Bien qu'imprégnée des règles d'ordre public interne et international, la survenance d'une procédure collective ne compromet pas pour longtemps l'exécution d'une convention d'arbitrage. En effet, l'ouverture d'une procédure collective ne permet pas à elle seule d'ignorer la clause compromissoire intervenue avant le jugement d'ouverture ou empêcher la conclusion d'un compromis d'arbitrage en cours de procédure collective. Altérer une convention d'arbitrage respectant toutes les conditions de sa validité, c'est porter un coup fatal et une violation notoire à l'autonomie des volontés. On assistera à cet effet, à la persistance de l'arbitrage face aux procédures collectives(A).

Si le recours à l'arbitrage suppose pour les parties la volonté d'écarter le pouvoir du juge étatique à connaitre le litige, toutefois, le juge étatique apparait lors du contrôle de la sentence arbitrale(B).

A- La persistance de l'arbitrage face aux procédures collectives

Compte tenu de la volonté manifeste des parties de recourir à l'arbitrage comme mode de règlement du différend qui les oppose, la

[164] Toumlilt, *op.cit*, p63.

[165] Philippe Fouchard, *op.cit*, p480.

[166] Eric Loquin, *L'arbitrage du commerce international*, 1ère édition, Issy-les Moulineaux, Joly édition, 2015, p. 56.

survenance d'une procédure collective ne peut être un motif pour le débiteur de s'échapper à l'arbitrage.

Etant donné que les règles d'ordre public des procédures collectives respectées, l'instance arbitrale sera mise sur pied par la simple naissance du litige objet de la convention d'arbitrage. Cette thèse est consacrée par l'article 13 de l'AUA. Pour cette raison, une convention d'arbitrage, comme tout acte de volonté valablement établie, doit impérativement être appliqué. Par son effet positif, la convention d'arbitrage exige aux parties de recourir à la justice privée, partant au tribunal arbitral au détriment de la justice étatique[167].

Le maintien de la compétence de l'arbitre malgré l'ouverture d'une procédure collective donne lieu normalement à l'application de la convention d'arbitrage[168].

Si l'effet positif de la convention d'arbitrage exige aux parties de recourir à l'arbitrage, son effet négatif exclut le pouvoir du juge étatique à apprécier le litige objet de la convention d'arbitrage. Le juge commissaire, en occurrence juge étatique, déclare son incompétence et renvoi les parties devant le tribunal arbitral, et cela indépendamment de l'ouverture ou non d'une instance arbitrale[169]. Donc, il revient à l'instance arbitrale de constater et d'évaluer la créance.

Il y'a lieu de souligner qu'il revient aux parties de soulever l'existence d'une convention d'arbitrage. Le juge commissaire ne peut en principe relever d'office son incompétence. Dans ce cadre, il est judicieux, pour la partie qui espère un avantage dans l'arbitrage de soulever l'existence d'une convention d'arbitrage[170].

En outre, le juge-commissaire ne peut statuer sur la compétence du tribunal arbitral. Il s'agit ici du principe compétence-compétence, qui donne le plein pouvoir au tribunal arbitral de statuer sur sa propre compétence et en même temps connaitre le litige. Cette position est consacrée à la fois en droit Ohada et marocain de l'arbitrage.

Si on comprend bien la philosophie du législateur Ohada et marocain, tant que la convention d'arbitrage n'éprouve pas des nullités manifeste ou manifestement inapplicable, il n'est pas admis de déroger à ce principe.

B- Le contrôle de la sentence arbitrale

Si les parties, par leurs volontés de recourir à l'arbitrage, ont exclu le pouvoir du juge étatique à connaitre le litige, celui-ci apparait lors du contrôle de la sentence rendue par le tribunal arbitral.

Cette étape permet au juge étatique d'apprécier l'effectivité de la sentence arbitrale vis-à-vis des règles d'ordre public interne et international des procédures collectives. Il s'impose, en effet, au tribunal arbitral, soucieux de faire accorder par le juge étatique une reconnaissance à sa sentence, de respecter les principes d'interdiction des poursuites individuelles et de l'arrêt de paiement des dettes antérieures.

Le contrôle du respect des règles d'ordre public des procédures collectives dans la décision arbitrale se matérialise dans la plupart des cas par la procédure d'exequatur et le recours en annulation.

---

[167] Thomas Clay, *Articulation harmonieuse de l'arbitrage et des procédures collectives*, Dalloz, 2004, p. 3184.

[168] Ossagou Diane Loïca*, op.cit,* p173.

[169] Article 13, al 2 de l'AUA.

[170] C. cass marocain, ch.com, 09 /07/2008, n°59/3/1/2005, Réf 15834.

D'abord, que ce soit en droit Ohada ou marocain d'arbitrage, la sentence n'est susceptible d'exécution forcée qu'en vertu d'une ordonnance d'exequatur[171].

La procédure d'exequatur permet au juge étatique de s'assurer de l'existence d'une sentence arbitrale et sa conformité à l'ordre public des procédures collectives. Pour cette raison, l'exequatur est accordé à toute sentence arbitrale rendue dans le respect des règles d'ordre public interne et international des procédures collectives.

Il va sans dire que le contrôle du juge de l'exequatur est limité. Il ne lui est pas permis de faire un contrôle approfondi, de vérifier si la sentence a été rendue suite à une convention d'arbitrage valable ou s'atteler sur la composition du tribunal arbitral.

Si le juge de l'exequatur ne dispose pas assez des moyens lui permettant d'apprécier la sentence d'une manière approfondie, cependant, celui qui reçoit les recours en annulation jouit des prérogatives lui permettant d'examiner si le tribunal arbitral a respecté la coordination entre l'arbitrage et les procédures collectives[172].Le recours en annulation est une manière pour la partie qui avait succombé dans le tribunal arbitral d'effacer l'exequatur et par ricochet la sentence arbitrale rendue en sa défaveur. Cette voie de recours ne peut être ouverte que dans des cas exhaustivement limités. L'acte uniforme sur l'arbitrage ne reconnait que six cas dans lesquels le recours est recevable. Tandis que le droit marocain d'arbitrage a reconnu sept cas ouvrant ainsi un recours en annulation.

En matière des procédures collectives, le recours en annulation peut être ouvert lorsque le tribunal arbitral statue sur les contestations nées de la procédure collective ou sur lesquelles celle-ci exerce une influence. De tels litiges sont inarbitrables.

Epilogue

Bien que l'arrivée d'une procédure collective ait pour effet d'altérer temporairement le déroulement de l'instance arbitrale, cette dernière ne tarde pas à prendre son envol.

Au terme de cette passionnante étude, nous déduisons que malgré les exigences des règles d'ordre public des procédures collectives, l'arbitrage et les procédures collectives tel que qualifié par la doctrine comme étant les deux fortes têtes du droit des affaires sont conciliables.

S'il parait au premier regard, qu'une conciliation des deux procédures est quasi impossible, toutefois, à travers le résultat de ce travail, on peut dire qu'une conciliation est réalisable. Cette difficile conciliation passe inéluctablement par le respect des fondamentaux de chaque procédure.

Ce travail met en exergue ce que doit suivre le(s) arbitre(s), le(s) créancier(s) et voire la partie défenderesse et en même temps défaillante, afin de parvenir à une conciliation sans équivoque.

La conciliation de ces deux grandes forêts du droit des affaires nécessite une grande vigilance de la part des parties. Les arbitres doivent respecter les règles d'ordre public interne et international des procédures collectives, et le juge-commissaire doit se dessaisir devant une convention d'arbitrage et faire valoir ainsi la volonté des parties à recourir à l'arbitrage.

Y.A.Y.

[171] Articles 30 de l'AUA et 67 de la loi 95-17 sur l'arbitrage et la médiation conventionnelle.

[172] Christophe Seraglini, L'affaire Thalès et le non-usage immodéré de l'exception d'ordre public, Gazette du palais, 2005, n°295, p419.

La CCJA et la propriété intellectuelle ou lorsque les plaideurs s'emmêlent

CCJA, 22 novembre 2022, Arrêt N° 173/2022 du 24 novembre 2022

Par Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APIA

Messieurs FATIME ASSILECK, ABDRAMAN AHMAT et HAROUN ADAM ABAKAR sont condamnés par la Cour d'appel d'Abéché (Tchad)[173] à payer à Monsieur MAHAMAT ADAM ABAKAR la somme d'un million FCFA à titre de dommages-intérêts.

Pour recouvrer la somme qui lui est due, Monsieur ABAKAR fait pratiquer une saisie-attribution des créances sur les avoirs de ses contradicteurs logés dans les livres de trois banques. Messieurs AHMAT et ABAKAR ont saisis la Cour suprême du Tchad aux fins de sursis à exécution de l'arrêt de la Cour d'appel d'Abéché.

La Cour suprême du Tchad a alors, dans une décision du 12 juillet 2021[174] ordonné le sursis à exécution de la décision de la Cour d'appel. Le saisissant s'est alors pourvu en cassation de devant la Cour commune de justice et d'arbitrage (CCJA) de l'OHADA qui a rendu sa décision le 24 novembre 2022[175].

Cet arrêt revêt un triple intérêt. D'abord dans la mesure où il porte sur la compétence de la CCJA, concernant des litiges en lien avec la propriété intellectuelle. Ensuite parce qu'il illustre la question de la cohabitation entre la CCJA et les Cours suprêmes des Etats de l'OHADA et enfin dans la mesure où il clarifie l'application de l'Acte uniforme relatif aux voies d'exécution.

Seul retiendra ici l'attention la question de la compétence de la CCJA en application de l'article 14 du traité OHADA. Ce texte dispose que *« la Cour Commune de Justice et d'Arbitrage assure l'interprétation et l'application commune du traité ainsi que des règlements pris pour son application, des actes uniformes et des décisions »*. Cette question de la compétence de la CCJA est directement liée à celle de l'application du droit OHADA lorsque le litige a un lien avec un droit régi par le Droit OAPI. Elle illustre la nécessité d'articulation des compétences juridictionnelles et normatives entre l'OHADA et l'OAPI[176].

Pour contester la compétence de la CCJA, le débiteur a argué du fait que la condamnation à l'origine de la voie d'exécution mise en œuvre est relative à un droit de propriété intellectuelle. Il s'agit d'une interprétation erronée de l'article 14 du Traité OHADA.

En effet, il y a lieu de faire une distinction. Soit le litige porte sur une procédure spécifique aux droits de propriété intellectuelle régis par l'OAPI (la saisie-contrefaçon par exemple) ou sur un aspect de droit substantiel prévu par le corpus de l'OAPI, y compris complété par des textes nationaux (en droit d'auteur principalement), alors le droit OHADA n'est pas applicable. Dans cette hypothèse, la CCJA n'est pas

[173] Arrêt n°001/2021 du 27 avril 2021
[174] Arrêt n°74/CS/CJ/SC/2021
[175] Arrêt N° 173/2022

[176] L.Y. Ngombé, « Droit OHADA et Droit OAPI : actualité et virtualités d'une concurrence normative », *Mélanges Dorothée Sossa,* éditions du CREDIJ, 2021, pp. 397

compétente, comme elle le rappelle avec constance[177].

Soit, comme c'est le cas dans l'affaire rapportée, il s'agit d'exécuter une décision de justice en appliquant la législation en la matière. Dans cette hypothèse, sauf règles spéciales, le droit applicable (y compris dans seize Etats de l'OAPI sur dix-sept) est le droit OHADA et plus précisément l'Acte uniforme portant organisation des procédures simplifiées de recouvrement et des voies d'exécution.

C'est donc sans surprise, que la CCJA a, dans une décision qui ne peut qu'être approuvée, fait droit à la demande du saisissant en rappelant qu'elle décide : *« de manière constante, que dès lors que la décision d'une juridiction nationale de cassation peut avoir des interférences directes sur la mise en œuvre du contentieux des Actes uniformes, elle fait conséquemment partie de celles « non susceptibles d'appel rendues par toute juridiction des Etats parties ».* Ce qui était bien le cas en l'espèce puisque le litige, qui a fait l'objet d'une décision en d'appel, portait sur un saisie-attribution de créance. Peu importe que l'origine de la créance réside dans une violation d'un droit de propriété intellectuelle[178].

Y.L.N.

[177] Voir par exemple Ngombé, « Les plaideurs insistent, la Cour persiste…et signe, CCJA, 1ère ch.,17 février 2022, pourvoi n°261/2021 **» :** *RSPIA* 2023, n°3, p.65.

[178] Dans le même sens, Cour d'appel de Niamey, Niger, arrêt no 2 du 5 mars 2008, *Société Rothmans of Pall Mall Limited c La Société Adil Compagny SA : Cahier de la propriété Intellectuelle,* Volume 26, Numéro 3, octobre 2014, p. 786, obs. Ngombé.

- **AU-DELA DE L'AFRIQUE**
  - **ETATS-UNIS/EUROPE**

Les travaux des IA dans les balances de la justice ou le purgatoire juridique d'« Une Récente Entrée dans le Paradis ».

United States District Court, District of Columbia. Stephen Thaler v. Shira Perlmutter, Register of Copyrights and Director of the United States Copyright Office, et al., Defendants. Civil Action No. 22-1564 (BAH), 18 août 2023

Par Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APIA

Une création artistique intitulée « A Recent Entrance to Paradise ». (Une entrée récente au paradis) » est générée par une Intelligence Artificielle. L'éditeur de l'intelligence artificielle a souhaité en faire un dépôt auprès du Copyright Office (Bureau du droit d'auteur).

L'éditeur indique alors dans sa demande d'enregistrement que l'auteur est une machine créative et que l'œuvre avait été « créée de manière autonome par un algorithme informatique fonctionnant sur un ordinateur ». Il précise également agir en qualité de cessionnaire de l'œuvre dont serait titulaire l'intelligence artificielle ayant généré de manière autonome la création.

La demande d'enregistrement a été refusée par le Copyright Office au motif que la création considérée n'était pas l'œuvre d'un être humain. Face à ce refus, l'éditeur, Monsieur Thaler a demandé, sans plus de succès, un réexamen du dossier en confirmant que la création en question était générée par une intelligence artificielle. La décision du Copyright Office est, en fait, conforme aux lignes directrices adoptée en mars 2023[179].

Puisque l'entrée de cette œuvre dans le champ de protection du droit d'auteur est refusée, l'éditeur de l'intelligence artificielle ayant généré « Une entrée récente au paradis » a décidé d'en référer à la justice.

L'affaire est alors portée devant le *United States District Court, District of Columbia* (le Tribunal) qui devait répondre à la question de savoir si une création générée par une intelligence artificielle peut être protégée par le droit d'auteur.

Le tribunal a, dans un jugement longuement motivé et didactique, rappelé que le droit d'auteur ne s'est jamais étendu au point de protéger les œuvres générées par de nouvelles formes de technologie fonctionnant sans intervention humaine. Le tribunal ajoute que l'un des fondements du Copyright réside dans le fait qu'un auteur ne peut être qu'une personne physique, un être humain.

Cette décision américaine peut avoir un écho tant en droit français que dans les Etats africains. Elle n'est pas sans rappeler ce qu'écrivait, il y a soixante-dix ans, René

[179] *U.S. Copyright Office, Library of Congress, Copyright Registration Gudance : Works Containing, Material Generated by Artificial Intelligence*, March 10, 2023, CFR part 202

Savatier qui relevait, à propos du sujet du droit d'auteur, que celui-ci ne peut être qu'une personne physique dans la mesure où l'œuvre est « ce clavier divin sur lequel joue l'inspiration, et que la loi protège précisément comme attribut de sa personnalité »[180]. L'intelligence artificielle n'ayant aucune personnalité, elle ne peut être titulaire d'un droit d'auteur. Et faute d'auteur, il n'y a pas création protégeable.

Dans une situation identique, l'application des lois des Etats africains serait-elle différente ? En compulsant les différentes lois des Etats africains, une solution identique devrait s'imposer aux juges. A titre d'exemple, dans l'espace OAPI, l'article 4 de l'Annexe VII de l'Accord de Bangui qui constitue un cadre normatif minimal prévoit qu'une œuvre protégée au titre du droit d'auteur est une création intellectuelle originale[181]. Or, la création originale s'entend, dans la majorité des lois des Etats membres, comme étant l'empreinte de la personnalité de l'auteur ou comme celle qui permet d'individualiser son auteur[182]. On chercherait vainement une empreinte de la personnalité d'une intelligence artificielle. La dimension personnaliste du droit d'auteur rend incompatible la notion d'originalité avec celle de création automatisée[183].

La porte reste néanmoins entrouverte lorsqu'un apport humain peut être décelé dans la création générée par une Intelligence Artificielle. Toute la question sera alors de savoir dans quel mesure un tel apport existe. Il s'agira alors de voir dans quelle mesure les *prompts* (consignes) dictés à l'intelligence artificielle ont été déterminants[184].

L'affaire « Une récente entrée au Paradis » illustre la difficulté qu'il y aurait à admettre, même dans le système du Copyright (tel qu'adopté dans les Etats africains anglophones), la protection d'une création générée par une intelligence artificielle. En effet, l'exigence d'originalité ne serait davantage pas satisfaite dans les Etats de l'ARIPO, par exemple, qui appliquent les critères de *skill, labour and effort*. Il semble en effet difficile, face à une création générée par une intelligence artificielle, de considérer qu'il existe un effort de création de la part d'un auteur (qui par définition n'existerait pas).

En tout état de cause, comme l'a rappelé le Tribunal dans cette affaire, encore faut-il que la création émane d'un individu, d'une personne physique, d'un être de chair et de sang. Seule une extension de la notion d'auteur à des systèmes automatisés pourrait permettre d'entrouvrir la porte du Droit d'auteur aux créations générées par des intelligences artificielles. Au cas d'espèce, « Une entrée récente au paradis », éconduite par le Copyright Office, n'avait aucune chance de succès dans les balances de la justice.

Les dispositions légales, par la voix des juges, ont cantonné cette création dans ce qui ressemble à un purgatoire juridique…en attendant une entrée, sans doute lointaine, dans le Paradis…du droit d'auteur.

Y.L.N.

---

[180] R. Savatier, Le droit de l'art et des lettres. Les travaux des muses dans les balances de la justice, LGDJ, 1953, n 146, p.109

[181] Accord de Bangui, Annexe VII, article 4

[182] Y.L. Ngombé, *Droit(s) africain(s) de la propriété littéraire et artistique,* PUAM 2022, n°58

[183] A. Lucas, A. Lucas-Schloetter et C. Bernault, *Traité de la propriété littéraire et artistique,* 5ème édition, LexisNexis, 2017, n°59

[184] Par exemple, Fabio Comparelli est-il auteur de l'histoire de l'art racontée par l'Intelligence Artificielle à laquelle il a donné des consignes ?

Un paradis fiscal n'est pas forcément un paradis numérique

L'affaire leclrec.com, Association des Centres Distributeurs E. Leclerc - ACD Lec, v. W S, WIS INC Affaire no. D2023-2315, Centre d'arbitrage et de médiation de l'OMPI, 15 septembre 2023

Par Yvon Laurier Ngombé,
Avocat, Docteur en Droit
Chargé d'Enseignements
Président de l'APIA

En septembre 2023, le Centre de Médiation et d'arbitrage de l'OMPI a rendu d'intéressantes décisions relatives à des affaires de typosquattage concernant des marques notoirement connues. Tel a, par exemple, été le cas s'agissant du nom de domaine *Lambroghini* qui portait atteinte aux droits de la société titulaire de la célèbre marque *Lamborghini.*

Dix jours après avoir ordonné le transfert du nom de domaine *Lambroghini* à la société Lamborghini[185], le Centre d'arbitrage et de Médiation a rendu une décision à la suite d'une plainte de l'Association des Centres Distributeurs E. Leclerc.

A l'origine de la plainte, la réservation du nom de domaine *leclrec.com* par une société installée aux Iles Caïman, territoire réputé pour être un paradis fiscal. La plaignante considère que ce nom de domaine crée une confusion avec la marque *Leclerc* sur laquelle elle a une légitimité. Au regard de ce qui n'est rien moins qu'un typosquattage, la plaignante a demandé avec succès le transfert du nom de domaine litigieux.

La commission administrative du Centre d'arbitrage et de médiation de l'OMPI a motivé sa décision en relevant d'abord que le nom de domaine litigieux est « confusément similaire » à la marque LECLERC sur laquelle la plaignante a des droits. L'inversion des lettres « e » et « r », précise la commission, est insuffisante à dissiper cette confusion.

La commission constate ensuite que la défenderesse (qui n'a pas adressé d'observation à la Commission) n'a pas de droits ou d'intérêts légitimes sur le nom de domaine litigieux et qu'elle n'a pas prouvé être autorisée par le titulaire de la marque à en faire un quelconque usage.

Enfin, la Commission considère que les pièces produites par la plaignante prouvent que la défenderesse avait, au moment de la réservation du nom de domaine litigieux, connaissance de la marque LECLERC, et qu'elle a agi de mauvaise foi. Elle relève le défendeur a intentionnellement tenté d'attirer, à des fins commerciales, des internautes vers son site web ou tout autre site en ligne, en créant un risque de confusion avec la marque LECLERC.

Face à cet acte manifeste de typosquattage, la défenderesse, quoiqu'installée dans un paradis fiscal, ne pouvait que se voir appliquer les règles UDRP[186] de résolution de litiges relatifs aux noms de domaines. Ainsi, certains paradis éloignent du droit fiscal sans permettre d'échapper au droit du numérique.

Y.L.N.

---

[185] Automobili Lamborghini S.p.A. v. Jinsoo, Yoon Case No. D2023-2655, Centre d'arbitrage et de Médiation de l'OMPI, 5 septembre 2023

[186] Uniform Domain Name Dispute Resolution Policy. Ces règles sont celles appliquées par le Centre de Médiation et d'arbitrage de l'OMPI. Certaines Chartes de nommage des Etats africains y renvoient (voir Ngombé, « Propriétés intellectuelles et commerce électronique dans l'espace OAPI et dans l'espace OHADA », *Recueil Penant* avril-Juin 2021, p. 277

L'originalité de la marque : quand les juridictions se jouent des *faux-amis*

Tribunal de l'UE, affaire T-324/22, Ecoalf Recycled Fabrics c. EUIPO, Décision du 13 septembre 2023

Par Christian Kpolo
Avocat au Barreau de Paris
Docteur en droit – Chercheur Associé
Université de Lorraine et Université d'Abidjan

Le 15 décembre 2020 la société Ecoalf Recycled Fabrics, SL (la requérante) a présenté à l'EUIPO une demande d'enregistrement de marque de l'Union européenne pour le signe verbal BECAUSE THERE IS NO PLANET B. La marque demandée désignait les produits relevant des classes 3, 16, 18 et 21.

Par décision du 24 septembre 2021, l'examinateur de l'EUIPO a rejeté la demande d'enregistrement de ladite marque, sur le fondement de l'article 7, paragraphe 1, sous b) du règlement (UE) 2017/1001 du Parlement européen et du Conseil, du 14 juin 2017, sur la marque de l'Union européenne.

Le 18 novembre 2021, la requérante a formé un recours auprès de l'EUIPO contre la décision de l'examinateur. Par la décision attaquée, la chambre de recours a rejeté le recours au motif que la marque demandée était dépourvue de caractère distinctif. Elle a notamment considéré que cette marque serait perçue par le public pertinent comme un slogan dont la nature serait purement promotionnelle, et non pas comme une indication de l'origine commerciale des produits en cause.

Dans sa décision du 13 septembre 2023, le tribunal de l'UE confirme le rejet de la demande de marque sur la base du fait l'expression « because there is no planet B » ayant une signification claire et étant conforme aux règles de la grammaire anglaise et, de surcroît, étant notoirement utilisée dans le cadre de la lutte contre le changement climatique, elle ne possède aucune originalité ou prégnance, ne nécessite pas un minimum d'effort d'interprétation, ni ne déclenche un processus cognitif auprès du public pertinent. En outre, le tribunal la chambre de recours a correctement considéré que la marque demandée sera perçue par le public pertinent comme un simple slogan promotionnel.

La réponse du Tribunal n'est pas surprenante en soi, mais ce qui intrigue c'est que, pour parvenir à sa décision, la juridiction ait suivi l'argument selon *« l'expression « planet B » est dépourvue d'originalité »*. Il y a de quoi faire tiquer les puristes du droit de la propriété intellectuelle pour qui le terme d'originalité ne doit être strictement utilisé que dans l'analyse des critères de protection de l'œuvre de l'esprit (en droit d'auteur)[187]. Il serait par ailleurs fâcheux de ne s'en tenir qu'à la formule utilisée par la juridiction, car d'un autre côté, l'originalité à laquelle elle fait allusion ne devrait pas être considérée au sens du droit d'auteur mais plutôt … au sens du langage courant à savoir *« Caractère d'une personne dont le comportement s'écarte de l'usage commun ; singularité, bizarrerie »*.[188]

Originale comme démarche… n'est-il pas ?!

Ch.K.

[187] S. Hans, *L'originalité au sens du droit d'auteur : contribution à l'étude de la notion*, thèse, Université Paris 1 Sorbonne, 1991.

[188] V° « Originalité », Dictionnaire de l'Académie française, 9e édition.

Clarification par la Cour de cassation de la date limite de dépôt d'une demande divisionnaire de seconde génération

Cour de cassation, Chambre commerciale, 30 août 2023, n°20-15.480

Par Christian Kpolo
Avocat au Barreau de Paris
Docteur en droit – Chercheur Associé
Université de Lorraine et Université d'Abidjan

Dans une récente affaire portée devant la Cour de cassation, qui s'est déroulée le 30 août dernier, la société Kubota Corporation s'est retrouvée au cœur d'une problématique complexe liée à ses demandes de brevet. Pour bien comprendre le contexte, examinons le déroulement chronologique de ces demandes. Tout a commencé par le dépôt initial d'une demande de brevet par Kubota Corporation. Sept années se sont écoulées, puis la société a introduit une première demande divisionnaire. Plus tard, en 2018, elle a soumis une seconde demande divisionnaire. Cependant, cette dernière demande a été rejetée par le directeur général de l'Institut national de la propriété industrielle (INPI).

Le litige qui s'est ensuivi portait sur la date limite jusqu'à laquelle un déposant de brevet est habilité à présenter une nouvelle demande divisionnaire. Pour trancher cette question délicate, la Cour de cassation a fait référence à l'article L. 612-4 du Code de la propriété intellectuelle. Cet article dispose que la demande de brevet ne peut porter que sur une invention ou un groupe d'inventions étroitement liées, formant ainsi un seul concept inventif général. Toute demande ne respectant pas cette disposition doit être divisée dans un délai prescrit. Les demandes divisionnaires bénéficient de la date de dépôt de la demande initiale, ainsi que de la date de priorité, le cas échéant.

La réponse de la Cour de cassation s'est basée sur une analyse approfondie de la pratique européenne en matière de demandes divisionnaires. Elle a noté que les directives en vigueur à l'Office européen des brevets (OEB) depuis le 1er novembre 2018 définissent l'expression « demande antérieure » comme faisant référence à la demande la plus proche sur laquelle la demande divisionnaire est fondée. Cette terminologie a remplacé celle de "demande initiale" qui figurait précédemment dans l'article 76 de la Convention de Munich sur la délivrance des brevets européens.

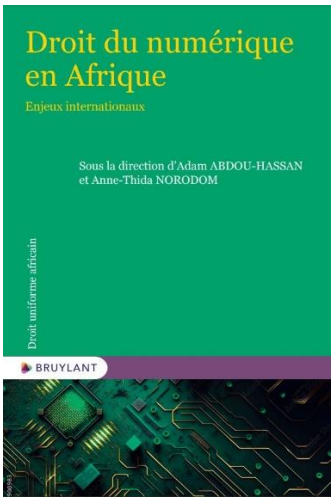
Avant 2011, l'INPI acceptait le dépôt d'une nouvelle demande divisionnaire jusqu'à la date de paiement des frais de délivrance et d'impression du fascicule du brevet issu de la première demande divisionnaire. La Cour de cassation a donc invalidé la décision de la Cour d'appel qui avait rejeté le recours de la société déposante de brevet. Elle a souligné que dans l'article R 612-34 du Code de la propriété intellectuelle, le terme "brevet" se réfère à l'expression "demande de brevet initiale" figurant dans la même phrase.

Cette disposition vise la première demande de brevet avant toute division et fixe ainsi une date de dépôt applicable à toutes les demandes divisionnaires ultérieures, sans possibilité d'interprétation différente. Par conséquent, la seconde demande divisionnaire soumise par la société après le paiement des frais de délivrance et d'impression du fascicule du brevet a été considérée comme irrecevable.

Ch.K.

BIBLIOGRAPHIE

Ouvrages



Le premier ouvrage sur le droit du numérique en Afrique est paru en septembre 2023 aux éditions Bruylant, sous la direction d'Adam ABDOU-HASSAN, docteur en droit public, et d'Anne-Thida NORODOM, professeur de droit public à l'Université Paris Cité.

L'ouvrage rassemble des contributions d'universitaires et de praticiens, en français et en anglais, sur les organisations internationales investies dans la gouvernance de l'Internet, les transformations étatiques, la cybersécurité, la fiscalité numérique, la protection des données, l'accès à Internet et à ses contenus. On y trouve également des articles sur le développement économique, les activités spatiales, l'éducation et la culture, ainsi que les droits de l'homme.

Sans aucun doute, cet ouvrage de droit international est bienvenu dans un contexte économique globalisé.

I.R.

Cinq ans de recherche sur le droit des affaires à l'épreuve de la digitalisation, en collaboration entre l'Institut François Gény, l'unité de recherche Confluence Sciences & Humanités, le laboratoire Transversales et le Centre de recherches juridiques de l'Université Grenoble Alpes, ont abouti à la publication d'un ouvrage collectif *Droit des affaires et intelligence artificielle*, sous la direction de Iony Randrianirina (UGA), Michel Cannarsa (UCLy), Jean-Luc Piotraut (Université de Lorraine) et Alexandre Quiquerez (Université Lumière Lyon 2).

Les contributions d'universitaires et de praticiens portent sur la blockchain, les *smart contracts*, les directives DSA et DMA, les productions générées par IA, les nouvelles pratiques bancaires, la cybercriminalité, les start-ups, le droit financier, l'arbitrage international.

I.R.

Baudin L., *Cyberattaques et droit international public : de la négociation entre états à l'intégration des acteurs privés pour parvenir à la cyberpaix ?*, Coll. « Logiques Juridiques », L'Harmattan, 2023, 418 pages

Brandre L., *Protection des données à caractère personnel en côte d'ivoire : comprendre les textes de loi*, Éd. Le livre en papier, 2023

Brandre L., *Protection des données à caractère personnel en côte d'ivoire : les bases légales en droit positif ivoirien*, Éd. Le livre en papier, 2023

Cluzel-Métayer L. et Sée A. (ss dir.), *Eléments de droit public du numérique*, Coll. « Logiques Juridiques », L'Harmattan, 2023, 176 pages

Demay S., *La charge de travail à l'ère du numérique : Réflexion sur la santé au travail, ?*, Coll. « Le Droit aujourd'hui », L'Harmattan, 2023, 306 pages

Fotso E. D., *Droit des affaires en Afrique - Recueil de jurisprudence 2022 : Cour commune de Justice et d'Arbitrage (CCJA-OHADA), cours d'appel, tribunaux de commerce*, LegiAfrica, 2023, 478 pages

Kianguebeni U. K., *Droits linguistiques et patrimoine immatériel au Congo*, Edilivre, 2019, 218 pages

Konaté M. K., *Contentieux du droit communautaire africain : Le juge national et le contentieux des normes communautaires de l'UEMOA*, Coll. « Harmattan Mali », L'Harmattan, 2023, 140 pages

Kutnjem A. M., *Introduction générale au droit camerounais du sport*, Coll. « Etudes africaines », L'Harmattan, 2023, 356 pages

Mpakam R. E., *Des brevets en droit congolais : Recherche d'informations et systèmes juridiques de leur protection,* Éd. Academia, 2023, 256 pages

Mvomo Ela P., *La protection de la culture au Cameroun : Enjeux et perspectives,* L'Harmattan, 2023, 232 pages

Sall A., *Singularités juridiques africaines : Ce que l'Afrique apporte au droit*, L'Harmattan, 2023, 322 pages

Semo Miekountima V. F. M., *Le juge et la cybercriminalité au Congo*, Coll. « JAMA », L'Harmattan, 2023, 224 pages

Traoré M., *Le règlement des litiges commerciaux en Afrique de l'Ouest,* Coll. « Etudes africaines », L'Harmattan, 2023, 368 pages

Articles de doctrine et chroniques de jurisprudence

Johnson-Ansah A., « Commerce électronique et épuisement du droit des marques dans l'espace OAPI », *Penant* 2023, n° 922, p. 167

Ngombé Y. L. (ss la dir. de), Ch. Kpolo, J.-P. Koso Omambondi, R. Mabouana, « Contentieux des signes distinctifs et de la concurrence déloyale en Afrique », *Propr. Industr.* 2023, n°6, étude 7

Savom Ambara R., « Étude comparée des mesures probatoires de la contrefaçon des œuvres de l'esprit dans l'accord de Bangui de 2015 et la loi n°2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins », *RFPI* n°17, octobre 2023, p. 31

Sawadogo F. M., « La construction d'un modèle de droit d'auteur pour l'OAPI : analyse de la technique légistique », *Penant* 2023, n° 922, p. 255

I.R., A.N., Y.L.Y., F.K. & Ch.K.

Revue Semestrielle de la Propriété Intellectuelle en Afrique

Revue de l'Association pour la Promotion de la Propriété Intellectuelle en Afrique (APIA)

Association enregistrée sous le n° W912014459

www.apia-asso.org

Revue Semestrielle de la Propriété Intellectuelle en Afrique

PLANNING PRÉVISIONNEL DES ACTIVITES DE L'APIA 2023

Podcast | Le Balafon	*Mars 2023*
BSPIA n° 3	*Avril 2023*
Podcast | Le Balafon	
Podcast | Le Balafon	*Mai |Juin |Juillet | Août 2023*
Journée de la recherche scientifique	*Septembre 2023*
RSPIA n° 4	*Octobre 2023*
L'arbre à Palabres de l'APIA	*Décembre 2023*
Assemblée Générale Annuelle	*Décembre 2023*

ISSN 3000-0025

n°4 October 2023

APIA

Semi-Annual Review of the Intellectual Property in Africa

Editorial	112
Portraits	113
Zoom	117
Study	126
Country sheet	136
News from APIA	138
Overview of case law	141
The decision of the semester	143
The digital semester	147
Academic activities	180
The pilgrim's semester	188
Bibliography	203

ISSN 3000-0025

Semi-Annual Review of the Intellectual Property in Africa

Journal of the Association for the Promotion of Intellectual Property in Africa (APIA)

Association registered under n° W912014459

www.apia-asso.org

EDITORIAL BOARD

Director of Publication
NGOMBÉ Yvon Laurier
Founder and President of the APIA Association
presidence@apia-asso.org

Editors-in-Chief
KPOLO Christian, ÉKANDZI Nilce
secretariat@apia-asso.org

Editorial Secretaries
KOUADIO Firmin, NGOMBÉ John-Pierce
publication@apia-asso.org

*****

Scientific Committee

FOMETEU Joseph
Full Professor, University of Ngaoundéré WIPO Expert (Cameroon)

JOHNSON-ANSAH Ampah
Professor, University of Lomé (Togo)

KIMINOU René
Lawyer, Full Professor
University of the West Indies and Guyana (France and Congo)

MONTCHO-AGBASSA Eric
Full Professor, University of Cotonou (Benin)

NDEMA-ELONGUE Max-Lambert
Senior Magistrate (Cameroon)
WIPO Expert

NGOMBÉ Yvon Laurier
Doctor of Law, Attorney at Law
Lecturer, WIPO Expert
(France and Congo)

NWAUCHE Enyinna
Full Professor, Nelson Mandela School of Law
University of Fort Hare (South Africa)

RANDRIANIRINA Iony
Professor, University of Grenoble
(France and Madagascar)

THIAM Samba
Full Professor Exceptional class
Cheikh Anta Diop University of Dakar (Senegal)
Lawyer, Member of CAMES

*****

Editorial Board

BILONG BILONG Abel
Doctor of Law, Lecturer

ÉKANDZI Nilce
Doctor of Law, Lawyer
Member of CEIPI, WIPO Expert

ÉKÉMÉ Isabelle
OAPI accredited agent

FOUDA Armelle
OAPI accredited agent

GOUADI Koussiama
OAPI accredited agent

KOUADIO Firmin
Lawyer, author

KOSO OMAMBODI Jean-Paul
Doctor of Law, Lawyer
Teacher-Researcher

KPOLO Christian
Doctor of Law, Lawyer, Lecturer
University of Lorraine and University of Abidjan

MABOUANA Roger
Lawyer

MOUBÉRI Abel
Engineer

NGANZI NDONI Théodore
Doctor of Law, Lawyer
Teacher-Researcher

NGOMA Marie-Alfred
Journalist

NGOUÉ Aline
Doctor of Law, Lecturer

OMAR AMINE Yasser
Doctor of Law, Lawyer
Teacher-Researcher

RANDRIANIRINA Roland
Engineer

TANO-BIAN Jeanine
Doctor of Law, cybersecurity consultant, lecturer and researcher, University of Abidjan

SAMB Abibatou
Lawyer

SOUMARÉ Youssou
Lawyer, Former Director of the Legal Department
Senegalese Copyright Office

WEMBO Paulin
Hearing magistrate

NOTE TO AUTHORS

All those wishing to publish their manuscripts should send them in digital form in Word format (as an attachment) to publication@apia-asso.org

The manuscript must be accompanied by a summary in French and English of a maximum of 1500 characters (not including spaces). Contributions are subject to reading/validation by the Scientific Committee and, if necessary, re-reading by the Editorial Committee. Manuscripts must be submitted at least 90 days before the desired publication date (15 January for the April issue, 1er August for the October issue).

RSPIA welcomes articles that are mainly (but not exclusively) concerned with intellectual property law in Africa. It also welcomes all scientific productions relating to business law in Africa, to emerging and cross-cutting issues or to analyses involving a comparative approach with a link to African legislation. The scientific committee has a discretionary power to assess the relevance of the subject proposed by the authors.

The maximum number of pages required, depending on the type of article, is as follows:

- Free speech or quick overview: 5 pages
- Case law reviews: 5 pages
- Commentary on legislation: 10 pages
- Studies or feature articles : 20 pages

The authors assign their economic rights to the manuscript free of charge and exclusively. The authors are solely responsible for the opinions expressed in their manuscripts.

The contributions to this issue were proofread and edited by
Yvon Laurier Ngombé, A. N., John-Pierce Ngombé and Christian Kpolo

CONTENTS

EDITORIAL

" A long road to protection? ", p. 112
By Yvon Laurier Ngombé

PORTRAITS

"Miriam Makeba, Angélique Kidjo and Aïcha Koné", p. 113
By The APIA Board

ZOOM

"The current state of intellectual property in the ARIPO area and in English-speaking African states in 2022", p. 117
By Enyinna Nwauche

STUDY

Copyright and image rights in the exploitation of visual works in the Democratic Republic of Congo, p. 126
By Théodore Nganzi Ndoni

COUNTRY SHEETS

"Côte d'Ivoire", p. 136
By Firmin Kouadio

ECHOES OF APIA

***"Le Balafon,* APIA Podcast", p. 138**
By The APIA Board

"2e APIA Scientific Research Day, p. 140
By The APIA Board

OVERVIEW OF CASE LAW

p. 141 *By Christian Kpolo*

THE DECISION OF THE SEMESTER

"Jurisdictional issues relating to trademark ownership disputes. About the case *'Elsafeer Falcon Pack Egypt Industries c/ Falcon Pack et al*, p. 143 *By Yasser Omar Amine*

THE DIGITAL SEMESTER

Cybersecurity & E-Health

The liability of healthcare facilities management providers in the event of IT vulnerabilities: a study of French law (Part 1), p. 147
By Christian Kpolo

Network security in the OAPI and OHADA areas, p. 167
By Jeanine Tano-Bian

Expected entry into force: the Malabo cybersecurity convention, p. 173
By Jeanine Tano-Bian & Christian Kpolo

Actors' cybersecurity obligations: analysis of the cybersecurity provisions in the Democratic Republic of Congo's new digital law, p. 174
By Jeanine Tano-Bian & Christian Kpolo

Electronic commerce

Provisions on the liability of technical intermediaries in the DRC's new Digital Act, p. 176
By Yvon Laurier Ngombé

Personal data and NICT

Review of personal data in Africa, p. 178
By Aline Mbenoun-Ngoué & Iony Randrianirina

ACADEMIC ACTIVITIES

Review of scientific works, p. 180
By Montcho Agbassa Éric, Ampah Johnson-Ansah & Yvon Laurier Ngombé

University news, p. 187
By Aline Mbenoun-Ngoué

THE PILGRIM'S SEMESTER

Beyond Intellectual Property

Arbitration and collective proceedings under OHADA and Moroccan law, p. 188
By Youssouf Adoum Youssouf

The CCJA and intellectual property or when litigants get tangled up *CCJA, 22 November 2022, Judgment No. 173/2022 of 24 November 2022*, p. 196
By Yvon Laurier Ngombé

Beyond Africa

The work of AIs in the scales of justice or the legal purgatory of "A Recent Entry into Paradise ", p. 198
By Yvon Laurier Ngombé

A tax haven is not necessarily a digital haven, p. 200
By Yvon Laurier Ngombé

Trademark originality: when the courts play *false friends off against each other* p. 201
By Christian Kpolo

"Clarification by the French *Court de Cassation* of the deadline for filing a second-generation divisional application", p. 202
By Christian Kpolo

BIBLIOGRAPHY, p. 203
By Iony Randrianirina, Firmin Kouadio, Christian Kpolo, Yvon Laurier Ngombé

EDITORIAL

A long road to protection?

By Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

Sixty years ago now, or rather just sixty years ago, or already sixty years ago... who cares? In 1963, on the banks of a majestic and famous river, a meeting was held which opened the debate and the way to the protection of a particular subject of intellectual property. From 5 to 10 August 1963, an "African Study Meeting on Copyright" was held in Brazzaville, Congo (organised by the Berne Union and Unesco). Following this meeting, it was decided to consider copyright protection for folklore.

Since then, a number of legislators in Africa (starting with Tunisia in 1966) and elsewhere (including Bolivia in 1967) have tried to open the door of copyright to "works of folklore". The 1976 Tunis model law, which for a long time served as a model for African legislators, provided for the possibility of protecting this rather misidentified object.

This was followed by a doctrinal craze, then inevitable and sometimes fascinating (even passionate) controversies. Subsequently, several specialists and many legislators felt that folklore should be subject to a special regime in view of its specific nature. Some texts focused more on the notion of the expression of folklore rather than that of a work of folklore. Today, the internationally accepted term is traditional cultural expression. Whatever the vocabulary, the subject remains the same and its protection under copyright is still provided for in several African laws relating to literary and artistic property, sometimes in a specific chapter.

For many specialists, traditional cultural expressions are not intellectual property. In reality, the path chosen at international and regional level is that of intellectual property. The only question is which one. In the ARIPO area, it is a *sui generis* right inspired by copyright and referring to customary rights.

All eyes are now on the instrument currently being adopted by WIPO. The countries that are home to the world's most widespread traditional cultural expressions are hoping for effective protection to prevent cultural appropriation or unfair enrichment of certain operators.

The success of an international instrument would contribute to the effectiveness of the expected protection, as the already numerous domestic laws cannot achieve this. Sixty years on, definitive adoption and mass ratification of the WIPO text would be a decisive step towards effective protection.

In the end, it doesn't matter what the intellectual property regime is, as long as the protection is effective and efficient.

Y.L.N.

PORTRAITS

Miriam Makeba, Angélique Kidjo and Aïcha Koné

"Women and Intellectual Property: Accelerating the pace of innovation and creativity". This is the theme of World Intellectual Property Day 2023.

The Association for the Promotion of Intellectual Property in Africa (APIA) wanted to mark the occasion. And to do so, the Association's board proposed to the editorial committee that the "Portrait" section of this issue be devoted to three African music divas.

Celebrating World Intellectual Property Day through the prism of women, and African artists in particular, is an opportunity to highlight not only the talent but also the cultural, social and political impact of those who have marked or are marking the history of music. RSPIA is therefore honoured to present a cross-portrait of Miriam Makeba, Angélique Kidjo and Aïcha Koné.

Miriam Makeba: The Voice of South Africa under Apartheid

Life and Journey

Miriam Makeba, nicknamed "Mama Africa", was born on 4 March 1932 in Johannesburg, South Africa. Her life was profoundly marked by the struggle against apartheid. Born in a country and at a time when segregation and oppression were daily occurrences, her life was littered with trials and struggles.

Musical Career

- **Early career**: Miriam began her musical career with the Manhattan Brothers before forming her own group, The Skylarks, which mixed jazz with traditional South African music.
- **Exile**: In 1959, after starring in the anti-apartheid documentary "Come Back, Africa", she was exiled from South Africa.
- **International success**: Makeba became the first African artist to popularise African music outside the continent, with hits such as "Pata Pata" and "The Click Song". Her duet with Harry Belafonte helped widen her audience outside Africa.
- **The UN and a return to favour**: In 1963, she testified before the UN against apartheid and her South African passport was revoked. Despite this forced exile, she continued to promote African music and culture throughout the world.

Notable anecdotes

- **Marriage and activism**: Miriam Makeba was married to Hugh Masekela and later to Stokely Carmichael, well-known activists, the former in music and the latter in civil rights.
- **Symbolic return**: After Nelson Mandela's release from prison in 1990, Miriam Makeba returned to South Africa, reconnecting with her homeland after decades in exile.

Inspiration and Influence

Miriam Makeba drew her inspiration from her South African roots and the struggles of her people. Her music reflects both the richness of African culture and a vibrant message of resistance against oppression. She has inspired artists and activists around the world with her grace, courage and determination.

Musical, social and political heritage

- **Musical**: Miriam Makeba left a repertoire that continues to be celebrated for its beauty and authenticity, becoming a timeless icon of African music.
- **Social**: Despite its worldwide success, it has always advocated equality, human rights and social justice.
- **Politics**: Miriam Makeba became a symbol of the fight against apartheid, using her voice and international platform to highlight the horrors of South Africa's segregationist regime.

Miriam Makeba's life and legacy are poignant proof of an artist's influence far beyond her art. Despite her international success, she never abandoned her identity or her convictions. Miriam Makeba embodies the resilience of the human spirit and the power one person has, not only to create beauty through music, but also to influence positive change in the world. The echoes of her voice and struggle still resonate in social justice movements and contemporary music.

* * *

Angélique Kidjo: World Music star and humanitarian activist

Life and Journey

- **Birth and childhood**: Angélique Kidjo was born on 14 July 1960 in Ouidah, Benin. She grew up in an environment where various types of music, including tribal traditions, pop, jazz and R&B, blended together.
- **Exile**: Due to the oppressive regime and unstable political climate in Benin, Angélique Kidjo went into exile in France at the age of 23 to pursue her passion, music, and escape the constant threat.

Musical career

- **Debut in France**: In Paris, she immersed herself in a variety of musical styles and quickly attracted attention for her powerful voice and electrifying stage presence.
- **International breakthrough**: His career took on an international dimension with albums such as "Logozo" and "Agolo", the latter earning him his first Grammy nomination.
- **Grammys and accolades**: Over the course of her career, Angélique Kidjo has won four Grammy Awards and been recognised for her unique musical style, which fuses different genres.

Notable anecdotes

- **Notable encounters**: She has collaborated with many famous artists, including Manu Dibango, Carlos Santana, Peter Gabriel, Ziggy Marley and Alicia Keys, forging links between different musical cultures.
- **TED Talk**: Angélique Kidjo gave a TED talk, sharing her vision of Africa, her experiences and her wisdom on the world stage.

Inspiration and Influence

- **Roots and musical diversity**: Inspired by the traditional music of her native Benin, funk, jazz and more, Angélique Kidjo creates a universal sound that defies borders and genres. She was inspired by Miriam Makeba and Bella Bellow.
- **Women's rights**: She also draws on her experiences as an African woman to address the themes of gender equality, women's empowerment and social justice in her work.

Musical, social and political heritage

- **UNICEF Ambassador**: She uses her fame to draw attention to issues such as education, health and the rights of girls and women in Africa and around the world.
- **Library of songs**: His musical heritage is a library of songs celebrating Africa, its culture, its struggles and its hopes.
- **Batonga Foundation**: She co-founded the Batonga Foundation, which works for the education of young girls in Africa, demonstrating her commitment to social and educational change.
- **Global influence**: Angélique Kidjo has not only influenced music around the world, but has also introduced African sounds to world pop, giving a voice to the voiceless.

Angélique Kidjo, with her distinctive blend of diverse musical styles and commitment to social justice and women's rights, is a force to be reckoned with in the global music industry and beyond. She eloquently demonstrates how music can be a bridge between cultures, peoples and causes, leaving a legacy that will resonate for generations to come, both musically and socially. Her activism in favour of just causes is perceptible in her fight for better protection of creators' rights, the most successful expression of which is undoubtedly her work within the International Confederation of Societies of Authors and Composers (CISAC), where she has held the position of Vice-President.

* * *

Aïcha Koné: The Melodious Voice of Côte d'Ivoire

Life and Journey

- **Childhood and first steps**: Born on 21 May 1957 in Abidjan, Côte d'Ivoire, Aïcha Koné is a Mandingo singer whose melodies have conquered not only West Africa, but the world. Her career began in her teens when she won a singing competition, heralding a rising star in the world of African music.
- **Political vicissitudes**: Her artistic career was marked by a luxuriant career but also by her interaction with politics, notably when she was forced into exile during a period of political unrest in Côte d'Ivoire.

Musical Career

- **Rise**: Aïcha quickly gained continental recognition for her powerful, expressive voice, winning acclaim in various African countries.
- **Musical characteristics**: His music, mainly zouk and coupé-décalé, is also infused with traditional sounds, creating a seductive and unique fusion.
- **Engaged songs**: Through her music, she deals with relevant social and political themes, lending her voice to the oppressed and the disenfranchised.

Notable anecdotes

- **Survivor**: Aïcha is also known for her resilience in the face of multiple challenges, including health problems and political obstacles, and continues to perform and produce music.
- **The Accomplished Artist**: She has sung in front of famous personalities.

Inspiration and Influence

- **Social inspiration**: Koné is deeply inspired by the society around him, using his music as a tool to discuss social and political issues.
- **Harmonies of tradition**: She skilfully integrates the harmonies of traditional African music with more modern genres, forming a captivating synergy between the old and the new.

Musical, social and political heritage

- **Music pioneer**: Aïcha Koné is regarded as one of the pioneers of African music, having paved the way for many of the continent's artists.
- **Social impact**: Through her songs and social involvement, she has played a key role in raising social and political awareness in various parts of Africa.
- **Educator**: Beyond her musical career, she has also devoted time to educating the younger generation about African values, traditions and history.

Aïcha Koné, with her moving voice and evocative melodies, remains an iconic figure in the world of African music. Her ability to blend the modern and the traditional, while tackling crucial issues with sensitivity and boldness, has earned her a respected place in the history of African music and culture. Her legacy continues to inspire, mobilise and educate, making her more than just an artist, but also an agent of change and a guardian of African tradition and consciousness.

The APIA Board.

Legal Developments In Anglophone Africa 2022

By Enyinna Nwauche
Full Professor, Nelson Mandela School of Law
University of Fort Hare (South Africa)

I. ARIPO

A. TREATIES

Recent amendments to the Harare Protocol on Patents and Designs

One of the resolutions of the ARIPO Administrative Council at its 46th Session that was held in Maputo, Mozambique, from 21st to 25th November 2022 was the adoption of the amendments to the Harare Protocol on Patents and Industrial Designs as well as its Implementing Regulations, which came into force on 1st January 2023.

The highlights of the 2022 Amendments to the Harare Protocol on Patents and Industrial Designs are as follows:

1. The preamble of the Harare Protocol was amended to include the Paris Convention and Patent Cooperation Treaty Articles.
2. New paragraphs 2 and 3 of Section 1 clearly defines the ARIPO patents, industrial designs and utility models and their national effect in Member States.
3. New Section 1bis amend Section 1 and introduce a new Section 1bis clearly indicating that an ARIPO patent, industrial design or utility model can have effect in any or all of the contracting states.
4. New Section 2(3) clearly facilitates applications by joint applicants designating different contracting states.
5. New Section 2(7) clearly supports Rule 5(2) in confirming the fact that application can be lodged in any language but must be translated to English within 2 months.
6. New Section 2(8) clearly defines the right of priority of each patent, industrial design or utility model.
7. New Section 3(1A to 1D) will clearly define that any ARIPO patent application will relate to one invention which will be clearly disclosed such that any person skilled in the art could reproduce the invention.
8. There is a need to link the physical requirements as defined in the Administrative Instructions as indicated in the new re-drafted Section 3, 2(A).
9. New Section 3(6A) clearly provides Member States the opportunity to either accept or refuse a patent granted or due for grant by the ARIPO Office. The old Section 3(6) will be re-numbered to 3(6B).
10. New Section 3(11A) clearly defines the novelty of an invention and the old Section 3(11) will be re-numbered Section 3(11G).
11. Section 3(11B) clearly defines prior art documents as everything made available to the public anywhere in the world by means of written disclosure (including drawings and other illustrations), oral disclosure or by use or exhibition, shall be considered prior art provided that such making available occurred before the date of filing of the application or, if priority is claimed, before the priority date validly claimed in respect thereof and further provided that a disclosure of the invention at an official or officially recognized exhibition shall not be taken into consideration if it occurred not more than six (6) months before

the date of filing of the application or, if priority is claimed, before the priority date validly claimed in respect thereof"

12. Section 3(11C) clearly defines exhibition in relation to the Convention on International Exhibitions.

13. New Section 3(11D) defines inventive concept of an invention.

14. New Section 3(11E) clearly defines industrial applicability of an invention lodged at ARIPO.

15. New Section 3(11F) clearly defines the possibilities for the amendment of an application.

16. Section 3(13A) provides for part or whole licensing in respect of the designated states.

17. New Section 3(13B) defines the assignment of an ARIPO patent.

18. New Sections 14A to 14E clearly define the ownership of the patent rights of an ARIPO patent and clearly indicates that in case of infringement, the national law takes precedence.

19. New Sections 3(15A to 15B) clearly defines the procedures for filing divisional applications with the Office.

20 New Section 3(16) clearly defines the terms and interpretation of the claims, description and drawings in an ARIPO application.

21. New Section 3(17) to 3(17)(iii)) clearly specifies the time limits laid down under the Administrative Instructions and Regulations for implementing the Harare Protocol.

22. New Section 3(18) clearly defines procedures for revocation or invalidation of an ARIPO patent.

23. Rule 5(3) amended to allow for electronic filling.

24. New Rule 5bis to allow for electronic filing of patents, industrial designs and utility model applications

25. Amended Rule 18bis (2) provides that novelty and industrial applicability instead of 'inventive step' within the Contracting States of the Protocol shall be applied with respect to utility models because for utility models inventive step is not taken into consideration and only novelty with reference to local documentation is taken into consideration.

26. Deletion of Rule 21 (3) is intended to remove the obligation of the Office to remind applicant or the owner of the patent to renew the patent or patent application at least one month prior to the date in which an annual maintenance fee shall fall due. This is to follow suit with other similar offices where applicants have to monitor the renewal dates of their respective patents or patent applications.

27. Amendment Rule 22(1) to include electronic communication between the Office and designated states.

Recent amendments to the Banjul Protocol on Marks

One of the resolutions of the ARIPO Administrative Council at its 46th Session that was held in Maputo, Mozambique, from 21st to 25th November 2022 was the adoption of the amendments to the Banjul Protocol on Marks as as well as its Implementing Regulations, which came into force on 1st January 2023.

The changes include an amendment to Rule 13*Bis* that includes the cancellation of a registered mark under Section 8:2 that should be communicated to the ARIPO Office in addition to other actions such as changes in registered particulars withdrawals of applications, cancellation of designated classes or reduction of classes.

There were also changes to the Banjul Protocol fees.

Emerging regulatory framework

Protocol on Geographical Indications

The ARIPO Administrative Council at its 45th Session in 2021 agreed to establish the ad Hoc Working Group on Geographical Indications and in 2022 is undertaking consultations on establishing a regulatory framework for managing Geographical Indications. A sub-working Group on Geographical Indications made up of Ghana, Kenya, Liberia, Malawi, Mozambique, and Zambia is deliberating on a suitable legal framework, the registration process, the quality control and enforcement mechanisms.

II. SOUTH AFRICA

A. Legislation

Emerging Legislation

The Reform of South African Copyright Law

The process of legislative reform of South African copyright law began in 2009, with the Department of Trade, Industry, and Competition (currently the DTIC, formerly the DTI) commissioning a series of studies. In the aftermath of the studies and public engagement, the DTI, in 2010, established the Copyright Review Commission headed by Justice Ian Farlam, which deliberated on issues such as the distribution practices of collecting societies. The CRC recommended that the DTI begin the process of amending the Copyright Act of 1978. Draft amendments to the Copyright Act were published for public comment in 2015 a Copyright Amendment Bill (CAB) was introduced to the National Assembly. Several versions of the CAB have been introduced to the National Assembly with extensive public commentary and hearings. In 2019, South Africa's National Assembly and the National Council of Provinces (the NCOP) passed the Bill that was subsequently sent to the President for his assent so that the Bill could become law. The President did not assent to the CAB but referred it back to Parliament in June 2020 citing constitutional reservations. In August 2020 the Parliament began the process of addressing the presidential reservations through calls for comments, and public hearings which are still ongoing.

B. Case Law

Blind SA v Minister of Trade, Industry and Competition and Others Case [2022] ZACC 33

On Wednesday, 21 September 2022 at 09h30, the Constitutional Court handed down judgment in an application for confirmation of the order of constitutional invalidity made by the High Court of South Africa, Gauteng Division, Pretoria (High Court). The High Court declared the Copyright Act 78 of 1978 unconstitutional to the extent that it fails to make provision for exceptions that would enable, through the conversion of works under copyright, suitable formats that enable access. It ordered that the provisions of the Copyright Amendment Bill [B 13B – 2017] (CAB), as set out in section 19D of the CAB, be read as if specifically incorporated in the provisions of the Copyright Act to remove the inconsistency of the Act with the Constitution.

Before the Constitutional Court, the applicant, Blind SA, and the first respondent, the Minister of Trade, Industry and Competition (Minister) agreed that the Copyright Act is unconstitutional to the extent so declared by the High Court.

Professor Owen Dean, Media Monitoring Africa Trust (MMA) and the International Commission of Jurists (ICJ) were admitted as the first, second and third amici respectively. The crux of the matter concerned Blind SA's contention that the Copyright Act limits the availability of works under copyright in formats accessible to persons with print and visual disabilities.

The Copyright Act requires the consent of the copyright owner to convert works into formats suitable for the use of persons with print and visual disabilities. As a result, such persons suffer severe limitations in accessing works under copyright that persons without these disabilities do not encounter. There is a legislative process under way to amend the Copyright Act. This process has endured since 2015. On 28 March 2019, Parliament passed the CAB. The CAB sought to introduce section 19D in terms of which prescribed persons may, without the authorization of the copyright owner, make, supply and undertake any intermediate steps to provide an accessible format copy for the benefit of a person with a disability; thus providing exceptions to copyright protections so as to allow blind and visually impaired persons and persons with other disabilities to access such works in formats that are appropriate for their particular disabilities.

On 16 June 2020, the CAB was referred back to the National Assembly by the President in terms of section 79(1) of the Constitution. Aggrieved by this lengthy legislative process, Blind SA approached the High Court for an order declaring the Copyright Act unconstitutional to the extent that it unjustifiably limits the rights of persons with visual and print disabilities.

On 7 December 2021, the High Court declared the Copyright Act to be unconstitutional to the extent that it fails to make provision for exceptions that would enable, through the conversion of works, access to such works by persons with visual and print disabilities. The application was unopposed. The High Court found that, acting in line with the declaration of intent to ratify the Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled (Marrakesh Treaty), Parliament adopted the CAB which proposes the insertion of the new proposed section 19D to create exceptions for the benefit of the blind and people with visual and print disabilities.

The Court found the delay to be unreasonable and contrary to section 36(1) of the Constitution as it unjustifiably perpetuates the violation of the rights of the blind, and visually and print disabled persons. In a unanimous judgment penned by Unterhalter AJ, the Constitutional Court confirmed the order of constitutional invalidity made by the High Court.

The Court first identified the case pleaded by Blind SA to be the scarcity of published literary works in accessible format copies for the use of persons with visual and print disabilities. A scarcity that is attributable to the difficulty of securing the required authorisation of the owners of copyright in literary works. Having identified the case advanced by Blind SA, the Court then identified what the case was not about: (a) the need for access to unpublished literary works; (b) the importation and exportation of copyrighted works and (c) a challenge to bring Parliament's delay under constitutional review.

The Court held that legislation that protects the rights of copyright owners must take account of the differential impacts of such protection upon different classes of persons. Therefore, where those with print and visual disabilities suffer great and particular hardship by reason of the requirement of authorisation, the requirement could not be applied as if all persons who need access to literary works were similarly situated. It found that to apply the requirement of authorisation to all exposed those with print and visual disabilities to the damaging scarcity of literary works. That constituted unfair discrimination on the grounds of disability, and thus infringed section 9(3) of the Constitution. In addition, the Court also found this requirement to infringe the rights of persons with print and visual disabilities as contemplated in sections 10 (dignity), 16(1)(b) (freedom of expression), 29(1) (right to basic and further education) and 30 (language and culture) of the Constitution, for like reasons.

The Court then considered whether the powers conferred upon the Minister in terms of section 13 to issue regulations in respect of general exceptions in the reproduction of works saved the statute from constitutional invalidity. In determining this, the Court deliberated on the distinction between adaptation and reproduction as contemplated in the Act. It found that the exact boundary was hard to draw, more especially because the parties failed to make adequate submissions on this distinction. The Court assessed Article 4(1)(a) of the Marrakesh Treaty which states that "[t]he limitation or exception provided in national law should permit changes needed to make the work accessible in the alternative format". It found that the reproduction of literary works, no matter how generously interpreted, was insufficient for the conversion of literary works into accessible format copies for use by persons with visual and print disabilities. Therefore, section 13 did not save the Act from its constitutional invalidity.

Having found this, the Court assessed remedies to cure the constitutional invalidity. It found a reading-in of section 19D of the CAB to be too wide and imprecise. According to the Court, such a reading-in went beyond the case advanced by Blind SA and beyond the submissions made by the parties. Thus, the Court formulated an order that was responsive to the case that Blind SA had established.

The following important elements feature in the order: (a) sections 6 and 7 (these sections vest exclusive rights to copyright owners to perform a list of activities in respect of literary and artistic works), read with section 23 (this section sets out the circumstances under which copyright will be infringed) of the Copyright Act were declared unconstitutional, invalid and inconsistent with the rights of persons with visual and print disabilities, as set out in sections 9(3), 10, 16(1)(b), 29(1) and 30 of the Constitution, to the extent that these provisions of the Act limit the access of such persons to published literary works, and artistic works as may be included in such literary works, in accessible format copies; and (b) key terms such as "a person with a visual and print disability", "accessible format copy", "beneficiary person", "literary works" and "permitted entity" were defined to make the reading-in provision immediately operable.

Accordingly, the Court confirmed the order of the High Court declaring the Copyright Act unconstitutional, but only to the extent as identified above. It ordered a reading-in of section 13 of the Act under the heading "section 13A Exceptions applicable to

beneficiary persons". This reading-in is to endure for 24 months to enable Parliament to cure the defect in the Copyright Act giving rise to its invalidity.

III. NIGERIA

A. Legislation

Nigerian Copyright Law 2022

The Nigerian Copyright Act 2022 was assented to by the then President Buhari ending decades of reform advocacy and activism around the Nigerian Copyright Act 1988. The objectives of the Act are to protect the rights of autheors to earn just rewards; provide appropriate access to copyright works; facilaiutate Nigeria's compliance with obligations arsing from international obligations and enhance the regulatory capacity of the Nigerian Copyright Commission.

The highlights of the 2022 Act include the folowing:

- A modified Resale Right: The repealed 1988 Act had provided that authors (including heirs and successors in title) of artistic literary and musical works had a right to share in the proceeds of the sale of the original of that work or manuscript by public auction or through a dealer. Three-dimensional works were covered in that Act. The 2022 Act now expressly excludes architectural works and works of applied art.

- Exceptions and Limitations to Copyright

  - An enhanced defense of 'Fair Dealing': The 2022 Act provision that incorporates parts of the 'Fair Use' provisions of the United States Copyright Act. The 1988 Act had provided for a fair dealing exception in the second schedule to that Act and included research, private use, criticism, review, the reporting of current events: parody, pastiche or caricature as grounds of fair dealing amongst others. The 2022 Act has now brought fair dealing to the body of the Act and added 'non-commercial research and private study 'as additional grounds. Of importance is the addition of factors arguably borrowed from the United States Copyright Act to be considered in arriving at a determination of fair dealing such as the purpose and character of its usage; nature of the work; amount and substantiality of the portion used in relation to the work as a whole and the effect of the use upon the potential market or value of the work.

  - Access to Works in Terms of the *Marrakesh Treaty*: The 2022 Act makes provisions to give effect to Nigeria's obligations undertaken as a State party to the Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired or Otherwise Print Disabled.

- **Compulsory licences**

- Provisions Relating to Online Content:
  - The 2022 Act now entitles a copyright owner to issue a notice requesting a service provider to take down infringing content.

- An Enhanced Protection for Performers: The 1988 Act protected performers but in a skeletal form. What the 2022 Act has done is to enhance the protection of performers by defining performers; determining the nature and extent of the exclusive rights granted to performers; adding new exclusive rights such as fixation of unfixed performance; renting or lending to the public of a fixation of a performance; and making available to members of the public; recognizing the moral rights of a performer and the rights of performers in collective performances.

- Prohibition of the Circumvention of Technological Protection Measures: The 2022 Act prohibits the circumvention of a technological protection measure (TPM); dealing in a technology, product, service or part designed to circumvent a TPM as well as the manufacture of a product or device designed to circumvent a TPM. There are exceptions to this prohibition designed to protect lawful uses such as the exceptions and limitations to copyright; and the enhancement of interoperability of a computer program.

Business Facilitation (Miscellaneous provisions) Act, 2022 Act n°5

On 8th February 2023, President Buhari signed an Act that introduces measures designed to ease doing business in Nigeria by removing perceived bottlenecks and seeks to ensure transparency efficiency and productivity. The Act amends relevant legislation including amendment of the First Schedule to the Patents and Designs Act, Cap. P2, Laws of the Federation of Nigeria, 2004 by inserting, a new paragraph "13A" that entitles the Minister of Trade and Industries to make regulations to prescribe the procedure for the application, grant, use and withdrawal of compulsory licenses.

Nigerian Start Up Act 2022

In a strategic move to boost innovation in Nigeria, the Nigerian Start-Up Act 2022 was recently signed into law. The Act is designed to tackle several challenges for Nigerian startups including lack of an enabling environment, unclear regulatory framework; inadequate local content support; inadequate protection and incentives, like tax breaks, incentives to attract foreign capital and access to an exclusive list of public and private-led local funding opportunities.

The Council for Digital Innovation and Entrepreneurship will implement the provisions of the Act and comprises the president, the governor of Nigeria's apex bank, representatives of the Startup Consultative Forum, the Director-General of Nigeria's information and technology regulator and other key government and private officials.

Part of the statutory responsibilities of the Council and the Secretariate is to ensure that holders of intellectual property rights are encouraged to exploit these rights through internationalising and commercialising. To this end the Secretariat shall collaborate with the Nigerian Copyright Commission and the Trademarks, Patent and Design Registries, in ensuring that they designate a separate section on the Startup Portal to ease registration of intellectual property for labelled startups; provide assistance to labelled startups for facilitating the application for grant or revocation of patents and institution of legal action for infringement of any intellectual property rights ; and (c) facilitate assistance to labelled startups for the filing and registration of their trademarks and patents at the international level and generally to ensure that registration and protection of intellectual property of labelled startups is seamless.

III. BOTSWANA

Bostwana Intellectual Property Policy 2022

Botswana's national development Vision 2036 provides an anchor for this by envisioning an economy that is 'efficient, vibrant and knowledge-based, with access to a skilled and internationally competitive workforce, leading-edge technology and infrastructure' (Republic of Botswana, 2016). The Vision recognises the role of science, technology, innovation and creativity in creating a knowledge-basedeconomy, hence necessitating the development of a conducive environment through effective Intellectual Property (IP) policies, institutional and legislative frameworks. The country has outstanding IP potential; however, it has not recognised IP as a driver for economic development.

This is evidenced by lack of integration of IP in National Development Plans (NDP) leading to inadequate resources allocated for IP generation and exploitation, thus hindering the country from reaping the economic benefits of IP. This gap informed the need to develop the Intellectual Property Policy for Botswana. The Botswana Intellectual Property Policy was developed with the assistance of the World Intellectual Property Organization (WIPO). The primary objective of the Policy is to leverage Botswana's IP potential for inclusive and sustainable economic growth and development, which will deliver prosperity for every Motswana. It has six interrelated pillars, i.e., to improve the IP governance framework for promoting the protection of IP rights; to facilitate availability and access to financing for IP generation, acquisition and commercialisation; to promote IP awareness, education and training; to effectively negotiate IP Agreements for the benefit of Botswana; to develop entrepreneurship capacities in selected IPdriven sectors; and to create appropriate institutional structures for IP development. The successful implementation of the Policy will enable Botswana to use its IP potential towards being a KnowledgeBased Economy (KBE) and to diversify Botswana's economy to create prosperity for all.

IV. KENYA
INNOVATION MANAGEMENT
Innovation Management
Intellectual Property Rights Recordal System

In a move that is a precedent and likely to be widely copied across Africa, Kenya's Anti

Counterfeit Authority (ACA) has commenced an Intellectual Property Rights Recordal System. The system is designed to capture particulars relating to protected IP rights, IP rights holders/owners, and appointed agents in an electronic database known as AIMS. This information will be used by the ACA to combat counterfeiting by verifying the status of recorded IP rights and the relevant persons to contact in case of suspected IP rights infringement. AIMS can also be accessed by border protection officers to ascertain the recordation status of goods to be imported into Kenya.

Since the enabling Anti-counterfeit (Amendment) Regulations prohibit the importation into Kenya of goods bearing a trademark, trade name or copyright for commercial purposes unless the IP right is recorded, importers also have the responsibility of ensuring that IP rights relating to the imported goods are declared via the recordal system. Non-compliance by importers will result in prosecution, seizure of the non-compliant imported goods, and forfeiture for destruction by the ACA. In addition, they are liable on successful prosecution to a fine of not less than three to five times the value of the prevailing retail price of the goods, and/or imprisonment for a term not exceeding five to 15 years.

E.N.

Copyright and image rights in the exploitation of visual works in the Democratic Republic of Congo

By Thédore Nganzi-Ndoni

Doctorate in Law from the University of Kinshasa
Teacher at the Institut national des arts (Kinshasa)

Copyright enshrines a monopoly limited by exceptions strictly enumerated in the law. However, the limitation of the image right is not an exception to copyright within the meaning of the Berne Convention of 1886.

Image rights are not defined in positive Congolese law. Article 23.b[189] of Ordinance-Law No. 86/033 of 05 April 1986 on the protection of copyright and related rights in the Democratic Republic of Congo[190] simply establishes the right to an image as a limit to copyright. However, we can consider that this right is an integral part of the right to privacy, which is protected by article 31 of the 1986 Constitution of the Democratic Republic of Congo[191] .

Current criminal law punishes a number of breaches of privacy, including violation of the home, violation of correspondence secrecy, violation of professional secrecy[192] ... There is also Law No 96-002 of 22 June 1966 protecting freedom of the press, with special provisions governing press offences, including the right of reply, reply and correction[193] Ordinance-Law No 23-010 of 13 March 2023 on the digital code criminalizes the dissemination of tribalist, racist and xenophobic content[194] and child pornography[195] .

Analysis of these provisions confirms the absence of a clear legal definition of image rights in the Democratic Republic of Congo. Thus, to fill this gap, we can propose a definition of the right to image as the prerogative granted to any natural person to authorise his or her face or entire body to be represented or reproduced in the graphic or

[189] Article 23. B of the RDC Copyright Act 1986 provides that, in the case of a plastic work or a commissioned portrait, the author or owner of a portrait may not reproduce it or display it in public without the consent of the person depicted in it. This section creates a potential conflict between copyright and the right to the image of the person portrayed in the portrait.

[191] Article 31 of the Constitution states: "Everyone has the right to respect for his private life and the secrecy of his correspondence, telecommunications or any other form of communication. This right may not be infringed except in the cases provided for by law".

[192] Articles 69 to 75 of the decree of 30 January 1940 on the Congolese Criminal Code, still in force.

[193] Articles 37-43, 67-75, 79 of Act No. 96-002 of 22 June 1966.

[194] Article 356 of the Digital Code states: "Anyone who intentionally Creates, downloads, disseminates or makes available to the public by means of a computer system writings, content, messages, photos, sounds, videos, drawings or any other representation of ideas OR theories of a racist, tribalist or xenophobic in nature or in any form whatsoever within the meaning of this Ordinance-Law and in accordance with the provisions of Ordinance-Law no. 66-342 of 07 June 1966 on the repression of racism and tribalism, shall be punished by imprisonment of between one month and two years and a fine of between one million and ten million Congolese francs, or by one of these penalties only".

[195] Article 357 of the Digital Code states: "The act of producing, distributing, disseminating, importing, exporting, offering, making available, selling, procuring for oneself or for others, or possessing any pornographic material depicting a child by means of a computer system or an electronic communication network, is punishable by five to fifteen years' imprisonment and a fine of two thousand to one million Congolese francs".

plastic arts, by photography or by a similar technique[196] .

This right to the image, in the law of the Democratic Republic of Congo on copyright, simply creates a limit[197] to the exercise of copyright for creators of visual works, mainly portraits of individuals and photographs. The creator of such a work may not use it in public without the authorisation or consent of the person depicted in the portrait or photograph.

This legal provision is rare[198] in French-speaking Africa. Out of more than 20 French-speaking countries, only five have adopted this rule. We therefore question the appropriateness of such a provision in the 1986 Copyright Act of the Democratic Republic of Congo. Indeed, the right to an image is a personality right, the violation of which is normally covered by criminal or civil law[199] . It is a problem that comes under the ordinary law of liability. Curiously, the legislator of the 1986 Copyright Act included it in Article 23.b as a limit on the exercise of copyright. This risks creating a conflict between the two rights (copyright and image rights).

This potential conflict between the creators of visual works (commissioned portraits or photographs) and the people depicted in them is possible in several cases. Indeed, it is possible that image rights prevent an author from exploiting a photograph for the simple reason that he or she has not obtained the authorisation of the person depicted in the photograph. Conversely, an author may prevent the buyer of a commissioned portrait from using it for public exhibitions. On the other hand, the two rights can coexist peacefully when one of the rights holders (copyright or image right) obtains the authorisation of the other.

We will therefore examine two situations. The first concerns the coexistence of image rights and copyright (I). The second situation concerns the potential conflict between the two rights (II).

I. The coexistence of two rights

The coexistence of these two rights is possible in two cases. The first case concerns the situation of the owner of the image right who freely and expressly consents to the exploitation of his image by the author (A). The second case concerns the author's consent to the exploitation of his or her work by the holder of the image right (B).

A. Exploitation of copyright with the consent of the owner of the image right

An individual who commissions a portrait may subsequently authorise the painter or designer of that portrait to use it, for example, in the form of a postcard reproduction. In this case, the image of the person concerned

[196] Our definition is based on the Larousse dictionary, 2012 edition, which defines image as the representation or reproduction of an object or figure in the graphic and plastic arts...

[197] This limitation is a sui generis exception to copyright which differs from those in force in the Berne Convention of 1886. Articles 10 and 10bis of this Convention provide for limitations on copyright for illustrations in education and news reporting. The protection of images is not affected by these limitations.

[198] It is found in the following five laws: Republic of Congo law of 1982 (art.43); Gabon copyright law of 1987 (art.18); Ivory Coast law no. 2016-555 of 26July 2016 (art.42); Burkina-Faso law of 1999 (art.29); DRC law of 1986 (art,23.b).

[199] Article 258 of the Congolese Civil Code, Book III on obligations, states that any act of man that causes damage to another person obliges the person through whose fault it occurred to make reparation for it.

will be used in public or in public places[200] . A photo taken with the consent of the holder of the image right may therefore be used in a calendar or on postcards and distributed in public. This complies with Article 23.b of the law of the Democratic Republic of Congo, which requires the author of a visual work to seek the permission of the person depicted in the work. However, the situation can become complicated in the case of photographs of groups of people in public places. Would it be necessary to obtain their permission to take and distribute these photos? In the Democratic Republic of Congo, there are as yet no court rulings on this issue.

But in France, opinions are divided on this type of photo. One view is that people in public places voluntarily expose themselves to public curiosity, in a way giving tacit permission for their image to be broadcast[201] .

However, there is a consistent dissenting opinion that "the mere fact of being in a public place such as a street, even a station frequented by celebrities, cannot constitute authorisation to reproduce one's image"[202] . However, the law of the Democratic Republic of Congo on copyright is deficient on this issue. Hence the need to enrich this law to regulate the situation of photographs of groups of people in public places. Consent does not have to be in writing. But it must be special. Authorisation to take a photograph does not necessarily mean that it can be published[203] .

The beneficiary of the portrait or photograph may tacitly tolerate his or her image being communicated to the public where such communication is lawful. This may be the case of a famous politician or an artist, who has no problem with his or her photographs or portraits being widely distributed in public. Politicians and famous artists often benefit from wide publicity, although they may also make a financial profit from using their image for advertising purposes.

These broadcasts are lawful when they take place in the context of news reporting. This is a legal exception set out in article 32 of the law of the Democratic Republic of Congo on copyright[204] . Indeed, the right to information protected by the Constitution of the Democratic Republic of the Congo[205] , justifies, nowadays, the photographic illustration of the facts reported. This right can also come into conflict with the right to an image when the person represented by the image considers that the reporter or journalist should have obtained their prior authorisation.

This problem arises when the photograph offends the person depicted. A certain doctrine considers that the photographer,

[200] A public place to which access is free and not subject to the consent of the person occupying the place.

[201] CA Versailles, 31 January 2002, Juris-Data 2002-216790 cited by Thomas Livenais, Image et Droit pénal, Master II thesis, Droit des Affaires, University of Toulouse I Capitole, Academic year, 2009-2010, p.25. N°64.

[202] TGI Nanterre, 20 March 2009, Légipresse 2009, I, p56, cited by Thomas Livenais, op.cit p.26. N°67.

[203] Thomas Livenais, Idem, p.26, No.67.

[204] Article 32 states: "The written or spoken press may reproduce an article published in a newspaper or magazine, provided that the source, title and author's name are given, unless the article or the periodical in which it is published states that reproduction is prohibited. News of the day and miscellaneous items that are simply press information may be freely used". This simply means that journalists who publish photos without the consent of the people depicted are covered by this legal provision. In this case, they will not need the authorisation of the holders of the image rights.

[205] Article 24 of the DRC Constitution of 18 February 1986,

who has not obtained the explicit consent of the victim, can be taken to court when this violation of the victim's dignity is intolerable[206] . However, this clarification is intended to avoid untimely legal action against photographers for views taken of groups of people in public places. Hence the importance of defining the notion of tacit consent, proof of which can be problematic.

Proof of tacit consent is difficult to establish when image rights are at risk. There is no legal provision in the Democratic Republic of Congo that justifies such tacit consent. We can simply refer to the adage "qui ne dit mot consent" ("he who says nothing consents"). However, this adage does not provide any legal certainty likely to protect the author of a photograph of groups of people in public places. The solution to cover the photographer is to use the exception for news events. In this case, the photo must be published close to the time it was taken (one or two days). However, if the photo is published several months later, it loses its topicality[207] . To sum up, the issue of consent by the owner of the image right limits the exercise of copyright if it is not circumscribed by strict conditions.

Infringement of image rights can only be punished if it is intolerable[208] . This is the case, for example, when the dignity or privacy of the person depicted in the photo or portrait is threatened. In our view, however, blanket authorisation for the exercise of copyright is overkill. What's more, infringements of image rights are more a matter of ordinary liability law, whereas copyright is a special issue. Hence the advantage of favouring special law over general law. Therefore, the authorization of the owner of the image right has no place in copyright law.

B. Use of a photo or portrait with the author's consent.

The author of a work of the mind enjoys, by the mere fact of its creation, an exclusive intangible property right enforceable against all[209] . This means that a tangible object (commissioned photo or portrait) bearing the image of the person who commissioned it cannot be used in public without the author's agreement. Therefore, to avoid any conflict, the owner of the tangible object must seek the author's permission before exploiting it in public for reproduction or publication in multiple copies. If the owner of the image right fails to do so, he or she is committing an infringement and is liable to civil or criminal penalties, even if it is his or her image that is represented in the work. This is because intangible property rights are independent of tangible property rights in the medium of the work.

In the Democratic Republic of Congo, the need to obtain the authorisation of the authors of the portraits became apparent in a practical case in the town of Lubumbashi. In this city, a Belgian priest, Léon Verbeek, who was over 90 years old, had bought commissioned portraits and photos from

[206] Thomas Livenais, Image et Droit pénal, Master II thesis, Business Law, University of Toulouse I Capitole, Academic year, 2009-2010, p.21. N°54.

[207] For example, it is not possible to publish a photograph of two people taking part in a demonstration of support taken ten months earlier. On the other hand, a photograph reproducing the features of people demonstrating against the PACS and illustrating an article published a few days later was deemed lawful. Thomas Livenais, op.cit, p.27, No. 69.

[208] However, to be protected, the image must be individualised, permanent, recognisable and require the authorisation of the person depicted. Marc Lesgour, le droit à l'image, 2nd Ed. Larcier, p.140.

[209] Article 1 of Ordinance-Law No. 86-033 of 05 April 1986 on the protection of copyright and related rights in the Democratic Republic of Congo.

individuals who had to leave the city of Lubumbashi in 1993 because of a community conflict between Kasaians and Katangese. Feeling exhausted by age, Father Léon Verbeek decided to donate these objects to the Lubumbashi museum in 2023, but he only had the agreement of the owners of the portraits and not that of the authors. To resolve this problem, the Waza Asbl association, which promotes the collection, suggested contacting the president of the Lubumbashi painters' association to identify the authors or their heirs and obtain their authorisation.

Waza Asbl also proposed another preventive solution: that of obtaining a global authorisation from the national organisation for the collective management of copyright in the Democratic Republic of Congo on behalf of the authors to avoid any potential conflict over these works, even if some of them were not signed by their authors (anonymous works)[210] . The Léon Verbeek case clearly demonstrates the extent to which the author's consent is required, even if the owners of the commissioned portraits and photographs had already given their consent. The author's consent makes it possible to create a peaceful coexistence between copyright and image rights. Otherwise, it opens the door to conflict between the two rights.

II. The potential conflict between the two laws

We examine the conflict linked to the primacy of image rights (A) and the conflict linked to the primacy of copyright (B).

A. The primacy of image rights

The rights of the author of a portrait or photograph may be paralysed by the absence of authorisation from the person depicted in the portrait or photograph. This raises the issue of the primacy of image rights over copyright. Can an author ignore the authorisation of the owner of the image right and publish or distribute portraits or photos? Under positive Congolese law, the author is bound by the authorisation of the owner of the image right, in accordance with Article 23.b of the 1986 Copyright Act. Therefore, without the authorisation of the owner of the image right, the author may be prevented from exercising his right.

Indeed, the artistic expression of photography cannot justify the infringement of the right to privacy that it entails. An artist's right to make his or her work known is not absolute and does not include the right to infringe, without any justification whatsoever, a fundamental right of the subject whose image the work reveals[211] . However, there are situations in which it is difficult to obtain authorisation from the owner of the image rights for a number of reasons: people who cannot be found or who have died, people who are unknown or anonymous in the photo, etc. How can this difficulty be overcome?

If the photo was taken as part of a news report, its simultaneous publication may be justified under the news exception[212] . But apart from this, the question is whether the author of the portrait can hide behind the

[210] This matter is currently being handled by the Waza Abl cultural association in Lubumbashi, which organised a workshop in Lubumbashi from 05 to 09 January 2023 to settle the various issues relating to the transfer of rights with Père Léon Verbeeck, the association of painters and the Lubumbashi museum.

[211] Marc Isgour, *Droit à l'image et création artistique*, Etudes Théatrales, p. 52 to 64, L'Harmattan, 2015.

[212] Article 26 of Ordinance-Law No. 86-033 of 05 April 1986 on the protection of copyright and related rights in the Democratic Republic of Congo.

caricature exception or general group photos. Under Congolese positive law, the caricature exception does not exist in the 1986 Copyright Act. Consequently, the owner of the image right can validly sue the author for infringement of the image right. However, in other African countries, this exception already exists in the law and protects the author from legal action[213] . Moreover, the law of the Democratic Republic of Congo does not lay down any rules likely to cover the author of group photos taken in public places. What would be the appropriate solutions for limiting the liability of the photographer or the author of the portrait against the holder of the right to the image? Five solutions may help to limit the author's liability against any legal proceedings.

The first solution is to introduce an exception for caricature or parody to cover the author against any legal proceedings. The constitutional principle of freedom of expression[214] could thus justify such an exception in copyright law. Freedom of expression cannot be called into question by the right to an image, which is not constitutional. By virtue of the principle of the hierarchy of norms, the right to an image can only confront freedom of expression in the event of a breach of public order or morality (respect for privacy or human dignity).

A second solution is simply to delete the incision in Article 23.b of the Congolese law on copyright relating to respect by the author of the right to an image, since this question is already settled by the ordinary law of civil liability, which obliges any person at fault to repair the damage he causes to others[215] . Image rights cannot dominate copyright in the name of the principle of freedom of expression.

The third solution is to strictly limit the time limit for legal action by the image right holder in civil or criminal procedural law. In this way, the national legislator will be able to establish a very short limitation period (five years, for example) for bringing an action against infringements of image rights. Such a statute of limitations would not apply to the right to one's image, which is an imprescriptible personality right[216] , but rather to legal action.

This solution of reducing the limitation period for legal action already exists in the Labour Code of the Democratic Republic of Congo. For example, in labour matters, the limitation period for legal action is three years[217] from the time the fault (unfair dismissal or dismissal) occurs. The aim is to

[213] Article 43 of the 2008 Senegalese law states: "the author may not prohibit the reproduction or communication of the work as a parody, taking into account the laws of the genre. This Senegalese legal provision places no limits on the right to image. We can therefore conclude that there are no legal restrictions on this right to image.

[214] Freedom of expression in the DRC is protected by Article 23 of the Constitution, which states: "Everyone has the right to freedom of expression. This right implies the freedom to express one's opinions or beliefs, in particular through speech, writing and images, subject to respect for the law, public order and morality.

[215] Article 258 of the Civil Code, Book III of the Democratic Republic of Congo, on civil liability.

[216] With regard to the duration of image rights, Thomas Livenais considers that these rights may be extinguished on the death of the person whose image has been infringed. However, the heir may still object to the reproduction of the image of the deceased, provided that he or she has suffered personal injury, which may be inferred from an infringement of the memory and respect due to the dead. Livenais. Thomas, "Image et droit pénal", Master II thesis, Business Law, University of Toulouse I Capitole, Academic year, 2009-2010, p.27, N°68.

[217] Article 317 of Law N°015/2002 of 16 October 2002 on the Labour Code in the Democratic Republic of Congo, *Journal officiel*, Special Issue of 25 October 2002.

avoid creating permanent legal uncertainty for the employer. It is a way of protecting the employer against untimely and permanent legal action. The same logic may apply to the holder of image rights. He cannot retain this legal possibility permanently, at the risk of paralysing, at any time, the author's right or the right to information.

The fourth solution is to regulate group photos taken in public places. According to one view, photos of groups of people in public places can be published freely unless the person pictured has been framed individually. In this case, the author will need permission before publishing the photo. In addition, the shots must be general and not framed[218] . Thus, when a person is identifiable in a group, there will be no infringement. However, when the image of the victim is targeted and framed, the victim's authorisation will be required. Otherwise, there is a risk of infringing image rights.

The strict regulation of photos taken in public places can be validly justified in the Congolese legal system since it takes into account the balance between the right to an image and the right to information. As the right to information is constitutional, it takes precedence over the right to an image. Consequently, the authorisation of the holder of this right to the image can only be valid when the author of the photograph of the group of people has gone beyond the right to information, either by causing intolerable harm to the author of the image or by publishing the photograph after the information has lost its topicality.

The fifth solution is to take inspiration from the Cameroon law of 2000, which provides for the transfer of economic rights to the person who commissioned the work unless there is a contractual stipulation to the contrary[219] . Thus, if the author wishes to reserve his economic rights, he will state this in the contract with the commissioning party; otherwise there will be an automatic transfer of economic rights to the commissioning party. In other words, in the absence of a contractual stipulation to the contrary, the owner of a commissioned portrait may become the owner of the author's economic rights. This is an effective rule for resolving this conflict between the author and the beneficiary of a commissioned portrait. This Cameroonian solution, although salutary, contradicts Article 1.3 of the 1986 Copyright Act of the Democratic Republic of Congo, which allows the author to retain his rights, even in the case of a contract for the hire of work or services[220] . This legal provision of the Democratic Republic of Congo creates a risk of conflict between the author and the person commissioning a portrait, for example. The author can sue the commissioning party in the event of unauthorised use of the portrait.

The legislator in the Democratic Republic of the Congo could draw inspiration from the solution adopted in Cameroon, which provides for an automatic transfer of

[218] Idem, p. 25.

[219] Article 12.1 of Cameroon Law no. 2000/011 of 19 December 2000 on copyright and related rights states: "In the case of a commissioned work, the author is the first owner of the copyright. However, in the absence of a contractual provision, the economic rights in the said work shall be deemed to have been transferred to the commissioning party, who shall exercise them within the agreed limits".

[220] Article 1.3 of the 1986 Copyright Act of the Democratic Republic of Congo states: "The existence or conclusion of a contract for the hire of work or services by the author of a work of the mind shall not restrict the enjoyment of the moral and economic rights granted to the author in the first paragraph of this Article".

economic rights to the commissioning party in a commissioning contract, unless otherwise stipulated in the contract. This may help to eliminate, in part, the risk of conflict between copyright and image rights.

Despite these possible solutions, the conflict over the primacy of copyright may persist.

B. The primacy of copyright

This conflict concerns situations where the owner of the image right or his successors in title have not obtained any consent from the author before exploiting the work in public. This is possible during the term of protection of the works. In principle, the image right holder must obtain written authorisation from the author in accordance with Article 34 of the 1986 ordinance-law on the protection of copyright in the Democratic Republic of Congo. Otherwise, the holder of the image right is guilty of infringement.

With regard to the exploitation of visual works during their term of protection, the law establishes two different terms of protection depending on the category of work.

For photographic works, the term of protection is 25 years[221] . It begins to run from the first year following publication of the work. In this case, the potential conflict between the owner of the image right is only possible during this 25-year period. On expiry, the risk of conflict disappears as the author's monopoly ceases. However, as image rights are perpetual, they persist after the expiry of the term of the author's economic rights in a photographic work. Image rights are valid until the death of the person depicted in the image.

This short term of protection for photographic works puts their authors at a disadvantage, as they will no longer be able to claim an exclusive right over their photographic works that can be enforced against all parties. Consequently, national legislators should extend the term of protection to at least 50 years, as prescribed by the 1996 WIPO Copyright Treaty[222] .

For graphic and plastic works, on the other hand, the term of protection is 50 years. It begins to run from the year of the author's death. In this case, if the holder of the image right publishes a portrait without the author's agreement, the risk of conflict between the two parties may persist for a long time.

Once the term of protection has expired, the risk of conflict between the author and the image right holder disappears, as the work falls into the public domain, which is free to use. The owner of the image right then becomes the only player in the field. The image right holder or his/her heirs will be the only players with a personal right to the work: the image right.

However, the conflict may also arise when the owner of the image right, during the term of protection of the work, refuses to make the material object containing or supporting the work available to the author for exploitation of the copyright. This is the case when the beneficiary or heir of a commissioned portrait refuses to hand it over to the author for reproduction or public exhibition. The 1986

[221] Article 77 of the Democratic Republic of Congo's 1986 law on copyright and related rights.

[222] Article 9 of the World Intellectual Property Organisation Treaty of December 1996, which abolishes article 7.4 of the Berne Convention. Article 7.4 of the Berne Convention of 1886 had discriminated against photographic works by granting them a term of protection of 25 years while other works enjoyed a term of fifty years from the death of the author (article 7.1 of the Berne Convention).

law of the Democratic Republic of Congo does not offer a solution to this conflict.

The solution may also come from comparative law with Senegal's 2008 copyright law, which proposes in Article 4.4 that the copyright owner may be authorised by the court, under the conditions it determines, to access the material object to the extent necessary for the exercise of its rights. In other words, we can state that the owner of the image right cannot paralyse the exercise of the copyright. The author may recover the material object, by legal means, with a view to exploiting his copyright (for example for reproduction or exhibition to the public) provided that he returns the material object to its owner and does not cause an intolerable violation of the dignity and privacy of the image right holder. The Congolese legislator can therefore, as part of the reform of its national law, adopt this Senegalese solution to settle this potential conflict and enshrine the primacy of copyright.

Conclusion

An analysis of Article 23.b of Ordinance-Law No. 86-033 of 05 April 1986 on the protection of copyright and related rights in the Democratic Republic of the Congo shows that this is a rare and ineffective legal provision that risks hindering the exercise of copyright for visual works in the Democratic Republic of the Congo. The author of a visual work may exploit it freely in the name of freedom of expression, which is a constitutional principle in the Democratic Republic of Congo. Copyright law is a special law and is not intended to regulate general questions of liability. We therefore propose that this legal provision (Article 23.b) be deleted from the current law on copyright in the Democratic Republic of Congo.

Finally, the legislator of the Democratic Republic of the Congo can draw inspiration from the law of Cameroon, which provides that in a commission contract, an automatic transfer of economic rights to the benefit of the commissioning party unless otherwise stipulated in the contract. This may help to eliminate, in part, the risk of conflict between copyright and image rights. Under these conditions, the conflict is resolved by the contractual stipulation, which may reserve the economic rights to the author. Otherwise, it is the beneficiary of the commissioned portrait who automatically acquires the economic rights by operation of law.

T.N.N

Country files : Côte d'Ivoire

By Firmin Kouadio
Legal writer
RSPIA Editorial Secretary

I. INTELLECTUAL PROPERTY INSTITUTIONS IN COTE D'IVOIRE

For industrial property: OIPI

- Year of creation: *2005*
- Institutional text (original) : *Decree no. 2005-112 of 24 February 2005 on the creation, organisation and operation of a public administrative body, the Ivorian Intellectual Property Office.*
- Revised institutional text (in force) : *Decree no. 2015-241 of 8 April 2015 determining the powers, organisation and operation of the Ivorian Intellectual Property Office, published in the JORCI of 29 June 2015*
- Head office and address: Abidjan, Rue des Jardins - Ilot 204 - Quartier II Plateaux (Email: info@oipi.ci / oipi@aviso.ci)
- Status: *National Liaison Structure (SNL), EPA*
- Mission: *cf. art. 4 of Decree no. 2015-112 of 24 February 2015 [In general, it receives and forwards applications for the filing of intellectual property titles to OAPI with a view to their issue].*
- Managing Director (current) : *Dr Paul Koffi ASSANDE*
- Chief Executive Officer (previous, 2017-2022): *Dr Jacques Roger Claude EKRA*

For literary and artistic property: BURIDA

- Year of creation: 1981
- Institutional text (original) : *Decree No. 81-232 of 15 April 1981 establishing the powers, organisation and operation of the Ivorian Copyright Office.*
- Institutional text (in force) : *Decree No. 2015-271 of 22 April 2015 establishing the powers, organisation and operation of the Ivorian Copyright Office.*
- Headquarters and address: Abidjan, II Plateaux-Vallon, Cocody - BP V 258 Abidjan (Email: info@buridaci.com)
- Status: Organisme de Gestion Collective (OGC), a civil company of a special type, under the supervision of the Ministry of Culture and Francophonie.
- Mission: *cf. art. 7 of Decree no. 2015-271 of 22 April 2015 [In general, it is responsible for collecting and paying royalties for the exploitation of works].*
- Managing Director (current, decree no. 2020-103 of 15 January 2020) : Mr Karim OUATTARA
- Managing Director (the very first, in 1981): Mr Serge RAIFF
- Director of Legal Affairs (current) : Mr Jean-Claude KOUADIO

➢ **Other structures**: *Autorité de Régulation des Télécommunications en Côte d'Ivoire (ARTCI)*, responsible for managing domain names and internet addresses [email: courrier@artci.ci); *Comité National de Lutte contre la Contrefaçon (CNLC),* responsible for centralising the fight against counterfeiting, in synergy with customs and the police in particular [email: contact@cnlc-ci.info).

II. LEGISLATION ADOPTED SINCE INDEPENDENCE

Reminder of texts applicable before independence :

- **Industrial property**: Law of 5 July 1844 on patents, amended by the Laws of 31 May 1856 and 7 April 1902; Law of 23 June 1857 on trademarks; Law of 14 July 1909 on designs and models.
- **Literary and artistic property**: law no. 57-298 of 11 March 1957 on literary and artistic property

The 2019 Penal Code and intellectual property:

- Counterfeiting in commercial matters: art. 343
- Unfair competition: art. 344-345
- Repeal of the provisions (art. 346 to 349) relating to literary and artistic property by art. 8 of Act no. 2021-893 of 21 December 2021 amending Act no. 2019-574 of 26 June 2019 on the Criminal Code.

➢ **Text currently applicable to industrial property**: The Bamako Act of 14

December 2015, the new Bangui Agreement, which entered into force on 14 November 2020, two months after the deposit of the instruments of ratification by two-thirds of the signatory States.

➢ **Texts adopted in the field of literary and artistic property :**

- Law no. 78-634 of 28 July 1978 on the protection of intellectual works
- Law no. 87-806 of 28 July 1987 on the protection of cultural heritage
- Law no. 96-564 of 25 July 1996 on the protection of intellectual works and the rights of authors, performers and producers of phonograms and videograms
- Law no. 2004-644 of 9 December 2004 on the legal status of audiovisual communication
- Law no. 2013-451 of 19 June 2013 on the fight against cybercrime
- Law no. 2013-865 of 23 December 2013 on combating counterfeiting and piracy and protecting intellectual property rights in the import, export and marketing of goods and services.
- Law no. 2016-555 of 26 July 2016 on copyright and related rights, published in JORCI no. 84 of Thursday 20 October 2016 (text in force)

III. ACCESSIONS, RATIFICATIONS OF TREATIES AND CONVENTIONS

- ***Paris Convention of 20 March 1883 for the Protection of Industrial Property, as revised at Stockholm on 14 July 1967***: instrument of ratification deposited on 1er February 1974, entry into force on 4 May 1974.
- ***Berne Convention of 9 September 1886 for the Protection of Literary and Artistic Works, as revised at Paris on 24 July 1971***: instrument of ratification deposited on 1er February 1974, entry into force on 4 May 1974.
- ***Treaties administered by WIPO***: accession on 8 July 1961, in force on 01/01/1962
- ***Libreville Agreement of 13 September 1962 establishing the Office Africain et Malgache de la Propriété Industrielle (OAMPI)***: signed on 13 September 1962 by 12 Member States, including Côte d'Ivoire, and ratified by Côte d'Ivoire on 21 August 1962.
- ***Bangui Agreement of 2 March 1977 creating the OAPI, revising the 1962 Libreville Agreement***: ratified on 8 February 1982
- ***Revised Bangui Agreement of 24 February 1999***: ratified by Ordinance no. 2000-388 of 24 May 2000, entered into force on 28 February 2002.
- ***TRIPS Agreement of 15 April 1994***: accession of the OAPI States through the Agreement signed in Geneva on 22 December 1995
- ***Geneva Act of the Lisbon Agreement on Appellations of Origin and Geographical Indications***: instrument of accession deposited with the Director General of WIPO on September 28, 2018
- ***Bamako Act of December 14, 2015***: deposit of instrument of ratification with the Director General at OAPI headquarters on June 28, 2019.

IV. STATE OF INTELLECTUAL PROPERTY DOCTRINE

It is becoming increasingly clear that intellectual property is of interest to theorists and practitioners alike, i.e. teachers and researchers, authors of artistic or literary works, inventors, company owners, lawyers, judges, etc. Below are a few authors who, to our knowledge, are interested in the subject:

- **Prof. OUATTARA Aboudramane:** Professor, Lawyer
  - *La preuve électronique : Etude de droit comparé Afrique, Europe, Canada*, Presses Universitaires d'Aix-Marseille, Collection Horizons Juridiques Jeunes Africaines, 2011, thesis, under the supervision of Prof ISSA-SAYEGH Joseph, Université de Cocody, 2003
  - "Données à caractère personnel et cybersécurité : des liaisons dangereuses", in *Enjeux du droit du numérique en Afrique*, round table on 24 September 2021.
  - "Les mesures d'urgence dans la lutte contre la contrefaçon en droit d'auteur (blocage, etc.)", in *International Colloquium on Intellectual Property Law in the Digital Age*: the Contributions of the Bamako Act, Lomé, 28-29 March 2022.

- **Prof. ALLA Koffi Etienne:** Associate Professor of Law, Lawyer
  - *Subjectivisme et objectivisme dans le droit sur l'invention des médicaments*, thesis, under the supervision of Jacqueline Lohoues-Oble and Jean-Marie Crouzatier, Toulouse 1, 2012
  - "L'équilibre des parties dans le contrat APA", in *International colloquium on Innovation, biological resources and traditional knowledge in West and Central Africa*, 29 November 2019, Yaoundé.
  - *Intellectual Property Law*, Abidjan, ed. ABC, 2021

- **Dr. BOHOUSSOU Dénis:** Teacher-researcher, Director General of OAPI
  - *L'obligation de garantie dans les contrats relatifs à l'informatique*, thesis, under the supervision of Christian le Stanc, Montpellier 1, 1993
  - "The African Intellectual Property Organisation and the Nagoya Protocol", in International Symposium on Innovation, Biological Resources and Traditional Knowledge in West and Central Africa, Yaoundé, 29 November 2019.
  - "L'évolution de la législation de la propriété intellectuelle dans l'espace OAPI", presentation at CEIPI, 31 March 2022 as part of the "Droit comparé de la propriété intellectuelle" series of lectures.

- **Dr. ASSOKO Héraclès Mayé:** Lecturer and researcher, Lawyer
  - *La régulation de réseaux numériques par le contrat*, thesis, under the supervision of Jacques Larrieu, Toulouse 1, 2006
  - *Intellectual Property Law*, Abidjan, ed. ABC, 2020

- **Dr. OUATTARA Simplice:** OAPI accredited agent
  - *La contrefaçon de médicaments dans l'espace U.E.M.O.A.*, thesis, under the supervision of Stéphanie Carre, CEIPI, University of Strasbourg, 2021

- **Dr. KPOLO Christian:** Lecturer and researcher, Lawyer
  - *Les présomptions en droit de la propriété intellectuelle, analyse à la lumière du droit commun*, thesis, under the supervision of Prof Patrick Tafforeau, Université de Loraine, 2019
  - Contributor to the book "*Droit de la propriété intellectuelle*" by Patrick TAFFOREAU, published by Gualino, 2015
  - "L'élaboration de la norme juridique à partir des présomptions : exemple en droit de la propriété intellectuelle", in RRJ-2021

F.K.

NEWS FROM APIA

▪ LE BALAFON, *APIA PODCAST*

In line with its ambition to promote intellectual property in Africa, APIA has taken a further step by setting up a dedicated podcast: "Le Balafon".

Le Balafon, the APIA Podcast, is a lively and interactive forum for discussion and reflection on all aspects of intellectual property... and beyond.

In the words of the editorial team behind this fully-fledged work of the mind, *"in each episode of this podcast, the various contributors offer a concise and educational presentation of one or more subjects relating to intellectual property, with a view to understanding its contours, the issues at stake and any controversies that may arise".*

The first season opened on 1er March 2023 with an episode entitled "Plagiarism, music and copyright" featuring none other than Maitre Yvon Ngombé, President of APIA.

The tone was set: tackling subjects that provoke debate, even controversy, in a deliberately assertive way that allows for contradiction and reflection.

The aim is certainly clear, but so is the format. Each episode of *Balafon is* no longer than 15 minutes. The idea is to cover the whole issue, with the idea that the debates will continue at other APIA events such as *L'arbre à Palabre, La journée de la recherche scientifique* and *La journée d'actualité jurisprudentielle.*

Le Balafon is a veritable field of analysis, subdivided into several complementary compartments. For example, in addition to episodes devoted to 'obvious' topics in intellectual property law, which have featured eminent specialists in the field, *Le Balafon* devotes episodes to topical issues, as well as episodes presenting a thesis topic, and a special issue that tries to think outside the box.

Soel Ngaba, a lawyer and industrial property attorney, presented two episodes on pre-litigation and litigation in trademark matters in the OAPI.

Current affairs were presented in episodes 7 and 8 by Jeanine Tano-Bian and Laurent Escriva respectively.

When it came to reminiscing about thesis defences, the podcast, in its episodes entitled ***Par(en)thèse***, had the immense privilege of welcoming Dr Jeanine Tano-Bian and Dr Théodore Nganzi Ndoni, who presented their work and took the opportunity to offer some valuable advice to future students.

As for the Special Edition, it was devoted to several chapters of the book *Rumbissimo: Rumba, Droit et Business* written by Yvon Laurier Ngombé.

There's so much to say about the **12 episodes** of this first season, but the best way to do it would be to let each *RSPIA* reader make up their own mind... while we wait for the next season, scheduled for January 2024! Long live *Le Balafon!!!*

The APIA Board

Le Balafon
Podcast de l'APIA
#1
Plagiat, musique et droit d'auteur
Invité
Maître Yvon Laurier Ngombé
Avocat au Barreau de Paris

Le Balafon
Podcast de l'APIA
#7
Rétrospective sur la célébration des 10 ans de la Loi ivoirienne sur la protection des données à caractère personnel
Invitée
Jeanine Tano-Bian
Docteure en droit - Consultante en cybersécurité
Enseignante-Chercheur à l'UFHB Abidjan

Le Balafon
Podcast de l'APIA
#5
La saisie-contrefaçon de marques OAPI
Invité
Soel Ngaba
Conseil en propriété industrielle OAPI

Le Balafon
Podcast de l'APIA
#8
Le consommateur moyen en droit de la publicité et en droit des marques
Invité
Laurent Escriva
Formateur

LE BALAFON
HORS - SÉRIE
RUMBISSIMO
RUM BISS IMO
RUMBA, DROIT ET BUSINESS
YVON L. NGOMBÉ
Chapitre 1 - Chez Faignon [Prélude]

Le Balafon
Podcast de l'APIA
Par(en)thèse #2
Le droit d'auteur à l'épreuve du numérique en droit comparé congolais, camerounais, ivoirien et sénégalais
Invité
Dr. Théodore Nganzi Ndoni

▪ THE 2E APIA SCIENTIFIC RESEARCH DAY

Guests: Jeanine Tano-Bian, Andrée Glancia Madinda and Lynda Ngo Nkot

For its second Scientific Research Day, APIA was keen to invite three female researchers in intellectual property and digital law. As women are in the limelight, the day was dedicated to them. Two doctoral students, Ms Ngo Kot and Ms Madinda, and a teacher, Ms Tano-Bian, gave brief presentations of their work on domain names in the OAPI area, copyright contracts in the OAPI area and cybersecurity in the OHADA area.

Nilce Ekandzi, Doctor of Law and associate researcher at CEIPI, moderated the day's proceedings.

Summaries of the three speakers' presentations will be published shortly in the RSPIA.

The APIA Board

OVERVIEW OF CASE LAW

By Christian Kpolo, *Lawyer*

Case Adjin Adimi v. Imprimerie Tropicale and others, Commercial Court of Cotonou, 26 December 2019, Judgment No. 154/2019/CJ /SIII/TCC

Attouh case, Abidjan Commercial Court of Appeal, RG N° 308/2018, 14 February 2019

Case Heden Golf Hôtel v. Uniwax, Tribunal de commerce Abidjan, 27 June 2019, RG n° 263/2019, *unpublished*

Safaricom PLC v. MultiChoice Kenya Limited and others, Court of Appeal of Kenya at Nairobi, Civil Application No. E376 Civil of 2020, 19 March 2021.

Al Atheed General Trading LLC v Colombina S.A, Decision No. 007/22/OAPI/CSR, 18 March 2022

Big Pictures Entertainment Limited, Adeyemi Adeuson and 27 others v. Burida and MTN, Cour d'appel de commerce d'Abidjan, 12 January 2022, 4th instance, RG no. 768/2021

BURIDA v. *Gnacadja Nouyeton Sophie,* tribunal d'instance Abidjan, RG no. 707/2018, civil judgment no. 375 of 11 April 2019

Cité Nazareth SARL v. Mr. Agomon Komlan, Lomé Commercial Court, 19 January 2022, No. 0043/2022

CSR, 17 June 2022, No. 0039/22/OAPI/CSR, LEGENDS

CSR, 18 March 2022, No. 007/22/OAPI/CSR, AMAZON + Logo

Dabé Zohora Bertin v. *Nouvelle Parfumerie Gandour*, Abidjan Commercial Court of Appeal, 1st Ch., Côte d'Ivoire, judgment no. 28/2019 of 21 March 2019

Ets AB PLAST v. Atikpohoun and Mahamadou, Lomé Commercial Court, 30 December 2020, No. 0687/2020

Ghandour Cosmetics Ltd v. El Paradis Cosmetics, decision no. 0048/22/OAPI/CSR, 17 June 2022

Lacoste SA v. Maxi Skf, decision *041/22/OAPI/CSR*, 17 June 2022

Lords Healthcare Limited v Cipla Limited & another, High Court of Nairobi, Milimani Commercial Courts, 22 December 2022, Commercial Case 305 of 2015

Magdalena Lamwaka v. Mukono Bookshop Printing and publishing Co, High Court of Uganda, Civil Division, Civil Suit No. 326 of 2014, 25 February 2019

MASSOKHNA KANE and eight (8) others v. *State of Senegal*, Supreme Court, 13 June 2019, Judgment No. 20

Mercy Munee Kingoo and Lydia Nyva Kingai v. *Safaricom Ltd. and Attorney General,* High Court of Kenya at Malindi, Constitutional Petition No. 5 of 2016, eKLR Report 2019

Mhg Ip Holding Pte Ltd v. Director General of OAPI, Decision No. 0038/22/0API/CSR, 17 July 2022

MultiChoice Africa Holding BV and SuperSport International (PTY) Limited v Intelvision Limited,

Supreme Court of Seychelles, (CS 46/2020 [2021] SCSC 10 (7 April 2021)

Nairobi Map Services Limited v. Airtel Network Kenya ans 2 others, 7th of June 2019, Court of Appeal at Nairobi, Civil Appeal n° 125 of 2016

Natural Valley Ltd v Farily Bottling Ltd and Others, Supreme Court of Zambia, Civil Jurisdiction, 13 January 2022, appeal no. 61/2016

ONG Action de Solidarité Islamique v. Pharmacie Nationale d'Approvisionnement and Imprimerie NOUROU PUB, Supreme Court of Senegal 18 April 2016

Saic-Gm-Wuling Automobile Co. Ltd, LLC v. Deng Ming, Cotonou Commercial Court, Jgt. No. 105/22/CJ1/SII/TCC, Sept. 8, 2022, RG BJ/e-TCC/2022/044

Sanitam Services (E.A.) Limited v. *Rentokil (K.) Limited And Kentainers (K.) Limited*, High Court of Kenya at Nairobi (Milimani Law Courts - Commercial, Admirality & Tax Division), 25 April 2019, Civil case no 338

SARL Application Agro-Industrielles Côte d'Ivoire v. SARL Castor, Abidjan Commercial Court of Appeal, 17 February 2022

Société DO MEDIA LIMITED v. Bureau Ivoirien du droit d'auteur dit BURIDA, Cour d'appel de commerce d'Abidjan, 4e ch., RG n° 883/2019 of 26 February 2020

Company Wm. Wrigley Jr v. Director General of OAPI, CSR, OAPI, 7 September 2021

Société Xyleco inc. v. Directeur Général de l'OAPI, CSR, decision no. 00221/OAPI/CSR of 28 April 2017

Suzhou Dake Machinery v. Total SA, Decision No. 0051/22/0API/CSR, 17 July 2022

The Gb Foods Africa Holding Company, Slu SA v. Sté Xino SARL et a., Tribunal de commerce de Cotonou, 10 November 2022

Jurisdiction over trademark ownership disputes

About the case "*Elsafeer Falcon Pack Egypt Industries v Falcon Pack et al.*

By Yasser OMAR AMINE
Member of the Cairo Bar
Doctor of Law
Associate researcher at the CECOJI-UP (EA 7353) - University of Poitiers
WIPO-accredited trainer

In this important case, the Civil and Commercial Division of the Egyptian Court of Cassation was called upon to rule, in a judgment dated 14 March 2019[223] , on questions of jurisdiction relating to disputes concerning trademark ownership. The question the Court of Cassation had to answer was which court has jurisdiction to hear disputes involving the validity or invalidity of a registered trade mark? Do these questions fall within the jurisdiction of the courts of the judicial order, in this case the Economic Courts, which have exclusive jurisdiction to hear cases and disputes relating to the application of the Egyptian Intellectual Property Code[224] (hereinafter "Egyptian IPC") since the enactment of Law No. 120 of 2008 establishing the Economic Courts (as amended by Law No. 146 of 2019)[225] or do they, on the contrary, fall within the jurisdiction of the administrative courts of the Council of State? In practice, the question raised is much more complex than it might at first appear.

Let's review the facts. In this case, an Emirati company, *Falcon Pack,* is the owner of the trade mark "Falcon" registered in several Arab countries to designate goods in classes 3, 5, 6, 16 and 21, which it markets on the Egyptian market through its agent, *Al Safier Company For Import & Export S.A.E.*. After noting that the latter had changed its name to *Elsafeer Falcon Pack Egypt Industries* and had fraudulently registered three trade marks entitled 'Falcon', in Arabic and English respectively under Nos 148270, 187217 and 187218, to designate goods in classes 3, 16 and 35, the Emirati company *Falcon Pack,* which claimed prior use, brought proceedings against it before the Cairo Economic Court (aff. No. 510/6e A.J.), seeking inter alia a declaration of invalidity and cancellation of the two trade marks registered in bad faith under Nos. 148270 and 187217.

However, the Appeals Chamber of the Cairo Economic Court, in a ruling dated 16 December 2014, had declared that it did not have jurisdiction to hear the dispute in favour of the Administrative Litigation Court at the Council of State on the basis of Article 82 of the Egyptian IPC, which provides for the jurisdiction of the Administrative Litigation Court to examine appeals lodged against the Office's decisions on the opposition, and to do so in accordance with the procedures and

[223] Cass. ch. civ. et com. 14 March 2019, appeal no. 2707/85e Année Judiciaire (hereinafter "A.J."). It should be noted that other cases opposing the two parties have been appealed to the Court of Cassation: Cass. ch. civ. et com. 26 March 2017, appeal no. 2726/85e A.J.; Cass. ch. com. et éco. 13 Feb. 2018, appeal no. 11414/85e A.J.; Cass. com. 23 Feb. 2020, appeal no. 4838/89e A.J.

[224] Enacted by Law no. 82 of 2002 on the protection of intellectual property rights (*OJ of* 2 June 2002, no. 22 *bis*).

[225] Articles 4 and 6 of Act 146 of 2019.

time limits prescribed by the Law of the Council of State.

It was in these circumstances that an appeal to the Supreme Court was lodged. On the sole ground of appeal, the appellant complained that the contested judgment based its decision on Article 82, which allows appeals against decisions of the Office to register, cancel or cancel trade marks to be brought before the competent Administrative Jurisdiction Court, whereas the dispute in question did not involve the State or other legal persons governed by public law, so that it could be considered an administrative dispute; rather, the dispute centred on the ownership of the contested trade mark, between the Emirati company *Falcon Pack* and the Egyptian company *Elsafeer Falcon Pack Egypt Industries*, which therefore fell within the jurisdiction of the ordinary courts.

In a judgment dated 14 March 2019, the Civil and Commercial Division of the Court of Cassation upheld the appeal and quashed the judgment of the Cairo Economic Court on the grounds of breach of law and misapplication, on the grounds that the Emirati company's action was based on its ownership of the "Falcon" trade mark and on the cancellation of the said trade mark registered in bad faith in the name of the Egyptian company insofar as Falcon Pack enjoyed prior use, so that the dispute thus concerned the ownership of the trade mark which falls within the jurisdiction of the ordinary courts to the exclusion of the Administrative Litigation Court.

To determine the scope of the exclusive jurisdiction of the Administrative Litigation Court, the Court of Cassation first took care to qualify the nature of the invalidity action. The Supreme Court pointed out that, under the terms of Articles 80, 81 and 82 of the Egyptian IPC relating to opposition proceedings, the jurisdiction conferred on the Administrative Court implies that the dispute between the parties relates either to their joint haste to register a trade mark, or to the contestation of one of the issues relating to the registration procedure or, within the limit, to the appeal against the authority's decision accepting or refusing to register the trade mark. From this it correctly deduced that a dispute concerning the ownership of the trade mark or the cancellation of the registration on the basis of prior use therefore fell within the jurisdiction of the ordinary courts to the detriment of the administrative courts.

In fact, it seems that the contested judgment of the Cairo Economic Court confused the nature of the invalidity action relating to a trade mark, which is not in fact an appeal against the administrative decision, with the opposition procedure against the decision granting the title, which is administrative in nature. While the Administrative Jurisdiction Tribunal only has jurisdiction to hear cases and disputes relating to the opposition procedure provided for in Articles 80, 81 and 82 above, including appeals against the authority's decision accepting or refusing registration of the trade mark, the ordinary courts do, however, have jurisdiction to rule on actions and claims involving infringement and the validity or invalidity of trade marks. As a result, an application for invalidation of a trademark registration based on bad faith or non-use of the trademark[226] can only be

[226] Cancellation of a trademark registration for non-use must be requested from the competent court (art. 91 of the Egyptian IPC).

brought before a civil court. It is clear that the legislator intended, by way of derogation from the disputes and cases that fall within the jurisdiction of the Council of State, to place all disputes relating to the ownership and invalidity of the trade mark that fall within the scope of Article 65 of the Egyptian IPC within the jurisdiction of the courts.

With regard to patents, the Egyptian High Administrative Court had already clarified the nature of an action for invalidity in a famous and highly instructive ruling dated 14 May 1966[227] , in which it stated: "*An action for invalidity of a patent is not in fact an appeal against the administrative decision which issued it, but relates to the monopoly of exploitation granted by law to its holder, and involves a dispute about the existence or ownership of the invention* between the holder of the patent and someone who disputes his rights to the invention or who denies its existence, and therefore such an action is not subject to any time limit for appeal for invalidity, in accordance with the law of the Council of State. [...]"[228] . This qualification, which is indeed transposable to trademark law, is explained by the fact that it is the trademark itself that is cancelled, and therefore the monopoly attached to it.

Finally, it should be noted that the Court of Cassation's solution in the case before it is firmly in line with its well-established case law. In its judgment of 22 March 2011[229] , the Court of Cassation had already had occasion to rule on the rules of jurisdiction in trade mark matters, in particular in the case of *Al Doha Company For Food Stuff* v *El Kawafel El Misria For Food Stuff Ltd et al.* In its submissions, the public prosecutor in this case argued that the Economic Court did not have jurisdiction to hear the case and that the Administrative Litigation Court should do so. However, the Court of Cassation, rejecting this plea of lack of jurisdiction, pointed out that although the Administrative Court has jurisdiction to hear disputes relating to the opposition procedure provided for in Articles 80, 81 and 82 above, disputes relating to the ownership of a trade mark or the cancellation of its registration based on prior use do not fall within the jurisdiction of the administrative court but, on the contrary, fall within the jurisdiction of the ordinary courts.

In short, the decision under review is of twofold interest, since it not only rules on the classification of trade mark invalidity actions, but also on the delimitation of the respective jurisdictions of the Administrative Jurisdiction Tribunal and the Economic Court in trade mark matters, the contours of which are sometimes somewhat blurred.

Y.O.A

[227] Appeal No 1582/7e A.J., unpublished, case *Abdel Moneim Ibrahim Saleh*. V. In the same sense : Trib. Adm., 29 Nov. 1966, Aff. *El Assas,* appeal no. 117/18e A.J. (unpublished).

[228] V. Y. OMAR AMINE, "De l'insécurité juridique induite par les incohérences pratiques de l'action en nullité des brevets d'invention en Égypte : une analyse comparatiste à la lumière du droit arabe de la propriété industrielle", *Revue Francophone de la Propriété Intellectuelle* (RFPI), Sept. 2015, No. 1, p. 30.

[229] Cass. com. 22 March 2011, appeal no. 6286/79e A.J. The same was true under the former law no. 57 of 1939 on trademarks and industrial and commercial designations: Cass. 15 March 1956, appeal no. 342/22e A.J., *Rec.* year 7, p. 341.

Registered trademarks	Fraudulent trademark registration

Trade mark - Ownership of trade mark - Invalidity - Competent court - Administrative court (no) - Ordinary court (yes) - Economic courts (yes)

▪ CYBERSECURITY AND E-HEALTH

The liability of healthcare facilities management providers in the event of IT vulnerabilities: a study of French law (Part 1)

By Christian Kpolo
Member of the Paris Bar
Doctor of Law - Associate Researcher
University of Lorraine and University of Abidjan

Introduction

The rapid evolution of technology in the healthcare sector has led healthcare players, including healthcare establishments[230] , to outsource the management of their IT infrastructures and data to specialist outsourcing providers. This outsourcing offers a number of advantages, including increased technical expertise, more efficient systems management and reduced operational costs. However, working with outsourcing providers raises fundamental questions about liability in the event of IT vulnerabilities.

IT vulnerabilities, such as cyber-attacks, data leaks or technical failures, can have serious consequences for healthcare organisations[231] . Not only can they disrupt essential medical operations, but they can also compromise the confidentiality, integrity and availability of patient medical records.

However, these are legal obligations and fundamental principles for the protection of personal data, in this case the principle of integrity and confidentiality. Under the terms of Article 5-1-f of the General Data Protection Regulation (GDPR): *"Personal data must be [...] processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*.

In the event of an IT vulnerability, it then becomes crucial to determine where responsibility lies: with the outsourcing provider, with the healthcare establishment itself, or with a combination of the two. Moreover, the criterion of responsibility is inherent in all processing of personal data, as specified in Article 5-2 of the RGPD, which states that: *"The controller shall be responsible for compliance with paragraph 1 [laying down the main principles of data protection] and shall be able to demonstrate that it is complied with (responsibility)"*. From a legal point of view, and beyond what is provided for in particular by Article 5 and Articles 24 et seq. of the RGPD, the responsibility of outsourcing providers in terms of IT vulnerabilities is often defined by the terms of the contract between the two parties. Contracts should clearly specify the obligations and responsibilities of each party in terms of data and system security.

[230] A. Laude, J.-L. Mouralis, J.-M. Pontier, L. Louvel (ss. Dir.), *Revue Lamy droit de la santé,* Éditions Lamy Liaisons, no. 205-7: *"a health care establishment may be defined as the physical structure for care and prevention which carries out the tasks legally defined in Articles L. 6111-1 of the Public Health Code and carried out, in compliance with a certain number of fundamental principles, by public or private persons"*.

[231] https://www.lemondeinformatique.fr/actualites/lire-cyberattaque-contre-le-pole-sante-leonard-de-vinci-a-chambray-les-tours-85367.html on cyber attacks on healthcare establishments; consulted on 9 May 2023.

In a very pragmatic way and due to the very complex status of the processor, from the point of view of the processing of personal data, the RGPD establishes a set of obligations concerning subcontracting by setting out a non-exhaustive list of elements that must be included in the subcontracting agreement. To this end, and by way of example, Article 28-3 of the RGPD states that: *"Processing by a processor shall be governed by a contract or other legal act under Union law or the law of a Member State which binds the processor to the controller, defines the purpose and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and rights of the controller"*.

However, problems can arise when the terms of the contract are vague or ill-defined, leaving room for different interpretations in the event of a problem. Here again, however, the Commission Nationale de l'Informatique et des Libertés (CNIL) provides examples of subcontracting contractual clauses in the appendix to its Guide du Sous-traitant[232] .
From an ethical point of view, the protection of patients' medical data is a paramount concern. Managed services providers must be diligent and responsible in implementing adequate security measures to prevent IT vulnerabilities. This means investing in cutting-edge security technologies, training their staff and putting in place rigorous processes to detect and respond rapidly to potential threats.

In addition, the issue of liability also raises concerns about compliance with current regulations, particularly with regard to the protection of patients' personal data. With the entry into force of the RGPD, healthcare institutions and their outsourcing providers are subject to strict data protection obligations. Failure to comply with these obligations can result in significant financial penalties[233] and reputational damage.

This outsourcing enables the organisation to concentrate on its core business, while benefiting from a high-performance, secure IT service tailored to its needs. Healthcare establishments are facing major challenges linked to digital transformation, regulations, quality of care, patient satisfaction, cost control and more. Managed services can provide them with effective solutions to meet these challenges, including :

- Reduced costs: by outsourcing their information systems, healthcare establishments can make savings on investment in hardware, software, human resources and training. They can also benefit from pricing tailored to their actual consumption and optimise their IT budget.
- Security and compliance: the outsourcing provider undertakes to comply with the standards and regulations in force in the healthcare sector, particularly in terms of personal data protection, confidentiality, traceability, etc. It also ensures the backup, restoration and availability of data in the event of a disaster or breakdown. It also ensures data backup, restoration and availability in the event of a disaster or breakdown.
- Performance and innovation: the outsourcing provider has the expertise

[232] CNIL, *Guide du sous-traitant - Edition September 2017: https://www.cnil.fr/sites/cnil/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf* consulted on 15 August 2023.
[233] Art. 83-4 RGPD: *"administrative fines of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of the total annual worldwide turnover for the preceding financial year, whichever is the greater"*; art. 83-4 RGPD: *"administrative fines of up to EUR 20,000,000 or, in the case of an undertaking, up to 4% of the total annual worldwide turnover for the preceding financial year, whichever is the greater"*.

and technological intelligence to offer healthcare establishments solutions tailored to their specific needs, such as telemedicine, shared medical records, big data, artificial intelligence, etc. It also provides preventive and corrective maintenance for the information system, as well as its ongoing development. It is also responsible for the preventive and corrective maintenance of the information system, as well as its ongoing development.

- Quality of service and satisfaction: the outsourcing provider offers healthcare establishments a personalised, responsive service, with a single, dedicated point of contact. It guarantees an optimal level of service, measured by clear and transparent indicators[234] in the RGPD aspects in order to respect the rights of data subjects[235] , as *"one of the legislator's objectives in the context of [the RGPD reform] was the rights of data subjects and to give them back control of their data"*[236] . In this way, the outsourcing provider is helping to improve the quality of care and patient satisfaction.

Under the RGPD, as data controllers, healthcare institutions are responsible for ensuring that outsourcing providers process personal data in accordance with legal requirements.

Under the terms of Article 4-7 of the GDPR, the "controller *[is] the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing*". The controller must implement appropriate technical and organisational measures to ensure the security and confidentiality of the data and to prevent

---

[234] Art. 5-1-a RGPD: *"Personal data must be... processed lawfully, fairly and transparently with regard to the data subject"*. As the CNIL states, *"transparency enables data subjects to know the reason for the collection of the various data concerning them; to understand the processing that will be carried out on their data; to ensure control of their data, by facilitating the exercise of their rights"* https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence consulted on 15 August 2023. In its guidelines, the EDPS states that *"The controller must be clear and open with the data subject and explain how it intends to collect, use and share his or her personal data. The purpose of transparency is to enable data subjects to understand their rights under Articles 15 to 22 and, if necessary, to make use of them. [...] With regard to the principle of transparency, the key elements of data protection by design and by default include the following: - Clarity - Information must be formulated in clear, simple, concise and understandable terms. - Semantics - Communication must have a clear meaning for the audience concerned. - Accessibility - Information must be easily accessible to the person concerned. - Contextuality - Information should be provided at the right time and in the right form. - Relevance - Information should be relevant and applicable to the specific data subject. - Universal design - Information must be accessible to all data subjects and include the use of machine-readable languages to facilitate and automate readability and clarity. - Understandability - Data subjects must have a fair understanding of what they can expect in relation to the processing of their personal data, particularly where children or other vulnerable groups are concerned. - Multiple channels - Information should be provided through different channels and media, beyond text, to increase the likelihood that the information will actually reach the data subject. - Layered - Information should be structured in layers to resolve the tension between completeness and comprehensibility, while taking into account the reasonable expectations of data subjects"*. EDPS, *Guidelines 4/2019 on Article 25 Data Protection by Design and Data Protection by Default*, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf accessed 15 Aug 2023. See also, Article 29 Working Party Guidelines on Transparency under Regulation (EU) 2016/679 - Revised version adopted on 11 April 2018, p. 6 f. https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf accessed on 15 August 2023.

[235] Articles 12, 13 and 14 of the GDPR. Article 12 of the GDPR requires data controllers to provide clear and comprehensible information to data subjects about the processing of their personal data. Article 13 specifies the information to be provided when personal data is collected, including the identity of the controller, the purposes of the processing and the potential recipients. Finally, Article 14 deals with cases where data is not obtained directly from the data subject, imposing information to be provided, including the origin of the data.

[236] A. Banck, *RGPD : la protection des données à caractère personnel, 20 fiches pour réussir et maintenir votre conformité*, coll. "Droit en poche", Gualino-Lextenso, 2023, p. 59.

data breaches. A healthcare establishment is an organisation that provides medical, surgical or paramedical care to patients.

Healthcare establishments may be public or private and may include hospitals, clinics, health centres, retirement homes, home care centres, palliative care centres and other medical facilities[237] . In their day-to-day work and in the course of their missions, they process massive amounts of data. This is systematically reflected in its relations with the facilities management service provider to whom it subcontracts the management of its information system. Article 4-8 of the RGPD defines a "processor" as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

Because of the risks involved in outsourcing operations (both technical and legal in terms of processing sensitive information), data processing agreements must be signed with service providers, clearly defining responsibilities in terms of data protection and reporting obligations, particularly in the event of a data breach or a breach of confidentiality or data integrity.

The framework of our analysis here is very restrictive in terms of entities, insofar as a certain number of establishments operating in the health sector will not be taken into consideration. This will notably be the case for pharmaceutical establishments.

In a context where cyber attacks and various breaches of personal data, in accordance with Article 4-12 of the RGPD)[238] , continue to pose a growing threat to the healthcare sector, the responsibility of outsourcing providers becomes all the more critical. As custodians of healthcare institutions' data and IT systems, these service providers have a duty to implement robust security measures to prevent, detect and counter cyber threats.

In the context of information systems, outsourcing is defined as *"the result of integrating a set of basic services, with the aim of entrusting all or part of a company function to a specialised service provider under a fixed-price, multi-year contract, with a defined level of service and duration" (AFNOR Z 67 801-1). The term facilities management refers to outsourcing services in the field of information systems"*[239] .

Computer vulnerabilities are flaws or weaknesses in a computer system that can be exploited by attackers to access sensitive data or to damage or disrupt the operation of the system. Computer vulnerabilities can result from configuration problems, malicious software, weaknesses in passwords, human error or other factors[240] . Computer vulnerabilities can be grouped into three main groups: *"hardware or software vulnerabilities that require the installation of a patch or workaround; application vulnerabilities that require a fix in the application's source code; configuration errors that require parameters to be changed, such as unnecessary*

[237] Art. L. 611-1 et seq. CSP.

[238] Under Article 4-12 of the GDPR, a personal data breach is *"a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed". This refers to* any security incident, whether malicious or not and whether intentional or not, which has the effect of compromising the integrity, confidentiality or availability of personal data: https://www.cnil.fr/fr/definition/violation-de-donnees

[239] ASIP - ANAP, *Mutualisation et Externalisation des SI de santé : Éclairage pour le décideur*, consulted on 9 May 2023 on the website https://www.afexis.com/wp-content/uploads/2016/10/Mutualisation-et-externalisation-SI.pdf p. 6.

[240] CLUSIF, *Gestion des vulnérabilités informatiques : vers une meilleure gestion des risques opérationnels [Value and indispensability of vulnerability management]*, tome 1, May 2014, p. 10.

services that require unnecessary or obsolete components to be removed or disabled"[241] .

Responsibility is the moral, legal or contractual obligation to answer for one's actions or negligence. In the event of a problem, responsibility means taking the necessary steps to repair the damage caused and to prevent the same problem recurring in the future[242] .
With this in mind, it seems legitimate to ask how the liability of a healthcare institution's outsourcing provider in the event of IT vulnerabilities could be assessed, taking into account the risks associated with the outsourcing activity or the outsourcing of healthcare institutions' information systems, the legal and contractual obligations of the parties, and the security measures to be put in place to prevent these vulnerabilities.

The aim is to contribute to a better understanding of the responsibility of the outsourcing provider in the event of IT vulnerabilities and health data breaches, and to improve IT security and the protection of health data in healthcare establishments. As a preliminary point, it should be noted that Article 4-15 of the RGPD defines health data as *"personal data relating to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about that person's state of health"*.

To achieve this objective, the following steps should be taken:

- Analyse the legal and regulatory obligations applicable to outsourcing providers in terms of IT security and health data protection in the context of healthcare establishments. This analysis should take into account the General Data Protection Regulation (RGPD)[243] , the French Data Protection Act (LIL)[244] , as well as professional standards and recommendations issued by the relevant authorities;
- Examine the contractual obligations between health care organisations and outsourcing providers in terms of IT security and health data protection. This analysis should take into account standard contractual clauses and specific clauses negotiated between the parties;
- Examine current practices in terms of IT security and health data protection in healthcare establishments and outsourcing providers. This analysis will make it possible to identify good practices to follow and practices to avoid in order to minimise the risks of IT vulnerabilities and health data breaches;
- To propose practical recommendations for healthcare establishments and outsourcing providers in order to minimise the risks of liability in terms of IT security and health data protection. These recommendations could cover the contractual, organisational, technical and human aspects of IT security and health data protection.

The hypothesis considered is that the liability of a healthcare institution's outsourcing

[241] CLUSIF, *Gestion des vulnérabilités informatiques Vers une meilleure gestion des risques opérationnels*, tome 2, 2015, p. 9-10.
[242] Civil liability: Civil Code art. 1231 et seq., 1240 et seq., anc. art. 1146 et seq., 1382 et seq.; Criminal liability: Criminal Code art. 121-1 and 121-2; Medical liability: Public Health Code art. L. 1111-2, L. 1142-1 f.

[243] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
[244] Law no. 78-17 of 6 January 1978 on data processing, data files and individual liberties.

provider in the event of IT vulnerabilities is complex and depends on many factors, such as the nature of the vulnerability, the terms of the service contract, the security policies and the prevention measures put in place by the provider and the healthcare institution. In-depth research into the factors influencing the responsibility of outsourcing providers in the context of the management of healthcare institutions' information systems can help to better understand the risks associated with the outsourcing and facilities management of these systems, and to propose recommendations for improving security practices and service contracts in this area.

Unfortunately, there are a number of limitations to this approach:

- Data availability: There may be limited data available on IT security incidents involving managed service providers in healthcare organisations, which may affect the quality and quantity of the research results;
- The availability of the players involved: The research may require the participation of key stakeholders such as outsourcing providers and healthcare institutions. Their availability to participate in interviews or surveys may be limited due to time or resource constraints;
- Complexity of the regulatory framework: The regulatory framework surrounding the management of health data security can be complex and vary from jurisdiction to jurisdiction. It can be difficult to take into account all the nuances and differences between different regulatory frameworks in research.

To address the issues raised, we will analyse the risk factors associated with outsourcing (I) before examining the treatment of these factors (II).

J. Risk factors associated with outsourcing healthcare facilities

As we mentioned in the opening lines of our analysis, there is a clear need for healthcare institutions to outsource the management of their IT systems. As stated by Agence nationale de la sécurité des systèmes d'information (ANSSI), *, "outsourcing is the process of entrusting to a third party all or part of an activity that was previously carried out internally"*[245] . For its part, facilities management corresponds to *"outsourcing applied to the field of information systems"*[246] .
In a more refined approach, IT outsourcing (commonly known as *facilities management*) is officially defined as *"*the *contractual assumption of responsibility for all or part of the management of an organisation's information system by an external service provider"*[247] .

Over and above the obvious advantages of this approach, the fact remains that it entails particularly significant risks that are likely to trigger the liability of facilities management service providers and, as a result, harm health data[248] . Outsourcing is the transfer of an organisation's activities to an external service

[245] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 6.
[246]ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 6.
[247] *IT vocabulary*: OJ 20 April 2007, p. 7078.
[248] Système national des données de santé, *Référentiel de sécurité: guide d'accompagnement*, consulted on 9 May 2023 at https://www.snds.gouv.fr/download/Guide_accompagnement.pdf, p. 11.

provider. Outsourcing data (sometimes to several service providers in a chain) can lead to breaches in the protection of data confidentiality.

Insofar as outsourcing is a technical operation founded on contractual and therefore legal bases, it would be appropriate to analyse the operational risk factors (A) before considering the legal risk factors (B).

A. Operational risk factors

Outsourcing for healthcare establishments can present both advantages and risks, which need to be assessed before the decision is made to integrate it into the healthcare data management process. The risks in terms of information systems security may be linked to the context of the outsourcing operation, but also to deficient or incomplete contractual specifications.

The French National Agency for Information Systems Security (ANSI) has produced a guide[249] to help IT decision-makers become aware of the information systems security (ISS) risks associated with any outsourcing operation, and to provide a coherent approach for taking ISS aspects into account when drawing up the specifications for an outsourcing operation. It is on the basis of these elements that the analysis will be carried out; and we will analyse successively, without these points being exhaustive, the loss of control of the information system (1), remote intervention (2), and the shared hosting of health data (3), all factors which are sometimes inherent in the use of cloud computing.

4. Loss of control over the information system

The loss of control over the information system is a risk that needs to be taken into consideration when a health care organisation decides to outsource. This threat may be linked to the outsourcing, the location of the data, the specific nature of the health data and the technical choices made by the service provider. Pursuant to Article 82-2 of the RGPD[250] , the subcontractor's liability will be established on the basis of the materiality of the damage suffered by the data subjects and, more specifically, if it is established that the damage is attributable to the subcontractor. This will be the case in particular if the damage results from a failure to comply with the obligations incumbent upon it under the RGPD and if the damage results from a failure to comply with the lawful instructions of the data controller, i.e. the healthcare establishment.

At this stage of the analysis, the technical risk factors must be considered from the point of view of both the health care organisation and the outsourcing provider.

At the outset, it should be borne in mind that healthcare establishments run the risk of losing control of their own information systems if they delegate too much project management to an external service provider.

---

[249] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance,* consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, *passim.*

[250] Art. 82-2 RGPD: *"Any controller who has participated in the processing operation shall be liable for damage caused by the processing operation which constitutes a breach of this Regulation. A processor shall be liable for damage caused by processing only if he has failed to comply with the obligations laid down in this Regulation which are specific to processors or if he has acted outside or contrary to the lawful instructions of the controller".*

To put this into context, it is important to know that in a company there are three essential aspects to controlling IT systems: control of operations, which is managed by the IT Director (ID) or the Information Systems Security Manager (ISSM), control of the development of new IT applications, which is the IT Director's area of expertise, and control of maintenance (upkeep, adaptation, improvement of existing applications)[251] .

The loss of control over the information system raises real problems when it comes to managing personal data and, more specifically, data insofar as, from the point of view of the regulations on personal data, the healthcare establishment remains the data controller.

Article 4-7 of the GDPR states that the *"controller [is] the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing; where the purposes and means of such processing are determined by Union law or by the law of a Member State, the controller may be designated or specific criteria for his designation may be laid down in Union law or in the law of a Member State"*.

As a general rule, therefore, the data controller is the customer (in this case, the healthcare establishment) and not its service provider (i.e. the facilities management service provider). French case law has clarified that *"the fact that data processing operations are entrusted to subcontractors does not relieve the data controller of his responsibility to preserve data security, without thereby infringing the constitutional principle of personal responsibility, provided that these subcontractors are acting on the instructions of the data controller"*[252] .

The loss of control over the information system due to subcontracting is a threat that arises when outsourcing. First and foremost, it should be pointed out that subcontracting is an *"operation whereby a contractor, known as the main contractor, entrusts another person, known as the subcontractor, with the performance of all or part of a works contract or part of a public procurement contract concluded with the project owner, by means of an agreement known as a subcontract or subcontracting contract. The use of subcontracting implies an obligation on the part of the main contractor to have the subcontractors accepted by the project owner"*[253] .

In practice, health care institutions interested in subcontracting may do so on their own, as part of a consortium with one or more other entities, or through subcontracting. And it is at this point that subcontracting can become a risk, particularly when the outsourcing service is subcontracted to a third-party supplier by the main service provider; this is the typical case of the subsequent subcontracting provided for in Article 28-4 of the RGPD.

In this type of situation, the healthcare establishment, as the data controller, may find itself indirectly dependent on the main service provider for the management of its information system. This can complicate communication and direct decision-making in the event of an incident or problem; all the more so as there is no guarantee that the purpose and means of a processing operation it has established with the subcontractor will be passed on to the subsequent subcontractor.

[251] J. des Courières, "Au-delà de la maîtrise des systèmes d'information la maîtrise de l'entreprise", *ADELI Newsletter* No. 39 - April 2000, p. 27.

[252] CE, 30 December 2015: *JurisData* no. 2015-029454.

[253] G. Cornu, *Vocabulaire juridique,* PUF, 13e ed., 2020, *v° "Sous-traitance"*.

Added to this is the fact that the healthcare establishment may lose visibility of the day-to-day operations and practices implemented by the subcontractor. This can make it more difficult to assess the quality of the services provided, identify potential problems and ensure compliance with the fundamental principles of health data protection.

Deterioration in service quality can be a risk factor associated with subcontracting due to the fact that the main provider may sometimes subcontract to a subcontractor for cost reasons. This can lead to a deterioration in the quality of the services provided, as the (subsequent) subcontractor may not have the same level of expertise and commitment to the healthcare organisation.
In very practical terms, in the event of a data security breach or IT incident, managing the response can be complex if the healthcare establishment is faced with a chain of subcontractors. Coordination between the main service provider, the subcontractors and the healthcare establishment can lead to delays in decision-making and in resolving the problem, which increases the risk of damage.

In all cases, the widespread use of subcontracting makes it more difficult for data controllers to manage data leaks. Article 82 of the RGPD establishes the responsibility of the data controller once it has participated in the processing that has caused damage. The controller must therefore manage data leaks from the processor before, during and after their occurrence[254] . A parallel should also be drawn with Article 28 of the RGPD, which sets out the framework for indirect liability. Articles 28 and 82 of the RGPD distinguish between the responsibility of the controller and that of the processor depending on their role and involvement in the processing.

The data controller is liable for any damage caused by the processing that constitutes a breach of the RGPD, unless it proves that it is not responsible for the event that caused the damage. The processor shall only be held liable if it has failed to comply with the obligations laid down in the RGPD that are specifically incumbent on processors or if it has acted outside or contrary to the lawful instructions of the controller. These two articles stipulate that the controller or processor must help the other party to fulfil its data protection obligations, particularly in the event of a data breach, data protection impact assessment, prior consultation or respect for the rights of data subjects.
In addition to this first level of risk associated with outsourcing, there is also the risk of losing control over the location of data, with the main problem being cross-border processing.

Outsourced hosting is not in itself a bad thing. In fact, cloud computing is an evolution of the provision of hosted applications. It is *"a method of processing a customer's data over the Internet in the form of services provided by a service provider"*[255] . It is specified that it is *"a particular form of IT management, in which the location and operation of the cloud are not made known to customers"*[256] .

These methods of providing remote IT services therefore enable companies to outsource their IT needs to[257] . They offer a

[254] K. Bouslimani, "Fuite de données émanant d'un sous-traitant: comment gérer?", published on 17 May 2022 on the website https://www.village-justice.com/articles/fuite-donnees-emanant-sous-traitant,42216.html, accessed on 24 July 2023.

[255] *Vocabulaire de l'informatique,* OJ 6 June 2010, p. 10453.
[256] *Idem.*
[257] The term "outsourcing" is often used.

definite advantage in terms of cost: the healthcare establishment, which is the customer in this case, does not have to worry about purchasing specific hardware to use the software package, and the cost of the software used is paid for over the period of its use, unlike a software package licence[258] , where the price is often fixed and paid in full when the contract is signed. What's more, this mode of operation allows great flexibility, as services can be subscribed to according to the customer's actual needs[259] .

Cloud computing is based on distributed infrastructures, which means that data files are atomised. Unlike a traditional outsourcing service provided by a service provider where the location of the data centre is known, a cloud service implies a location in several places simultaneously. Such solutions *"often increase the risk of data confidentiality breaches"*[260] . A more vicious aspect of this process lies in the fact that the data may be hosted on servers located in countries whose legislation on the protection of personal data is lax or even less rigorous than the framework laid down by the RGPD, and in particular by Article 4-23 of the RGPD, which defines cross-border processing.

For its part, Article 44 of the GDPR specifies that: *"a transfer to a third country or to an international organisation of personal data which is being or is intended to be processed after that transfer may only take place if, subject to the other provisions of this Regulation, the conditions set out in this Chapter are complied with by the controller and the processor, including for subsequent transfers of personal data from the third country or international organisation to another third country or to another international organisation"*.

This situation is likely to increase the risk of personal data breaches. These are legal issues with practical implications.

The question of data security arises from a technical point of view, insofar as the location and operation of the cloud are not made known to healthcare establishments.

In addition, ANSSI points out that uncontrolled data localisation can entail other risks: difficulty in exercising a right of supervision and control over the service provider's staff; difficulty in carrying out a security audit of the underlying infrastructure; difficulty in responding to any legal injunctions, for tax reasons for example, or other legal reasons[261] . To this should be added the aspects relating to compliance with the obligations imposed by the RGPD, in particular the obligation of transparency and traceability, which takes the form of the processor providing the controller with all the information necessary to demonstrate compliance with its obligations, in line with the provisions of Article 28 of the RGPD.

---

[258] Software package: *"is, according to the official computer vocabulary, a "complete and documented set of programs designed to be supplied to several users for a single application or function" (Official Journal of 17 January 1982). Software packages are therefore a category of software: they are standard software designed to meet the common needs of a large number of users/customers, as opposed to "specific software" which is developed especially for a company (either by its IT specialists or, more often, by an external IT service provider) to meet the company's own needs"* cf. https://www.dictionnaire-juridique.com/definition/progiciel.php consulted on 17 August 2023.

[259] F. Macrez, "Contrats d'externalisation informatique - Infogérance, fourniture d'application hébergée, informatique en nuage", JurisClasseur Communication, No. 815, 1er September 2022.

[260] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf , p. 8.

[261] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf , p. 8.

For example, the processor must ensure *"that the persons authorised to process the personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality"*[262] .

Moreover, given the complexity and specific nature of this outsourcing operation, it seems difficult to place all responsibility for data confidentiality and security on the service provider: the respective responsibilities of each contracting party need to be considered and stipulated. From a legal point of view, the issue is addressed by very specific regulations[263] .

The typical case of this type of risk can be seen in the DEDALUS affair concerning a massive health data leak[264] . On 23 February 2021, a massive data leak involving almost 500,000 people was revealed in the press, implicating the company DEDALUS. The surname, first name, national insurance number, name of the prescribing doctor, date of the examination and, above all, medical information (HIV, cancers, genetic diseases, pregnancies, drug treatments taken by the patient and genetic data) of these people were published on the Internet. On 24 February 2021, the CNIL carried out a number of inspections, including at DEDALUS BIOLOGIE, a company that markets software solutions for medical analysis laboratories. At the same time, the CNIL referred the matter to the Paris judicial court, which blocked access to the site on which the leaked data was published. This decision on 4 March 2021 limited the consequences for individuals. On the basis of the findings made during the inspections, the CNIL's select committee[265] considered that the company had failed to fulfil several of its obligations under the RGPD, in particular the obligation to ensure the security of personal data. The select committee therefore imposed a fine of €1.5 million and decided to make its decision public. The amount of this fine was decided in the light of the seriousness of the breaches identified, but also taking into account the turnover of DEDALUS BIOLOGIE[266] .

Another risk factor linked to the choice of service provider may be the fact that the service provider may be responsible for updates, security patches and improvements to the information system. If these updates are not carried out correctly or in a timely manner, this can lead to security vulnerabilities and performance degradation.

Furthermore, if the outsourcing provider does not keep a close eye on changes in technology and the needs of the healthcare organisation, this can lead to delays in the adoption of new functionalities or missed opportunities to improve the information system. In all circumstances, the applications used should ideally be interoperable, guaranteeing at the very least compatibility

[262] Art. 28-3-b of the RGPD.

[263] In particular, Article L. 1111-8 of the Public Health Code: "Any person who hosts personal health data collected in the course of preventive, diagnostic, care or social and medico-social monitoring activities, on behalf of the natural or legal persons responsible for producing or collecting such data or on behalf of the patient himself, shall do so under the conditions set out in this article. Hosting, on whatever medium, paper or digital, is carried out after the person being cared for has been duly informed and unless there is an objection for a legitimate reason. The hosting of personal health data shall be the subject of a contract.

[264] Deliberation of the restricted formation No. SAN-2022-009 of 15 April 2022 concerning the company DEDALUS BIOLOGIE.

[265] The CNIL's Restricted Section is the body responsible for imposing sanctions. "*It is made up of 5 members and a Chairman other than the Chairman of the CNIL. It may impose various sanctions on data controllers who fail to comply with the law". See* https://www.cnil.fr/fr/definition/formation-restreinte

[266] https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie

with the most widely used operating systems and databases.

The risks inherent in remote intervention should also be considered, insofar as this corresponds to the technical operation adopted.

5. Remote intervention

Outsourcing in general, and more specifically facilities management, can involve remote intervention, where service providers manage and maintain the healthcare establishment's IT systems remotely, without being physically present on site. Remote interventions are an important part of outsourcing. They enable service providers to work on customers' IT systems without having to travel to the site.

This has a number of advantages, such as faster response times and better availability of IT systems and, by extension, personal data, as provided for in Article 32-1-b and 32-1-c of the RGPD, under which *"the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia, as necessary [...] means to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services [...] means to restore the availability of and access to personal data within appropriate time limits in the event of a physical or technical incident"*.

The Agence Nationale de la Sécurité des Systèmes d'Information has published two documents covering certain aspects of remote intervention:

- The guide *"Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information"*[267] ;
- The technical note *"Safety recommendations relating to remote assistance"*[268] .

The ANSSI guide covers IT or telecommunications services entrusted to third parties, whatever their nature. It deals in particular with remote services. For remote services, it indicates the vulnerabilities frequently encountered, highlights the main risks of intrusion and abuse of access privileges, and makes recommendations. As for the technical note, it concerns the security of remote assistance and in particular remote control of a workstation. It specifies the associated risks and gives minimum recommendations to be complied with.

The main recommendations of these two documents have been included in the document entitled: *"Rules for remote interventions on health information systems Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - April 2014"*[269] . This document defines the security rules and recommendations relating to interventions carried out remotely on a Health Information System (HIS). It is one of the specific guides in the General Security Policy for Health Information Systems (PGSSI-S)[270] .

[267]https://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-dessystemes-d-information-un-guide-pour-maitriser.html

[268]https://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-la-tele-assistance.html

[269] ASIP Santé/DSSIS: Remote intervention rules - April 2014 - V0.3

[270] The PGSSI-S brings together thematic guidelines (electronic identification of players, evidential value of healthcare documents, accountability of actions, etc.) and practical guides, which remind the various players in healthcare information systems of the best practices for complying with the regulations in force. The French government has entrusted the Agence du Numérique en Santé (ANS) with drawing up and publishing the general security policy for health information systems (PGSSI-S) , a framework that must be respected by all players in the health, social and medico-social sectors in order to secure health

This guide provides a definition of what is covered by remote interventions involving Health Information Systems, and mentions in particular: remote monitoring, remote maintenance and remote assistance.

He defines[271] as follows:

- ***Remote monitoring*** refers to the process of remotely collecting and analysing information relating to the technical functioning of a Health Information System (HIS), with the aim of monitoring its operation, anticipating future trends and identifying any irregularities. For example, this may involve monitoring the load parameters of a set of devices or regularly running tests on an application to ensure it is always available.

- ***Remote maintenance*** encompasses actions undertaken remotely to adjust the parameters and configure the software of part or all of a Health Information System, with the aim of maintaining its optimal operation or upgrading it. This may include activities such as technical operation and management, technical incident resolution and software updating.

- ***Remote assistance*** involves providing help from a remote station where the access interfaces of the person being helped are faithfully reproduced. In some situations, the only interface reproduced is the screen display, and the helper is able to observe only what the person being assisted sees or does. Concrete examples include the logical troubleshooting of a user on their workstation or the direct provision of expertise by an administrator on a server console.

It has to be said that security is not always well understood when carrying out this type of intervention, even though the solutions used provide vulnerabilities and give those involved significant rights. By its very nature, a remote assistance tool gives very broad access to the resources available on a user's workstation. As a result, any individual accessing a workstation remotely during a remote assistance operation can view all the information stored on the machine, including personal data, use the various peripherals connected to it (microphone, webcam, etc.) and even use the various applications installed in place of people connecting locally.

This raises issues of protecting and preserving the confidentiality of information contained in the workstation, traceability of operations carried out and user control of operations carried out on the machine.

From a personal data protection perspective, it should be noted that the risks associated with remote access to personal data by a subcontractor include several aspects. Remote access could increase the risk of data security breaches, as remote connections could be vulnerable to computer attacks and unauthorised intrusions. Also, if the processor is located in a country outside the European Economic Area (EEA) or a country recognised as having an adequate

information systems (SIS). Article L. 1470-5 of the French Public Health Code stipulates that the ANS must draw up, in consultation with the ecosystem, guidelines aimed at guaranteeing the exchange, sharing, security and confidentiality of personal health data by digital health services. cf.: https://esante.gouv.fr/sites/default/files/media_entity/documents/180528_PGSSI-S_0.pdf

[271] ASIP Santé/DSSIS: *Remote intervention rules* - April 2014 - V0.3, p. 6.

level of data protection, the international transfer of data could be carried out without appropriate safeguards, which would be a breach of the GDPR. Furthermore, where processors have remote access to personal data, control over the way in which this data is processed may become more difficult to exercise by the healthcare establishment responsible for processing the said data.

In terms of cybersecurity, a number of threats are posed by remote interventions and are risk factors in the context of outsourcing services for healthcare institutions' information systems. These include, for example, the cases mentioned in the ASPI Santé/DSSIS Guide[272] :

- If the person responsible for the SIS does not control the security of the organisational environment in which the service is provided, the threats to the Information System include: defects in the performance or quality of the service, leading to unavailability of the SIS, loss of confidentiality or data integrity. Disclosure of service data to the supplier's entities or to third-party organisations (particularly in the case of subcontracting), which may result in a breach of legal or regulatory obligations or an inability to comply with court orders. Logical access to the SIS by unauthorised personnel of the supplier.
- If the SIS manager does not control the security of the technical environment in which the service is provided: threats to the Information System include: propagation of security incidents in the SIS via the supplier's platform: malicious code, logical attacks on the platform. Illicit logical access to SIS data by platform users.
- If the SIS manager does not control the security of the physical environment in which the service is provided, the threats to the Information System include: Physical capture of service data in the environment of the supplier's platform, observation of personnel, theft of storage media. Destruction of the platform, resulting in the inability to provide the service.

In addition to the remote data processing methods mentioned above, it is also useful to consider another approach, which involves the shared hosting of health data, and which is of undeniable interest when it comes to understanding the risk criteria for outsourcing.

6. Shared hosting of healthcare data

Health data hosting involves hosting personal health data on behalf of the natural or legal persons who produce or collect the data[273] . Shared hosting involves hosting several services on a single server, in order to rationalise resources. In most cases, the services concerned are websites, email services or databases. In this case, the customers (the health establishments) do not have direct access to the servers or shared resources as administrators. Configuration is carried out and managed by the hosting provider or a third-party company[274] .

More specifically, shared hosting of healthcare data and facilities management are

[272] ASIP Santé/DSSIS: *Remote intervention rules* - April 2014 - V0.3, p. 6.

[273] Articles R.1111-8-8 and R.1111-9 of the French Public Health Code.

[274] ANSSI, *Externalisation des systèmes d'information : maîtriser les risques d'infogérance*, consulted on 9 May 2023 on the website https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf, p. 13.

two concepts linked to the management of IT systems in the healthcare sector. Shared hosting involves storing the healthcare data of several healthcare institutions on the same shared IT infrastructure. This allows facilities to share IT resources, which can reduce infrastructure costs. However, it also means that data from several establishments is stored in a shared environment, which raises issues of confidentiality and security.

The use of the *Cloud, for* example, places the healthcare establishment in a situation of technological dependence on the supplier, which has control over the processing resources and the data, and which may therefore be tempted to prevent the user from accessing them during or at the end of the contract. However, users may have good reasons for wanting to access their data: during the course of the contract, for example, in order to comply with legal obligations (such as the right of access or the right to portability) or to ensure that the contract is being properly fulfilled; at the end of the contract, in order to ensure reversibility (in the event of re-outsourcing) and transferability (in the event of continued outsourcing to another supplier) of the services.

Outsourcing can include server management, network maintenance, data security, technical support, etc. Outsourcing allows healthcare establishments to benefit from specialist technical skills without the need to maintain an in-house team dedicated to these tasks.

When shared hosting of healthcare data is combined with outsourcing, healthcare institutions can choose to entrust the management of their shared IT infrastructure to an external outsourcing provider. This enables establishments to benefit from both the advantages of shared hosting, such as reduced costs, and the advantages of outsourcing, such as access to specialist technical expertise.
According to ANSSI, the risks stem from the fact that the hosted service is more or less closely linked to other services, some of which are more vulnerable than others. Furthermore, attacks targeting one of the shared resources (network, software, hardware) could have consequences for all the co-hosted services.

From the point of view of information systems security, the main risks associated with co-hosting and their repercussions are as follows: loss of availability; loss of integrity and loss of confidentiality. These risks are amplified when data is processed in an uncontrolled environment.

Although outsourcing providers put security measures in place to protect data, there is always a risk of unauthorised access by malicious staff of the outsourcing provider. This can be particularly worrying when sensitive medical data is involved.

Added to this risk factor is the complexity of managing authorisations, which can arise when several establishments share a shared hosting infrastructure. For the analysis to be complete, it is necessary to address the legal risk factors.

B. Legal risk factors

In addition to the various operational risks we have discussed above, which seem obvious when it comes to an outsourcing operation, we need to add more subtle and therefore more complex factors linked to the legal aspect of outsourcing healthcare information systems. On the one hand, we will compare the elements that appear to be risks, but which in reality are sources of complexity for

the operation, and which stem from the legal nature of health data (1). Secondly, we will examine the contours of the contractual relationship (2).

1. The subject of the breach: health data

Although it may seem trivial, the special nature of healthcare data[275] , which is the subject of outsourcing, is a legal risk factor that the co-contractors must take into consideration. Because of its complex and highly regulated nature, health data should not be managed in the same way as other types of personal data under outsourcing arrangements.

According to Article 4-15 of the GDPR, health data is personal data relating to the physical or mental health of a natural person, including the provision of healthcare, which reveals information about that person's state of health[276] . It is considered to be sensitive data, i.e. data that is subject to enhanced protection under the law, as it is particularly intimate and likely to infringe the privacy or fundamental rights of individuals[277] .

Article 4-15 of the GDPR is at the heart of an important debate concerning the definition of health data and its implications for the processing of personal data. The definition of health data is crucial as it determines whether certain information falls into this category and is therefore subject to stricter processing under the GDPR. The debate centres on the clarity and scope of this definition, including what constitutes "disclosure of health information".

Article 9-1 of the GDPR sets out a general prohibition on the processing of health data, unless exceptions apply. These exceptions include the explicit consent of the data subject, the performance of legal obligations in the field of health, the protection of the vital interests of the data subject, etc.

Among the exceptions, explicit consent is often the subject of debate, as it must be free, specific, informed and unambiguous. In the medical context, obtaining truly informed consent can be complex, particularly when the person concerned does not fully understand the implications.

The broad scope of Article 4-15 of the GDPR encompasses not only traditional medical data, but also information related to healthcare services. This can include data related to fitness tracking, dietary habits, etc. This broad scope raises questions about privacy and data security. The disability debate is important because some disability information can be interpreted as health data. This could potentially pose challenges in terms of processing this information while respecting confidentiality and non-discrimination.

The legal nature of health data depends on the context in which it is collected, processed and used; but it is also based on the multitude of texts that provide a framework for its protection and which are likely to create legal uncertainty in the way in which such data will be handled by both health establishments and outsourcing providers.

---

[275] A. Banck, *RGPD : la protection des données à caractère personnel, 20 fiches pour réussir et maintenir votre conformité*, coll. "Droit en poche", Gualino-Lextenso, 2023, p. 29.

[276] CNIL: "What is health data", https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante, consulted on 24 July 2023

[277] N. Martial-Braz, F. Jault-Seseke, "Données à caractère personnel - Cadre légal - Champ d'application matériel", *Répertoire IP/IT et Communication*, July 2019, n° 70 s. ; Ch. Féral-Schuhl, *Cyberdroit,* coll. "Praxis", Dalloz, 2021, n° 132.01 s.

According to Recital 35 of the GDPR: *"personal data concerning health should include all data relating to the health status of a data subject which reveals information about the data subject's past, present or future physical or mental health. This includes information about the natural person collected when registering that natural person to receive healthcare services or when providing such services within the meaning of Directive 2011/24/EU of the European Parliament and of the Council for the benefit of that natural person; a specific number, symbol or element assigned to a natural person to uniquely identify him or her for healthcare purposes; information obtained from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information concerning, for example, a disease, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition of the data subject, irrespective of its source, whether it comes, for example, from a doctor or other healthcare professional, a hospital, a medical device or an in vitro diagnostic test."*

The CNIL's concept of health data is now broad[278] . It must be assessed on a case-by-case basis, taking into account the nature of the data collected, and on this basis health data can be classified into three categories:

- *data which is health data by nature: medical history, illnesses, care received, test results, treatments, disabilities, etc.".*
- *data which, when cross-referenced with other data, becomes health data in that it enables a conclusion to be drawn about a person's state of health or health risk: cross-referencing a weight measurement with other data (number of steps, calorie intake measurement, etc.), cross-referencing blood pressure with exercise measurements, etc.*
- *those which become health data by virtue of their intended purpose, i.e. the use made of them for medical purposes"*[279] .

The legal nature of health data has consequences for the conditions under which it is processed. Indeed, the GDPR imposes specific obligations on data controllers and processors who process health data, particularly with regard to the legal basis[280] , consent[281] , integrity and confidentiality[282] , the rights of data subjects[283] and transfers outside the European Union[284] .

Added to this are the debates surrounding the principle of prohibiting the processing of sensitive data[285] , which includes health data, as set out in Article 9-2 of the RGPD, and its derogations, whose contours are still unclear and which constitute legal risk factors in the context of the outsourcing operation.

The RGPD unequivocally prohibits the processing of so-called sensitive data. This prohibition is justified in particular by the nature of the data and the potential risks to the privacy of the individuals concerned. This is based on the fact that so-called sensitive data is eminently personal data that is likely to lead to discrimination if it is revealed or processed for purposes or in ways that do not guarantee the data subject protection of his or her rights and freedoms. This is why the

[278] CNIL: "What is health data", https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante consulted on 24 July 2023.
[279] CNIL: "What is health data", https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante consulted on 24 July 2023.
[280] Article 6-1 of the RGPD. The CNIL states that *"The legal basis for processing is what legally authorises its implementation, which gives an organisation the right to process personal data. It may also be referred to as the 'legal basis' or 'legal basis' for processing". https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales*
[281] Art. 6-1-a and art. 7 of the RGPD.
[282] Art. 5-1-f and art. 32
[283] Right to information (art. 13 and 14 of the RGPD); Right of access (art. 15 of the RGPD); Right of rectification (art. 16 of the RGPD); Right to be forgotten (art. 17 of the RGPD); Right to limitation of processing (art. 18 of the GDPR); Right to data portability (art. 20 of the GDPR); Right to object (art. 21 of the GDPR); Right not to be subject to an automated individual decision (art. 22 of the GDPR).
[284] Articles 44 to 49 of the RGPD.
[285] L. Maisnier-Boché, "Données de sante à caractère personnel. - Régime général", JurisClasseur Communication, Fascicule n° 945, 31 December 2019.

processing of this category of data is prohibited as a matter of principle[286] .

Exceptions to the principle of prohibiting the processing of sensitive data are provided for in both the RGPD and the Data Protection Act.
The RGPD authorises the processing of sensitive data in specific cases (RGPD, Article 9, § 2)[287] .

As for the Data Protection Act, it goes beyond the list of exceptions that allow sensitive data to be processed, within the framework of the leeway provided by the RGPD (L. no. 78-17, 10 Jan. 1978, art. 44). It does, of course, include the list of exceptions set out in Article 9 of the RGPD, but adds certain cases[288] :

To this first list of risk factors must be added factors relating to the framework within which the obligations laid down by law are carried out, i.e. the contractual framework.

2. The achievement framework: the contract

The specific nature of the outsourcing contract is the starting point for a risk factor inherent in the contractual delimitation of the outsourcing provider's involvement, since there is a direct and obvious link between the manipulation of health data, computer fraud and the vulnerability of the system, insofar as it is the illicit nature of the processing of this data that will be the starting point for all the considerations.

A vulnerability is a *"malicious or clumsy error in the specification, design, implementation, installation or configuration of a system, or in the way in which it is used"*[289] . From a personal data protection point of view, vulnerability is envisaged by the RGPD in Articles 5-1-f (principle of integrity and confidentiality)[290] ; Article 32 (security of processing)[291] , Article 33 (notification of data breaches to the supervisory authorities)[292] and Article 34 (communication of data breaches to data subjects)[293] already mentioned.

[286] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulted on 24 July 2023.
[287] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulted on 24 July 2023.
[288] https://open.lefebvre-dalloz.fr/droit-affaires/protection-donnees-personnelles/connaitre-regles-applicables-traitement-donnees-sensibles_a93004 consulted on 24 July 2023.
[289] ANSSI glossary: https://www.ssi.gouv.fr/entreprise/glossaire/v/ consulted on 24 July 2023.
[290] This principle stipulates that personal data must be processed in such a way as to guarantee appropriate security. This is a fundamental principle of data protection which emphasises the need to put in place technical and organisational measures to prevent unauthorised or unlawful processing, as well as accidental loss, destruction or damage to data. This makes it possible to minimise the risks of vulnerability by ensuring that data is processed with adequate security.
[291] This article details the measures that data controllers and processors must take to guarantee an appropriate level of security for the processing of personal data. These measures include, among others, pseudonymisation, encryption, the ability to restore data availability in the event of an incident, and regular procedures for testing and evaluating the effectiveness of security measures. By implementing these measures, organisations can significantly reduce the vulnerability of data to threats and risks.
[292] Article 33 requires data controllers to notify personal data breaches to the competent supervisory authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. This provision is crucial to mitigate the consequences of data breaches and to enable the authorities to take appropriate measures to protect the rights of vulnerable individuals whose data has been compromised.
[293] Article 34 states that, in certain circumstances, data subjects must also be informed of data breaches if these are likely to result in a high risk to their rights and freedoms. This communication enables vulnerable

The outsourcing contract is a contract for services as set out in article 1710 of the French Civil Code[294] , and as such it contains the seeds of several risk factors. The first of these is the difficulty in strictly defining the scope of intervention of the outsourcing provider, and more specifically of its staff. It should also be pointed out that this type of contract excludes any power of representation (i.e. it cannot be seen as an agency contract). Although, traditionally, the services provided under a contract for services concerned material acts, today there is no difficulty in considering that they may be intellectual*: "work of an intellectual nature is not excluded from the definition of a contract for services"*[295] .

To this provision of the Civil Code relating to the general scope of the subcontracting contract, it is essential to add the obligations set out in Article 28 of the RGPD. Article 28 of the RGPD deals with the relationship between data controllers (those who determine the purposes and means of data processing) and processors (those who process data on behalf of data controllers). This article imposes specific obligations on processors with regard to the protection of personal data. The provisions of this article include the need to conclude a data processing contract between the controller and the processor, which must contain certain specific clauses to guarantee the security and protection of personal data.

Computer fraud consists of an unauthorised and damaging intrusion into the health care organisation's computer system. This means not only that the intrusion has been made outside the terms of the contract, but also that it has caused damage to the health care organisation and, by extension, to the people to whom the health care organisation is legally considered to be responsible for data processing.

This aspect makes it possible to systematically switch to the criminal aspects of such an intrusion. The Law of 5 January 1988[296] was a pioneer in the field of specific information technology offences, and its provisions are still at the heart of the matter. The legislative provisions on combating IT-related offences[297] punish :

- fraudulently accessing or remaining in all or part of an automated data processing system;
- hindering or distorting the operation of an automated data processing system;
- fraudulently introduce data into an automated processing system;
- fraudulently extract, hold, reproduce, transmit, delete or modify the data it contains.

Added to this is the fact that an IT outsourcing contract involves a number of related obligations, making the contractual process complex.
In very concrete terms, it is relevant to mention the reversibility clauses and the mandatory audit clause in Article 28-3-h of the RGPD. Reversibility clauses are contractual provisions that aim to ensure that, in the event of the end of a contract or a

individuals to take steps to protect themselves against the potential consequences of the breach.

[294] Art. 1710 Civil Code: "A work contract is a contract by which one of the parties undertakes to do something for the other, in return for a price agreed between them".

[295] Cass. 3e civ., 28 February 1984, no. 82-15.550: *Bull. civ.* III, no. 51.

[296] Law no. 88-19, 5 January 1988 on computer fraud, OJ 6 January 1988, p. 231.

[297] C. pén., art. 323-1 et seq.

change of processor, the data transferred to the processor is returned or transferred securely to the controller. This may include requirements for the return of data, the deletion of data, the provision of copies of data, and so on. However, the practical implementation of reversibility clauses can be complex, particularly where data is processed on multiple systems, in different formats, or where it is interconnected with other data.

Reversibility can become problematic if the subcontractor does not have good documentation of the location of the data, its format and processing methods. There may also be costs and technical difficulties associated with migrating or restoring the data.

In addition, Article 28-3-h of the RGPD stipulates that the data processing contract must include a clause allowing the controller to have audits carried out by the processor or by a third-party auditor to assess compliance with the processor's obligations. This is intended to ensure that the controller can verify the processor's compliance with the requirements of the GDPR. However, the practical application of this clause can be complex. Audits can require time, resources and close coordination between the controller, the processor and the third-party auditor. In addition, there may be concerns about the confidentiality of the processor's commercially sensitive information. Nevertheless, this clause is essential to maintain adequate oversight and ensure that data is processed in accordance with data security standards.

A Data Protection Impact Assessment (DPIA) is an assessment of the risks associated with the processing of personal data, required under Article 35 of the RGPD for processing operations presenting a high risk to the rights and freedoms of data subjects. In the context of outsourcing health information systems, it is important to carry out a DPIA to identify the risks associated with health data and put in place measures to mitigate them.

Moreover, this complexity makes it difficult to determine precisely the nature of the obligation that will be incumbent on the outsourcing provider. As legal doctrine has pointed out, the distinction between obligations of means and obligations of result, which is *"more clumsy than wrong"*[298] , has not been enshrined in the reform of contract law. However, it will continue to play a full role, particularly in contracts for work and services. The elements that lead to the solution are the activity, the hazard, the will of the parties and the role of the customer[299] . Once these various risk factors have been identified, it seems natural to analyse the liability regime relating to facilities management in healthcare establishments.

[298] Ph. Malaurie, L. Aynès, Ph. Stoffel-Munck, *Droit des obligations*, LGDJ, 11e ed., 2020, no. 941.

[299] F. Labarthe, C. Noblot, "Le contrat d'entreprise", *JurisClasseur Contrats - Distribution*, Fascicule no. 425, 1er July 2021, no. 163 ff.

Network security in the OAPI and *OHADA* areas

By Jeanine Tano-Bian

Doctor of Law, Cybersecurity Consultant Lecturer-Researcher, University of Abidjan

Summary

An integral part of the information system, the network is both a channel and a container. It receives data that it transports. It is therefore necessary to consider the confidence of the holders of the rights attached to this data, as well as their relationship with the network. It is also interesting to study the issues of interaction between networks and, consequently, interconnection. How do OAPI member states ensure network security? What technological tools and legal mechanisms are available? Technological advances call for a review of network security, which is fundamental in terms of intellectual property. The aim of this study is to show the adaptations made by States in terms of network security using techniques linked to the digital economy.

Key words: States, OAPI, OHADA, networks, security.

Introduction

Network security is a vast and wide-ranging field involving confidentiality, integrity and availability. According to the typology of networks and systems developed by Michel RIGUIDEL[300] , there are computer networks[301] , telecoms networks[302] , television broadcasting networks, information systems for the state, institutions, businesses, banks, organisations, home networks (domestic network), management of critical infrastructures and the emerging digital heritage of families and individuals.

In support of this typology, ensuring network security means protecting an information system and the activities that run on it, the functionality of the system and the integrity of the network, especially the data that passes through it using hardware and software technologies: information system networks are internal[303] and external[304] . Consequently, ensuring the security of information systems[305] requires anticipating attacks that could damage the said systems and responding to attacks with acts of defence and repair where necessary.

The mechanisms implemented are based on legal texts, most of which were drawn up following technical observations. In other words, the technical understanding of safety, in other words action, precedes the framing of this safety in law.

Technological activity is upstream of the development of the foundations for preventive and curative behaviour. Indeed, it is the recurring cybercrime attacks that have led governments to think about repressive legislation in this area.

---

[300] Cf. Riguidel Michel, la sécurité des réseaux et des systèmes, 2006

[301] Local corporate networks, IP video surveillance networks, the Internet, wireless networks (WiMax, Wifi, Bluetooth), passive smart label networks (RFID);

[302] Satellite networks, GPS or Galileo positioning networks, telephone networks, mobile phone operator networks (GSM, GPRS, EDGE, UMTS)

[303] Under Beninese law, an internal network is an independent network set up entirely on the same property, without using the public domain (including the radio), atmospheric space or third-party property.

[304] Like facilities management, which the Agence française de normalisation (AFNOR) defines as the result of integrating a set of basic services to entrust an IT service provider with all or part of a customer's information system, under a fixed-price, multi-year contract with a defined level of services and duration.

[305] AKOKA Jacky, BRIOLAT, Dominique and COMYN-WATTIAU Isabelle (1998) "La Sécurité des réseaux : une approche de détection de malveillances," Systèmes d'Information et Management : Vol. 3 : Iss. 2, Article 2. Available at: http://aisel.aisnet.org/sim/vol3/iss2/2

The network, an integral part of information systems, is no exception to the rule. More specifically, Act No. 2017-20 on the Digital Code in the Republic of Benin[306] defines a network as a connected set of computer systems, regardless of how they are connected. Connections may be grounded, wireless or both. It should be noted that a network may be geographically limited to a small area or cover a large area and such networks may themselves be interconnected.

How do the Member States of the OAPI and OHADA envisage network security?

It may seem audacious to study these two areas together, but on closer inspection, they intersect and overlap: the Member States are the same 17 Member States of the OAPI and OHADA. They are Benin, Burkina Faso, Cameroon, Central African Republic, Chad, Comoros, Democratic Republic of Congo, Côte d'Ivoire, Equatorial Guinea, Gabon, Guinea, Guinea Bissau, Mali, Mauritania, Niger, Senegal and Togo. It is against this backdrop that the member states of the African Organisation for the Protection of Intellectual Property are at the heart of the debate on network security.

In practice, several texts[307] converge in this sense insofar as the activity of securing networks is multifaceted and obliges legislators to take into account all the sectors concerned.

In order to understand network security as provided for by the OAPI States without betraying the fundamental objective of protecting intellectual property, it is necessary to check how network security is ensured from the point of view of prevention before assessing its structural effectiveness. This approach shows that network security in the OAPI and OHADA areas takes account of the technical nature of the field (I), which seems to require it. In addition to this technicality, structural needs impose it *a posteriori* (II).

II- A priori security required by the technical nature of the field

In drawing up the rules governing it, network security seems to borrow a little from general international law as defined by COMBACAUD and SUR[308] in the repressive field of cybersecurity. Above all, the regulations have specific aspects that are specific to regionalism, as emphasised by TCHAMENI[309] . Whichever prism is chosen, network security implies security of access to the network. This refers to the security of telecommunications in terms of their availability (1) and the security of the transport of these communications, which presupposes the operation of the networks (2).

3. Network availability: an essential prerequisite

The network is said to be secure when it is available. According to Solange Ghernaouti, this availability is ensured by the creation of a secure network infrastructure for network

[306] Law available on https://sgg.gouv.bj/doc/loi-2017-20/

[307] The OAPI and OHADA areas will be highlighted, but the texts called together could be drawn in particular from the digital code and laws relating to cybersecurity, and not just intellectual property and business law texts. The latter will also be called upon, but in addition to texts more specific to the field of security.

[308] Jean COMBACAUD and S. SUR, Droit international public, Paris Montchrestien 2012, P. 46

309 TCHAMENI, les évolutions du régionalisme africain, Paris, L'Harmattan, 2013, p.17 et seq. see also Dr. Abdulqawi A. YUSUF, Panafricanisme et droit international, Hague Academy Special edition, 2017.

access and information transport[310] . Access to the network is secured by the implementation of a *login* mechanism incorporating an identifier and a password, with the proviso that these passwords must be changed regularly and kept confidential. This aspect combines the need to ensure the integrity of the information while guaranteeing its secrecy and, ultimately, the operational nature of a system that functions correctly and flawlessly.

One type of attack on availability is denial of service. This is an attack on the information system that blocks it by preventing people from accessing it, or by preventing access to the services offered by the site or interface consulted. The fact that the OAPI countries have legislation to criminalise and punish this type of reprehensible behaviour, which undermines the availability of networks, is a guarantee of the security of network availability.

A network is said to be available when the service it offers is operational during a specified period. In this respect, Solange Ghernaouti emphasises that it *is not enough for a resource to be available; it must be usable with acceptable response times. Its availability is inseparable from its ability to be accessed by all rights holders (notion of accessibility). The availability of services, systems and data is achieved by appropriate dimensioning and a certain amount of redundancy, as well as by effective operational management and maintenance of resources.*

In order to ensure the availability of networks, article 1 of the Congolese cybersecurity law[311] states that it governs the national legal framework for the security of information systems and electronic communications networks. As such, it aims in particular to organise and coordinate the security of information systems and electronic communications networks. The rest of the provisions of this law provide for a set of mechanisms to prevent possible and certain risks. In addition, article 27 of the Congolese law on cybersecurity states that "content providers of electronic communications networks and information systems are required to ensure the availability of content, as well as that of data stored in their facilities".

4. Network operating security: content, necessary corollary

The operation of networks refers to their use and, consequently, to the information they transport and store, for which they represent a channel. As Ghernaouti points out, operational security relates to the *proper functioning of computer systems and telecommunications networks*. It includes the implementation of tools and procedures relating to operating, maintenance, test, diagnostic, performance management, change and update management methodologies.
Content involves applications and software that are used to secure networks. At this stage, it seems imperative to ask what the intellectual property provisions say about these security tools. It is true that there are plans to secure a network, but are the people who produce these security tools assured of the ownership of their invention?

Protecting the people who have created security tools remains a fundamental issue in guaranteeing security and avoiding the risks of hacking or hijacking. This aspect relates to

[310] Cf. S. GHERNAOUTI, cybersécurité, analyser les risques, mettre en œuvre les solutions, 7e édition DUNOD

[311] Law no. 26-2020 of 5 June 2020 on cybersecurity published in the JO 2020-23.

the structural security of networks, which needs to be addressed.

III. Structural a posteriori security

Network security as understood by the texts of the OAPI or OHADA States is structural insofar as it ultimately targets the objectives of competitiveness, logical security and competition.

2. Long-term, high-performance safety targets

A secure network is more competitive because it is more attractive. This is why secure sites will be more productive insofar as customers will be more confident in the owners of these sites offering spaces without fear. In particular, they can be sure that their information will not be stolen. Network security is becoming a mark of trust and an indicator of merit and excellence. It is therefore a competitive advantage, since it now represents a strength for the company or site that guarantees it to its visitors, customers or prospects.

Studying the strength of network security requires performance indicators. Using behavioural studies of visitors to sites, accounts or virtual shop windows, we can see how important it is to secure the performance sold throughout the value chain.

The protection of software and databases[312] has evolved in terms of its legal framework. This legal protection is provided in the OAPI area by copyright and related rights. The Bangui text enshrines the protection of databases and sets as a criterion "the choice, coordination or arrangement of subject matter". In terms of security, there is really no specific protection for them alone.[313] . The arrangement of the data and its organisation in the database mentioned above is indeed a manifestation of originality.

In addition to this example of Ivorian legislation, Senegalese law provides for minimal protection of the database. But it is restricted to the structure and does not extend to the composition as such. Following in the footsteps of Elhadji Oumar Ndiaye[314] , who in his thesis describes the protection of databases under Senegalese law, it is regrettable that Senegalese law has not taken this opportunity to provide greater protection for the content of databases, which in general are the result of a combination of criteria that give them originality. What is undoubtedly lacking in African law is sui generis protection.

---

[312] Nathalie Mallet-Poujol, that "the database can be either a simple reservoir of data on a computer medium, or a reservoir of data that has undergone preliminary indexing, or a reservoir of fully structured data files. Nathalie Mallet-Poujol, "Protection des bases de données", JCL Propriété littéraire et artistique, Fasc. 6080, no. 20.

[313] Case law had long accepted the need to protect the original structure of a collection whose content was not protected by copyright. It has been ruled that "the fact of assembling these data into an ordered and complete whole, and classifying them in various nomenclatures constitutes a personal work" 95. More recently, in its judgment of 28 December 1998, the Lyon Regional Court considered that a collection of collective agreements could be protected as a work on the grounds that "the arrangements, presentation and layout used make consultation of the 'Permanent Dictionary' (the collection) simpler and more attractive than the original": for cases in France, see Cass. 1re civ., 9 Nov. 1983: JurisData no. 1983-702217; JCP G 1984, II, 20189, note A. Françon. - Cass. ass. plén., 30 Oct. 1987, n° 86-11.918 : JurisData n° 1987-001712 ; JCP G 1988, II, 20932, rapp. X. Nicot and note by J. Huet; JCP E 1988, II, 15093, obs. M. Vivant and A. Lucas; D. 1988, p. 21, concl. J. Cabannes; RTD com. 1988, p. 57, obs. A. Françon 95 CA Paris, 18 Dec. 1924, Didot-Bottin, regarding data compiled from the telephone directory.

[314] Elhadji Oumar Ndiaye, La protection des bases de données par le droit d'auteur : approche comparative entre le droit français et le droit sénégalais. Droit. University of Montpellier; University of Saint-Louis (Senegal), 2017. French.

To this end, the criteria vary according to the needs for which the databases are created, which explains why it is not easy to find the same criteria from one database to another. The composition of a database should have been protected in the same way as its structure.

In reality, it should be noted that protection is primarily guided by the transfer of skills[315] . On the basis of the transfer of technological skills, the distribution of copyright over a database or software will depend on the level of freedom of the software in question[316] . For example, in the production or creation of applications, a number of pre-established algorithms or algorithms created by reputable firms holding patents or making operating licences available are used as borrowings from previous creations. Depending on whether they are open source or duplicable, these earlier creations will have minimal protection. This consideration does not facilitate the specific protection of software created in this context.

Logical security refers to data protection and the implementation of software security mechanisms that contribute to the proper functioning of the programmes and services offered. The quality and security of software development and security testing, and the appropriate use of cryptography to ensure data integrity and confidentiality. Logical access control and authentication procedures. All of these derivatives of logical security, as described by Solange Ghernaouti, make it possible to apply the provisions relating to network security and specifically facilitate the achievement of security objectives: they guarantee the confidentiality and integrity of data.

For structural security to be complete, the OAPI member states must define the levels of responsibility and identify the players involved in securing the networks.

2. Players with precisely defined responsibilities: responsibilities proportionate to the players

Cameroon's 2010 law governing network security includes a general electronic security policy. On the basis of this policy, Cameroon is separating the National Agency for Information Technology[317] and Communication from the Telecommunications Regulatory Agency.

In the Congo, the Digital Code distinguishes between the stakeholders, principally the authorities responsible for network security, which are the Digital Regulation Authority, the National Electronic Certification Authority and the National Digital Council. Each has coercive or consultative missions. It is in this respect in particular that it is possible to mention that networks are subject to risk monitoring requirements, which are obligations contained in the Congolese cybersecurity law[318] . For example, article 12 of the law states that: "*The information systems and electronic communications networks of the various public bodies are subject to a system of mandatory and*

[315] Raoul EHODE ELAH Tourere ZENABOU Victorine Ghislaine Nzino MUNONGO, le droit de propriété intellectuelle et le transfert de technologie, *Revue* Valaque d'Etudes Economiques, *Volume 5(19) N* °1. *2014*

[316] Saerens Patrick, Les créateurs, maillons faibles des Tic en Afrique ? N° 15/2B - Supplement 2014 ICT, cultural industries and creative industries: Social appropriation and cultural diversity Communication & Social Change in Africa 3rd International Colloquium Douala, 10 to 12 April 2014

[317] Law No. 2010-12 of 12 December 2010 on cybersecurity and cybercrime in Cameroon

[318] Law no. 26-2020 of 5 June 2020 on cybersecurity (JO 2020-23)]

periodic audit of the security of information systems". It should be noted that the mandatory and periodic audit of information system security is a security technique that takes several forms, including intrusion tests[319] . It is a security obligation incumbent on access providers and information system operators.

In Benin, the Digital Code sets out cross-cutting provisions with 360-degree security from the creation of the system through to its use and attacks: not only by users, but also by interconnections[320] and attacks from outside the network.

The fact that African legislators[321] have made provision for security managers is accompanied by penalties in the event of non-compliance with the obligations laid down. These requirements make it compulsory to secure systems, and consequently telecommunications and digital networks.

Conclusion

Network security in the OAPI and OHADA areas is ensured upstream by legislation under construction and downstream by practical applications under construction. Much of the legislation developed is at the experimental stage, as are digital technologies.

The legal framework for achieving security objectives for information systems and their components, as well as for the data passing through these networks, means that the availability of these networks must be observed and ensured. The corollary of this availability is the confidentiality but also the integrity of the data or information transported as a guarantee of security.

States would benefit from strengthening their cooperation insofar as Community instruments such as the OAPI and OHADA make it possible to pool security issues and objectives. Achieving effective and total security to curb cybercrime and high-level digital crime is a guarantee that covers not only national economies but also digital investment in Africa.

J.T.-B.

---

319 Jonathan Tournier, François Lesueur, Frédéric Le Mouël, Laurent Guyon, Hicham Ben-Hassine. Audit of an IoT system using penetration testing. RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, May 2018, Nancy, France. pp.1-3. ffhal-01937223e

320 This is defined as the physical and logical linking of networks open to the public, operated by the same or a different operator, to enable users of one operator to communicate with users of the same or another operator, or to access services provided by another operator, see on this subject N. COLIN et al, "Économie numérique", in Notes du conseil d'analyse économique 2015/7 (No. 26), pp. 1-12. [Https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2015-7-page-1.htm] quoted by Hervé Martial TCHABO SONTANG, in Les piliers juridiques du développement de l'économie numérique au Cameroun.

321 All the legislation of the countries involved has a section reserved for sanctions against operators or suppliers in the event of non-compliance with their obligations.

Expected entry into force: the Malabo cybersecurity convention

By Jeanine Tano-Bian & Christian Kpolo
Doctors of Law, Researchers, University of Abidjan

For several weeks now, social networks and specialist news forums have been chanting the ratification of the African Union Convention on Cybersecurity and the Protection of Personal Data. FINALLY! one is tempted to add. Indeed, it was on 27 June 2014 that the African Union represented by its member states adopted the said Convention in Malabo[322] .

African countries are criticised for not having uniform or harmonised texts regulating digital security. Scientists, researchers and even professionals are complaining about the inadequacy of court rulings in this area, as well as other drawbacks linked to a relatively slow awareness of the risks associated with the digital era.

It should be emphasised that ratification of the Malabo Convention has taken some time: almost ten years. Until recently, the expected number of ratifications by Member States had not been reached. However, the Convention only required the signature of fifteen (15) countries[323] as a condition for ratification. Traditionally, this includes a minimum number of ratifications. No other condition was required. For further information, the Malabo Convention will apply in the following States: Angola, Benin, Cape Verde, Côte d'Ivoire, Democratic Republic of Congo, Ghana, Mauritania, Mauritius, Mozambique, Namibia, Niger, Rwanda, Senegal, Togo and Zambia.

In 2023, the entry into force of this Convention is a cause for celebration. It should also be mentioned that adopting the Convention on Cybersecurity is an integral part of the African Union's Agenda 2063[324] .

It is now possible to refer to an African regional instrument for combating cybercrime, insofar as this text not only contains provisions for preventing cybercrime, but also for punishing cybercriminal acts and for regulating the protection of personal data, the breeding ground for all the abuses committed against and via digital networks.

Other advantages, such as the speed of proceedings, can be cited in favour of ratifying the Malabo Convention. In addition, it becomes the African regional instrument that will facilitate the contextualisation not only of any offences that may occur but also of effective cross-border judicial and legal cooperation. The fact that so few States have ratified the Convention raises questions about the place of cybersecurity issues in the governance of African States.

J.T.-B. & Ch.K.

[322] The African Union Convention on Cybersecurity and the Protection of Personal Data.
[323] Article 36 of the Convention states that: "This Convention shall enter into force thirty (30) days after the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification or accession".
[324] Flagship projects of Agenda 2063 | African Union (au.int)

Actors' cybersecurity obligations: analysis of the cybersecurity provisions in the Democratic Republic of Congo's new digital law

By Jeanine Tano-Bian & Christian Kpolo
Doctors of Law, Researchers, University of Abidjan

Cybersecurity is the set of policies, mechanisms and applications developed to achieve a real state of security for information systems and related networks. It has become a standard for competitiveness, a guarantee of confidence in digital technology and a value for the world's economies. The repressive challenges that governments face in the face of cybercrime are no longer enough; they need to be increasingly proactive through anticipation and prevention mechanisms, in all sectors of activity. As a result, each State is developing a policy for the security of its telecommunications and data transfer or transport areas.

How is the Congo approaching cyber security, integrating all parties into its preventive and defensive measures?

This dedicated space is an opportunity to study, in the light of the Congolese law on cybersecurity and ordinance-law 23/10 of 13 March 2023 on the digital code, how the Republic of Congo is integrating its stakeholders into the heart of their respective activities in the cause of cybersecurity.

Congolese legislation, with Act No. 26-2020 of 5 June 2020 on cybersecurity, has set itself the role of implementing measures to guarantee the security of networks and information systems. It places obligations on all stakeholders in the economic and social sphere.

The policy for applying these provisions aims to eradicate cybercrime and all forms of reprehensible behaviour or behaviour conducive to digital crime. As a guiding principle, the Congolese cybersecurity law categorises stakeholders and defines levels of responsibility, with penalties for non-compliance.

In the text relating to cybersecurity, the law puts in place mechanisms to prevent information systems from criminal activity. This body of rules for prevention and anticipation proposes measures to repair the flaws created by attacks.

Articles 4 and 5 of the Congolese cybersecurity law place a security obligation on anyone to take appropriate measures to protect and prevent any risks incurred by third parties as a result of this use. These provisions explicitly refer to companies as entities.

It is possible to analyse this formulation within the legal entities that may incur liability with regard to the extent of the risks envisaged by the use of communication and exchange channels made available to the public. Anticipating risks in the use of information systems and networks is primarily the responsibility of the user.

Article 5 also emphasises the responsibility of IT Departments to detect and respond to security incidents when they develop, supply, manage, maintain or use systems and networks. At this stage, the responsibility is more accentuated: it becomes responsible and accountable (guarantor) for security and, in addition, is required to constantly review and evaluate its own policies, practices,

measures and techniques to ensure that they are adapted to its various interfaces of intervention. It is therefore responsible for the compliance of its information system. In other words, compliance, which is an expected superior quality, refers to a set of approaches that make companies accountable through obligations specific to supply and management,

The Congolese legislator intends these provisions to provide a framework for behaviour and to specify the obligations incumbent on companies: security imperatives are taken into account and include, in particular, the processing of information and data, the availability, confidentiality and integrity of which must be guaranteed and preserved. In addition, the legitimate interests of other users and owners of information systems and networks must be respected. To borrow analyses from France, in particular from the Commission Nationale de l'Informatique et des Libertés (CNIL), the interest is legitimate if three cumulative conditions are met: it is manifestly lawful, determined in a sufficiently clear and precise manner, and it is real for the organisation concerned and not fictitious.

The mechanisms contained in Congolese law are realistic and technical, so that this law is avant-garde and specifies in its terms the prerequisites for security: it deals with the upstream, i.e. the prevention of acts that could constitute offences.

The Congolese legislator has adopted a concrete approach to a culture of cybersecurity, with self-regulation of the players involved. Companies and public authorities are adopting a security management approach based on risk assessment. This risk assessment not only concerns all levels of activity, but is also involved in all aspects of the operations of companies and public authorities.

They will have to implement the necessary resources to achieve the desired level of digital security, primarily through self-regulation). This includes, in anticipation, responses to identifiable or foreseeable threats, as well as the prevention, detection and resolution of incidents, systems recovery, ongoing maintenance, control and audit.

Article 8 of the Congolese law places the responsibility for this risk assessment on companies, and takes into account the damage to the interests of others or caused by others, made possible by the interconnection of information systems.

With these provisions in place, it seems possible to protect against cybercrime, even if it is virtually impossible to repair the damage when it occurs.

J.T.-B. & Ch.K.

Provisions on the liability of technical intermediaries in the DRC's new *Digital* Act

By Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

In this dense and abundant text, the DRC legislator has governed the digital aspects of the economy. The text covers personal data[325] , cybersecurity, cybercrime[326] , infringements of intellectual property rights and e-commerce. With regard to e-commerce, the new Congolese law covers freedom of trade, contracts[327] and the liability of e-commerce players. For the purposes of this article, only the provisions relating to the liability of those involved in e-commerce will be discussed briefly.

The provisions relating to the liability of e-commerce operators are included in a title devoted to the security of IT systems, more specifically in a chapter entitled general and specific obligations[328] .

Firstly, a section entitled general obligations lists the obligations incumbent on Internet service providers and online service providers. This section bears a striking resemblance to France's *Loi pour la confiance dans l'économie numérique*. The text of the DRC stipulates that these players are not subject to any general monitoring obligations (art. 286), but that they must combat certain specific offences (art. 287).

Under DRC law, Internet service providers and online service providers are required to identify the users of their services. Article 284 of the DRC's digital law provides that Internet access providers and online service providers "shall *not be held civilly and/or criminally liable for activities or information stored at the request of a recipient of their services, if they were not actually aware of their unlawful nature or [...] if, as soon as they became aware of it, they acted promptly to remove the data or make access to it impossible*". Internet access and service providers are therefore not a priori responsible for the content they carry. They can only be held liable if, after being informed of the content, they do not promptly remove the content of which they have been notified that it is unlawful.

With regard to notification of illegal content, the DRC text departs from both French law and other African texts (Benin's Digital Code, for example). Whereas other African laws, such as French law, cite cumulative conditions for presuming knowledge of illegal content on the part of the Internet service provider (or hosting provider), the DRC text cites alternative conditions. It reads: *"knowledge of the disputed facts is presumed to have been acquired by the online service provider when it is notified of <u>one of the following</u>[329] : 1. the date of notification [...]"*. By way of comparison, for example, the Beninese Digital Code states[330] : *"knowledge of the disputed facts is*

[325] See the column by A. Ngoue and I. Randrianirina forthcoming
[326] See the column by Ch. Kpolo and J. Tano-Bian above.
[327] See the forthcoming column by R. Mabouana
[328] DRC Digital Act, art. 281 et seq.
[329] We underline
[330] Art. 498

presumed to have been acquired by the online service provider when it is notified of the following[331] .

The wording of the DRC text is perplexing, as its application could pose practical problems. How, for example, can it be presumed that a technical intermediary is informed of the presence of infringing content simply because it has received the identity of a rightholder, even if it has not specified the content to be removed? The interpreter is then inclined to assume that this is a *lapsus calami.*

After the section devoted to general obligations, the DRC law envisages specific obligations. These concern cache providers (art. 290), hypertext link providers (art. 291), search engine providers (art. 292) and hosting providers (art. 293).

The cache provider is liable if it intervenes in the content or if, after being informed of the presence of content, it does not (promptly) remove it or make it inaccessible.

The hypertext link provider, like the hosting provider, is liable if it does not remove the disputed content following an injunction from the judicial or administrative authorities or "*if it did not become aware or aware of specific illegal information stored or illegal activities carried out by the recipients of its services, other than by injunction from the judicial authority*". The hypertext link provider or host who could not have been aware of the illegal nature of a content cannot be held responsible for it.

Specifically with regard to the hypertext link provider, the text specifies that it is also not liable if it *"has not promptly informed the judicial authorities to enable them to assess the nature of the information or activities and, if necessary, to order the removal of the content"*. The cache provider must inform the authorities, who will decide whether or not to remove content reported as illegal. This obligation is not repeated for hosting providers, although it is not clear why there is a difference between the liability of hypertext link providers and that of hosting providers on this point.

The search engine is liable if it is at the origin of the transmission of the disputed content, or if it selects the recipients, or if it modifies the content in question.
On the whole, the legislator has opted for a particularly light system of liability for those involved in e-commerce. This seems to run counter to the trend towards greater responsibility (which must be put into perspective) observed in European Union legislation.

Y.L.N.

[331] We underline

Review of personal data in Africa

By Aline Mbenoun-Ngoué
Doctor of Private Law and intellectual property law
Advisor to the OAPI and DPO-certified (RNCP)
Lecturer at the University of Lyon

Strengthening African personal data legislation

We welcome the arrival of two new pieces of legislation. The first is Tanzania's Personal Data Protection Act, which was published in 2022 and came into force on 1er May 2023, and the second is the Democratic Republic of Congo's Ordinance-Law no. 23/010 of 23 March 2023 on the DIGITAL CODE. However, only the Ordinance-Law of the Democratic Republic of the Congo, which we present briefly in this publication, is applicable.

The new legislation adopts a global approach. The legislator of the Democratic Republic of Congo is thus closer to the Cameroonian legislator and differs, for example, from the Senegalese legislator (see RSPIA April 2023). This global approach is characterised by the integration of the protection of personal data, referred to as "Personal Data", in a text that applies to several digital-related activities. However, in the context of the Ordinance-Law of 23 March 2023, this global approach is stronger because the protection of personal data is not expressly mentioned in the scope of the text. Chapter 1, Article

1 that: "(...) this Ordinance - Law applies :
1.digital activities and services ;
2.written documents, electronic tools and trusted service providers ;
3.digital content ;
4.the security and criminal law protection of IT systems.

It also sets out the tax, parafiscal, customs and foreign exchange rules applicable to digital activities and services in the Democratic Republic of Congo.

It is in Chapter 2, Article 2 (entitled Definitions), paragraph 30 that the concept of personal data is defined in the text. It is defined as "any information relating to an identified or identifiable natural person, directly or indirectly". This definition is similar, for example, to that in the **Additional Act A/SA.0/01/10/ of 16 February 2010 on the protection of personal data within the ECOWAS zone.**

In this regional text, personal data is**: "**any information relating to an identified or identifiable natural person, directly or indirectly by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, mental, cultural, social or economic identity". Certain new notions are provided for, such as the notion of Public Data defined in Article 2 paragraph 31: "**Public data**: data produced and stored in public data registers on the territory of the Democratic Republic of Congo as part of a public service mission by the State, the provinces, the territorial entities, the public services, establishments and bodies as well as legal persons under private law entrusted with a public service mission".

All the provisions relating to the protection of personal data are set out in Articles 183 to 270 of the new text. This legislation is fairly comprehensive, providing a complete

institutional framework with the creation of a Data Protection Authority (DPA) "(...) An independent administrative authority with legal personality and administrative and financial autonomy". This Data Protection Authority has powers (Article 262 et seq.); it is also made up of three bodies with powers specified in Article 264 et seq:

1. The Planetary Assembly ;
2. The Executive Committee ;
3. Standing Committees (...)".

The new legislation of the Democratic Republic of Congo contains more comprehensive provisions than some national laws in African countries. It is therefore of great interest. An analysis of this text is planned for the next issue of RSPIA.

A.M.N.

REVIEW OF SCIENTIFIC WORKS

By Ampah JOHNSON-ANSAH
Head of the Private Law Department
University of Lomé (Togo)

Éric MONTCHO-AGBASSA
Professor of Law,
University of Cotonou (Benin)

Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

AKPAH Ayélé Edwige

The FTAA and the free movement of intellectual goods

Master's thesis in corporate law, Institut supérieur de droit et d'interprétariat, Université de Douai, 2022

Ms AKPAH has set herself the task of envisaging how the free movement of intellectual property will be operationalised in the new African area forming a continental free trade zone. The creation of such an area could presuppose the automatic free movement of products incorporating intellectual property rights. However, the European experience clearly shows that the establishment of a common market governed by the free movement of goods, people and capital does not always automatically mean the free movement of intellectual property. Everyone knows that it is the mechanism of the exhaustion of rights, which can be summarised as the distribution of intellectual property, that has made it possible to respond to this problem in a more or less effective way. This question will certainly be posed in different terms in African law for the simple reason that Africa is not yet a large market for intellectual property. This is one of the main themes of this dissertation, as Ms AKPAH has rightly pointed out.

According to the author of the brief, the automatic nature of the free movement of goods incorporating intellectual property rights needs to be toned down. In particular, she refers to the mechanism of exhaustion of intellectual property rights as a means, in relation to the FTAA, of tempering the automaticity of the free movement of such rights. This compares with Europe, where the common market was established in the 1950s without there being any free movement of these special products, which are relatively exempt from the general law of free movement. On the contrary, it took a process of reading and understanding the specific purpose and essential function of each right to organise free movement on the basis of intra-Community exhaustion. The question of the permanence of the territoriality of intellectual property rights and the non-harmonised methods of exhaustion throughout the continent will continue to arise.

Some countries have subscribed to national exhaustion, others to international exhaustion, which also constitutes a kind of flexibility, following the example of the OAPI since the Bamako Act of 2015. The impossibility of automatic free circulation may lead to resistance from holders to the exhaustion of their rights. African judges would then have to be relied upon to overcome it, just as European judges have made the free movement of products incorporating intellectual property rights conditional on certain fundamental requirements such as consent and the marketing of products in the European area.
The FTAA must not ignore this philosophy in implementing the free movement of intellectual

assets. Despite the continental fact surrounding it, the desirable mode of exhaustion for intellectual goods seems to be international exhaustion. Counterfeit goods must be excluded from the scope of exhaustion and border controls must be tightened. We can only agree with the conclusion of this paper, which states that "*a new era is opening up for the African continent and it seems important to measure the stakes of this strong initiative in order to derive maximum benefit from it in the interests of the African people*".

A.J.A.

EKUE Foli Fabrice Crédus

The criminal law of infringement of industrial property rights in the OAPI area

Master's thesis in Private Law, University of Lomé, 2021

Mr Ekoué Folly Fabrice's dissertation reveals the problem of the deterrent effect of criminal law in intellectual property law. However, he clearly notes that counterfeiting must remain a hybrid offence, as its criminal aspect is an effective deterrent in the fight against infringement. This observation is reinforced by the strengthening of penalties for counterfeiting in the Bamako Act, which renews the expression of the dissuasive force of the criminal law of counterfeiting. It puts criminal law back at the heart of the fight against counterfeiting. The author rightly points out that criminal sanctions alone are not enough. On the one hand, victims must make frequent use of criminal counterfeiting law and, on the other, the penalties provided for must actually be applied. Victims would thus be encouraged by the satisfactory results of the criminal route.

Apart from the lack of interest shown by victims, the scarcity of criminal sanctions for counterfeiting in the African context is also the result of the weakness of the means used to enforce industrial property rights. The lack of means of enforcing laws makes it hypothetical that the rights of owners will be respected. In this case, the author argues that the effectiveness of the protection of industrial property rights has a major economic stake: the influx of foreign investors, who are very attentive to the legal and judicial environment of States. It also makes the judge a decisive player in the fight. Through their decisions, they should relay the legislator's message of firmness with regard to counterfeiting. In addition to improving the institutional and legal framework, it would seem appropriate to adopt other anti-counterfeiting strategies. The fight against counterfeiting cannot prosper without greater societal acceptance of industrial property. The public within OAPI has a limited understanding of the economic and even social dimension of industrial property rights. For the author, precariousness plays an important role in the current situation of OAPI countries with regard to counterfeiting.

It would encourage the mass use of counterfeit products that are dangerous to human health, particularly medicines. We therefore need to raise awareness of the proven dangers of counterfeiting for the economy, employment, national security and, above all, health. It follows that the fight against counterfeiting must involve making the various players involved in the counterfeiting circuit accountable, mainly for counterfeit products that are a direct threat to human life, particularly medicines. Accountability therefore appears to be a moralising concept, a moral responsibility that consists in making those involved in the counterfeit trade aware of the need to protect the general interest.

Over and above this awareness-raising, which has little to do with industrial property, he shows that the legislator's desire to combat counterfeiting is encountering various obstacles that are not conducive to the emergence of criminal proceedings, before concluding with the bitter observation that "counterfeiting, a hybrid action, is suffering from hemiplegia. It is becoming one-legged because criminal proceedings have been all but abandoned". Let's hope that the author's cry of distress will be heard by practitioners in the field and that they will also seek to punish acts of

counterfeiting in order to fully restore the criminal field and the rights of owners, and above all so that counterfeiting is genuinely taken seriously. As a doctoral student working on a topic relating to intelligent contracts, we hope that he will soon return to intellectual property law.

A.J.A.

DOUTY Marléne

The obligation to work a patent in the OAPI

Master's thesis in Private Law, University of Lomé, 2019

Mr DOUTY Marléne obtained a master's degree in private law before embarking on a career as a writer and performer, a field in which he feels even more at home. He already has nearly five published plays to his name and is the initiator of the "Théâtre chez vous" programme, which takes his team to schools, public places and even homes for theatrical performances. In his paper on the obligation to exploit patents, he discusses the relationship between industrial development and patents through the exclusion of importation from the acts conferred on patentees in the 1977 agreement. He emphasised that through this exclusion and the requirement of local exploitation, the objective pursued by the 1977 Bangui Agreement seemed clearer, with the patent occupying a predominant place. Its development is an infinite source of wealth.

The OAPI legislator had therefore made local exploitation of the patent a hobbyhorse, a sacrosanct principle. The obligation to work the patent therefore acts as a lever to enhance the socio-economic value of the patent in the general interest of the population. Indeed, the exploitation of a patent creates a definite economic and social interest. In view of all these interests, which are a matter of public policy, the legislator in the OAPI region has instituted an obligation to exploit the patent, severely penalising non-exploitation by means of a compulsory licence and other mechanisms such as the refusal of any infringer of this obligation to take legal action for infringement, and the non-renewal of the patent, the legal exploitation period of which is ten years, renewable once. Unfortunately, the same legislator is going to break down the watertight walls he has erected.

The author does not really emphasise the failure of sanctions for the local non-exploitation of inventions. However, he points out that the TRIPS Agreement, which was signed on 15 April 1994 in Marrakech by the WTO member countries, including the OAPI countries, and the OAPI itself as an organisation, has largely contributed to this disaffection with this mechanism, which is so important in controlling the economic effects of invention patents. This agreement would introduce a certain number of rules unfavourable to OAPI countries, namely the legal duration of patent exploitation, which is twenty years, and the standardisation of rules governing all intellectual property rights. At the same time, the new agreement seems to considerably dilute the force of the compulsory licence. The author believes that in this case the obligation to exploit the patent in situ has lost its substance and vigour. It would even be reduced to nothing with the admission of importation as a conferred right.

By weakening the obligation to exploit, the legislator has deprived it of the possibility of provoking industrial development through technology transfer, and social development through the creation of well-being for the population. However, thanks to the emulation around patent exploitation created by strong competition between companies, it can be seen that the patent retains a certain place in the development of space and that its exploitation in space is being revived. This is a form of survival or even a revival of the obligation to exploit in situ. It seems to us, however, that it is only by raising awareness that Africa can develop its culture of industrial property to meet its own challenges.

Furthermore, there is nothing to prevent the OAPI legislator from imposing the exploitation obligation

despite the TRIPS Agreement. The author concluded his brief by expressing the hope that States will be able to derive maximum benefit from the international exhaustion adopted in the 2015 agreement in order to compensate for the loss of vigour of the exploitation obligation. We wish Mr Douti Marléne all the best, so that his inspiration does not run out as a performer and author and his works are exploited to the full.

A.J.A.

ADZOH Oli-Sika

The effectiveness of intellectual property rights in the OAPI area: the case of the invention patent

Master's thesis in Trial Law, University of Kara, 2019

If there is one point that is hotly debated in intellectual property law in Africa, it is the effectiveness of these rights, which rhymes with their effectiveness, efficiency and usefulness for a continent that is struggling to build itself and the foundations of a genuine intellectual property culture. The issue emerged in the 1970s and persisted until 1995 with the TRIPS Agreement. It does not appear to be closed. This is what Ms ADZO Oli-Sika's dissertation reveals.

The author begins by pointing out that effectiveness manifests itself in terms of the purposes of patent law and in terms of the exercise of the patentee's exclusive right. Curiously, he constructs effectiveness solely on the existence of patent law. She notes that, with regard to the aims of patent law, the OAPI legislator has set itself the objective of effectively protecting the rights of patentees. It adds that supranationality is a significant factor in assessing this effectiveness. This supranationality can be seen in the centralisation of the procedures for obtaining a patent. Above all, it highlights the attractive nature of the African patent. This character is inherent in the quest for efficiency. In addition, the protection of the patentee is reinforced by the OAPI's adherence to international conventions. This adherence to international conventions is a guarantee of security not only for the patentee, but also for investors.

The author did not fail to highlight the eternal problems of the African patent due to the weakness of the African intellectual property culture. The social function is in a bad way because of the extension of the field of rights conferred on imports. The issue of access to pharmaceutical products was mentioned as one of the weak links in the patentability of medicines.

However, the general interest is being taken into account, albeit intermittently. This insufficient consideration of the general interest is marked by the flexibilities granted by the TRIPS Agreement. The Bamako Act, which revised the Bangui Agreement of 1999, took into account certain flexibilities such as the Bolar exception and the postponement of the patentability of pharmaceutical products until 2031. The effectiveness of African patent law would also be compromised if there were no requirement for patents to be exploited locally.

As a result, many foreigners obtain OAPI patents but do not exploit them in the OAPI, making the patent an instrument of marketing monopoly. They use OAPI patents to control the import and sales market for their patented products. This situation has a negative effect on all OAPI member states. Efficiency is also demonstrated through the exercise of exclusive rights by patentees. He enjoys a monopoly of exploitation by which he can exploit his invention. Exploitation can also take place through third parties by means of licence or assignment contracts.

This is proof that only the patentee has the right to exploit his invention. Exploitation by a third party without the patentee's authorisation is an infringement. However, the patentee may be deprived of this right if he does not exploit his invention. The mechanism of compulsory

exploitation and compulsory licensing helps to limit the patentee's exclusive rights. However, it is used very rarely and is of only relative interest in assessing the exclusive right. The marketing monopoly, for its part, will be considerably affected by the Bamako Act of 2015 as a result of the international exhaustion adopted by this agreement.

Ms ADZOH states that "a semblance of effectiveness is restored by amputating the patentee's prerogative of absolute control over the circulation of protected products" and encourages litigants to use Alternative Dispute Resolution methods to settle their disputes. This proposal for effective dispute resolution must please the OAPI Arbitration Centre.

A.J.A.

PORPORTY Aféké Comi

Protection of employees' works under OAPI law

Master's thesis in Basic Private Law, University of Lomé, 2017

The specificity of this study is that it took place during a period of transition between the 1999 law on takeover bids and the 2015 law, which had not yet come into force. The author was faced with the dilemma of choosing between prospective law and positive law. He chose to look in depth at positive law, which has never really been studied in Togolese law despite the age of this legislation. The analysis consisted mainly in seeing whether article 31 of annex VII of the Bangui Agreement of 24 February 1999, which governs literary and artistic property, effectively protects the salaried creator, considered to be the weakest party in the creator-operator relationship. The author began by noting the realism of the OAPI legislator.

At the same time, he criticises the weaknesses of this legislation in his conclusion. He notes that the legislator has not departed from the principle of recognising the employee author's original ownership of copyright, but has instituted a legal transfer of his economic rights to the employer, while prohibiting the alienation of the employee author's moral rights. Thus, despite the legal assignment of economic rights to the employer, the employee author retains his moral rights over the work he has created. However relevant this option may be, it contains weaknesses and approximations that do not entitle the author to protection. Understandably, it is a desire to share the waters of the pre-eminence of the economic prerogatives of *copyright* with those of the intangible force of the moral prerogatives of French copyright. For the author, the 1999 legislation did not resolve all the difficulties inherent in salaried creation, but subtly created another difficulty: that of determining the employer's habitual activity.

This raises the problem of determining the scope, timing and terms of the transfer. This creates legal uncertainty to the detriment of the employee author, who runs the risk of being subject to the employer's discretionary power because the employer is, above all, the sole judge of the economic choice of his company. In addition, it is possible that the employee author, who retains his moral prerogatives despite the transfer of his economic prerogatives to the employer, could hinder the exploitation of the works by the employer, especially as he alone is in a position to determine whether or not his intellectual interests have been affected and the exercise of moral prerogatives is above all discretionary.

Similarly, the untimely exercise of moral rights could lead the employer to seek to invoke the contractual liability of the salaried author. Faced with this conflict between the various prerogatives involved, the author has tried to reconcile the requirements of copyright with the prerogatives of the employer and the economic constraints of the company. Mr Porporty therefore proposes an improvement to the mechanism of legal assignment because of the uncertainties it contains, as well as a framework for the exercise of moral rights so that the employee author cannot, in the name of a misappropriated moral right, compromise the acts

of exploitation of the employer who has invested in creation and whose legitimate ambition is to exploit the works of his employees.

It is absolutely true that the OAPI legislator saw all these problems coming and preferred to bring salaried works into line with salaried inventions under French law. It remains to be seen whether the relevant questions about moral rights will remain when the 2015 legislation is implemented. Having entered the Ecole Nationale de la Magistrature this year after a competitive examination, we hope that Mr Porporty will have the opportunity as a judge to settle disputes and find appropriate solutions to these conflicts between the divergent interests of the company and the employee author in the light of the 2015 Bangui Agreement.

A.J.A.

ALONYO Yawa Senyediva

The risk of confusion in trademark infringement

Master's thesis in fundamental private law, University of Lomé, 2017

By choosing to work on the risk of confusion in trade mark law, Ms ALONYO Yawa Senyediva had in fact chosen to tackle head-on the crucial issue of trade mark infringement. Obviously, since a trade mark is unquestionably a customer right, the distinctive sign plays an essential role in regulating competition. As all property rights are focused on this sign, it is in the field of confusion that most offences are committed. This is precisely what is revealed in Ms Alonyo's dissertation, which she unfortunately chose to write on banking law.

Firstly, it objectively noted a broadening of the likelihood of confusion. Thus, the likelihood of confusion, which was confined exclusively to similarity between signs, now applies even in cases of identity. The likelihood of confusion has thus supplanted the criterion of identity, and cases of identical reproduction are declining or even becoming rare. This is why proof of likelihood of confusion is subject to infringement of the essential function of the trade mark. Secondly, it held that the assessment of the likelihood of confusion is governed by well-defined and established rules. These rules, most of which have been developed by case law, determine the criteria and method for assessing the likelihood of confusion. The criteria, which are very rigid, can be grouped into two categories. On the one hand, there are the so-called objective criteria, which consist of the similarity between the goods or services and between the signs. On the other hand, there is the subjective criterion, which revolves around the agent referring to the likelihood of confusion, also known as the average consumer.

This observation is a reminder that the average consumer, just like the tradesman in patent law or the Internet user in copyright law, is a reference point like any other intellectual property family. As such, they are essential to the assessment of trade mark infringement. However, in OAPI law, the identification of consumers of average attention may depend on regional specificities. The interest of this work lies in having identified this particularity in the assessment of this consumer due to, by way of illustration, the level of literacy of the populations as well as their economic and social level. The author is aware of the difficulties that such an approach may entail, and stresses that "even if this position has been strongly criticised, this innovation in African law, which seeks to distinguish itself from Western conceptions, is to be welcomed". She stresses the probable rapprochement of OAPI law with French law with regard to the so-called global assessment method of the likelihood of confusion, since the different criteria are interdependent, even if it was not so named.

The author concluded her paper with the decisive role played by judges in assessing the likelihood of confusion in trade mark infringement cases, with the risk of this tool, which is malleable at will, being exploited. However, she relies on the wisdom and prudence of the judges, who must play their part in

framing this concept with its undulating contours through a judicious interpretation of the Bangui Agreement and prevent excesses that are prejudicial to the parties. We wish Ms Alonyo every success in her thesis on banking law, and hope that she will return to her first love. It is fortunate that the subject has been taken up by a doctoral student who will be presenting us with the results of his research in the near future.

A.J.A.

KOSSADOUM Cédric

Exceptions to copyright tested by the courts in the OAPI and ARIPO areas

Master 2 thesis in Creative and Digital Law, Université Paris-Saclay, September 2023

This research paper analyses the exceptions to copyright in the OAPI and ARIPO areas as experienced by the courts. Judges in the OAPI and ARIPO areas encounter a number of difficulties in interpreting exceptions to copyright. Among these difficulties, the author notes the absence of a jurisdiction allowing a harmonised and effective interpretation of exceptions within the OAPI Member States.

Furthermore, explains the author, the interpretation of exceptions to copyright sometimes differs depending on whether they are interpreted by the OAPI or ARIPO judge. The author considers that there is a need for a common interpretation of exceptions to copyright in both the OAPI and ARIPO areas, with regard to the African context. For example, as the author points out, *"there would be no point in interpreting exceptions to copyright differently, because the similarity between these two areas is the African context, with its cultural, family and solidarity dimensions, but also the need to give Africans access to knowledge"*. The author has not been able to make use of all the relevant decisions available, but has nonetheless provided some interesting comparative analyses that could be taken further by himself or others.

Y.L.N

HONMINOU Edem Kokouvi

La marque au regard de 1'Accord de Bangui Révisé, Acte du 14 décembre 2015, Mémoire de Master Droit privé fondamental defended, Wednesday 28 December 2022.

Faced with criticism of the trademark under African Intellectual Property Organisation (OAPI) law and the need to comply with the requirements of the agreements on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the OAPI member states revised the Bangui Agreement in 2015. With a view to ensuring greater protection for trademarks against counterfeiting, the RBA broadened the scope of trademarks eligible for protection. In addition to broadening the scope of protection, the SLA provides victims with sufficient evidence to justify any infringement of their trademark.

Whether it's the measures taken at borders or the information retrieval procedure, victims are now in possession of all the information they need to defend their rights; they can claim full compensation for the damage they have suffered and see counterfeiters ordered to pay five times the fine provided for in 1999. All these innovations introduced by the 2015 AB are designed to protect both the trademark and its owner against counterfeiting. However, in an emerging Africa where technology and industry are on the rise, is it not appropriate for OAPI to include tactile, olfactory and gustatory marks on the list of trademarks to be protected?

E.M.A.

SODJI Alexis

Benin customs' contribution to the fight against counterfeiting

Master's thesis in Business Law and Taxation, University of Abomey-Calavi, defended on 11 October 2023

Does customs make an effective contribution to the fight against counterfeiting? That is the question underlying this study. Based on a cross-reading of the legal and organic frameworks, the aim was to assess the contribution made by customs in the fight against counterfeiting, highlighting the concrete actions taken, but also, and above all, pointing out the shortcomings.

Legislators have gradually provided customs with the legal instruments they need to combat counterfeiting. In addition, several national and foreign players are involved in this fight alongside the customs authorities.

Benin Customs is active in the fight against counterfeiting. On its own or under the aegis of the World Customs Organisation (WCO), it has carried out various operations (PANGEA, BIYELA, ACIM, VICE-GRIPS), which have led to the arrest of large quantities of counterfeit medicines and the initiation of appropriate legal proceedings against the perpetrators of this offence.

To improve Benin Customs' contribution to the fight against counterfeiting, its remit needs to be strengthened. More specifically, we would like to see the creation of a directorate dedicated solely to combating counterfeiting.

E.M.A.

▪ UNIVERSITY NEWS

➢ RGPD Day in Lyon

The Association Française des Correspondants à la protection des Données à caractère personnel (AFCDP) organised an RGPD day on 13 September in Lyon, with the aim of giving professionals in the sector an opportunity to discuss the RGPD and the best practices to adopt, based in particular on recent decisions by the CNIL. In addition, the association produces a NEWSLETTER providing news on the regulations, activities and meetings of professionals in the sector.

➢ Security & RGPD Day

At the initiative of Aline MBENOUN-NGOUE, the Institute of Communication of the University of Lyon 2 (ICOM) organised a half-day on RGPD under the theme: Cybersecurity and RGPD compliance on 20 /03/2023.

Aurèlie DUSONCHET, Cybersecurity & RGPD Expert, spoke at the invitation of Aline MBENOUN-NGOUE.

This project was set up for the OPSIE Masters (Organisation and protection of information systems in companies). The aim of this first meeting was to highlight the link between security and the RGPD.

➢ 30 Years of OHADA Law Day

To mark the thirtieth anniversary of OHADA, the Catholic University of Lyon is hosting a symposium on 23 November on the theme of 30 years of application of OHADA uniform business law, under the scientific direction of Prof. Gérard Anou and Dr Louis-Daniel Muka Tshibende.

APIA is proud to note that two of its members, Ms Mbenoun-Ngoue and Mr Falilou Diop, will be chairing sessions.

Arbitration and collective proceedings under OHADA and Moroccan law

Youssouf Adoum Youssouf
Lawyer

The overlap between arbitration and collective proceedings is not a recent problem. Several authors have dealt with it. However, the abundance of litigation on the subject has renewed its importance and accentuated the already rich debate on arbitration and collective proceedings. This can be explained by the fact that it involves reconciling two naturally antagonistic subjects. Bringing together two forms of justice, one private (arbitration) and the other state (collective proceedings), is not such a simple matter[332] . In doing so, the specific features of each procedure must be taken into account on both sides.

In addition to their adversarial nature, arbitration and insolvency proceedings have divergent objectives.

Arbitration, being a form of private justice, is the consecration of contractual freedom, autonomy of wills and binding force, which are sacrosanct principles of contract law. OHADA legislators have deliberately omitted to define arbitration. The Uniform Act on Arbitration Law of November 2017 does not mention any definition of arbitration.

Faced with such a situation, we inevitably turn to the Moroccan legislator, who has enshrined the definition of arbitration in article 1er of the dahir[333] n° 1-22-43 of 23 choual 1444 (24 May 2022) promulgating law 95-17 relating to arbitration and conventional mediation. The said article provides that: "The purpose of arbitration is to have a dispute settled by an arbitral tribunal which receives from the parties the mission of judging by virtue of an arbitration agreement".
Arbitration is the dispute resolution method of choice for those involved in domestic and international trade. Arbitration is becoming a common method of settling disputes arising from commercial contracts[334] .

For some authors, arbitration is as old as humanity itself. It is not just an international phenomenon, but sometimes an intercultural one. Arbitration is thought to have appeared in ancient Greece in the 6th-5th centuries BC. Arbitration is said to have originated at this time. A number of arbitrations took place between Greek cities from the 4th century BC onwards. Very early on, Aristotle distinguished arbitration from state justice: "the arbitrator aims at equity, the judge at law.

[332] Julie Daniel, Nicolas Borga, Arbitrage et procédure collective : de l'art de coordonner les procédures, Recueil Dalloz, 2013, p2891.

[333] In Morocco, a dahir is a decree issued by the King. It is the King's seal affixed to legislative texts.

[334] OSSAGOU Diane Loïca, Arbitrage et procédures collectives, Thesis, Université Toulouse 1 Capitole, 2017, p17.

Arbitration was invented so that equity could be applied". The history of arbitration also dates back to ancient Rome (7th-6th BC) with the "arbitrium liti aestimandae", in which an arbitrator set the amount of compensation to be paid by the guilty party who lost the case. Subsequently, arbitration became commonplace. In the words of Cicero: "Arbitration is the way to avoid completely winning a good case and losing a bad one".

To regard arbitration as the sole preserve of Greco-Roman civilisation is to take a one-sided view of history. The Islamic holy book has already distinguished between the arbitrator (Hakam) and the judge (qadi). The Bible also mentions them[335] .

The recognition of arbitration as an alternative means of settling contractual disputes under Ohada law was established at the outset. The preamble to the Treaty of Port-Louis of 17 October 1993 expressly states the willingness of the States parties to promote arbitration as an instrument for settling contractual disputes[336] . Article 1er of the said treaty states that encouraging recourse to arbitration is one of the objectives of the treaty. Article 2 of the same treaty lists arbitration law among the disciplines that fall within the field of business law. The original treaty therefore devoted an entire title to arbitration.

Notwithstanding this consecration, the notion of arbitration remains relatively exposed by this text. We had to wait a few years for arbitration to be given its own body of law, which expands on the concept. Arbitration, as an alternative dispute resolution method, was strengthened in Ohada law by the Uniform Act on Arbitration Law of 11 March 1999. The latter was revised by the Uniform Act on Arbitration Law (AUA) of 23 November 2017[337] .

On the other hand, the Moroccan arbitration law has undergone several changes. It has gone from being a law linked to the Code of Civil Procedure to an autonomous law. The Code of Civil Procedure of 12 August 1913 devoted a chapter to arbitration. This text established the legal regime for arbitration in the Kingdom. It was amended by the Dahir of 28 September 1974. Act No. 08-05 of 2007 repealing and replacing Chapter VIII of the Code of Civil Procedure is part of the drive to improve the business climate and provide legal certainty for investments. However, although Act 08-05 introduced the first provisions governing international arbitration, it has not been able to protect itself against criticism from investors and professionals[338] . This is the background to Dahir No. 1-22-43 of 23 Shoual 1444 (24 May 2022) promulgating Law 95-17 on arbitration and conventional mediation. This innovative law provides solutions to the much-criticised shortcomings of the former law no. 08-05. The formalities relating to recourse to arbitration by the State, local authorities, public companies and public establishments have been relaxed. From now on, meetings and hearings may be held using new information and communication technologies. This also applies to procedural

335 Charles Jarrosson, La notion d'arbitrage, Paris, LGDJ, 1987, p1 et seq.

336 Preamble to the Treaty on the Harmonisation of Business Law in Africa.

337 Gaston Kenfack Douajni, Droit de l'arbitrage Ohada, ERSUMA, 2010, p1.

338 Abdallah Khial, L'Arbitrage en droit marocain, p1. Article available on the page of the International Court of Mediation and Arbitration. https://www.cimeda.ch/

exchanges, which may be conducted electronically[339] .

Unlike arbitration, collective proceedings, which are governed by rules of public order, seek to centralise disputes in the hands of the state judge, in order to remedy the difficulties faced by companies.

Arbitration and insolvency proceedings are two areas that sometimes overlap in practice. Their treatment requires unprecedented vigilance on the part of both state judges and arbitrators[340] .

This raises two fundamental questions: Don't collective proceedings take precedence over arbitration? Can we speak of a conciliation between the two procedures? In order to answer these questions, we will deal in the first part (I) with the predominance of collective proceedings over arbitration, and in the second part (II) with the resistance of arbitration to collective proceedings.

III- The predominance of collective proceedings over arbitration

Although the positive effect of the arbitration agreement requires the arbitration proceedings to take their course, this should not be a windfall for the parties to avoid the public policy rules of insolvency proceedings.

If no obstacle to the arbitrability of the dispute has been found, the public policy governing insolvency proceedings appears to be the major obstacle to the arbitration procedure. As a result, the public policy governing insolvency proceedings has an influence not only on the conduct of the arbitration proceedings but also on the arbitrator's powers[341] .

In this context, all the rules of public policy specific to insolvency proceedings must be preserved, such as the stay on individual lawsuits and the prohibition on paying prior debts. These rules are binding on the parties and the arbitrators to the extent that their violation leads to the annulment of the arbitral award[342] . Consequently, the arbitrator must ensure compliance with these rules throughout the proceedings. Any negligence on the part of the arbitrator will render the award incompatible with the public policy of collective proceedings[343] .

Indeed, it is essential that there be limits to arbitration proceedings that take place at the same time as the debtor's collective proceedings or that have commenced prior to the opening judgment. As mentioned above, collective proceedings are imperialistic and have an influence on arbitration proceedings(A). In addition, the possibility of compromising subsequent(B) to the opening judgment must not be lost sight of.

C- The influence of the public policy of collective proceedings on arbitration

In principle, there is nothing to prevent an arbitration procedure provided for in an arbitration clause drawn up prior to the opening judgment from being recorded when

[339] Kawtar Jalal, La loi 95-17 relative à l'arbitrage : un propulseur du Maroc comme place de rang de premier choix comme siège d'arbitrage-Avancées et lacunes, La lettre D'ARTEMIS, n° 23-2ème trimestre 2022, p39.

[340] Youssouf Adoum Youssouf, Arbitrage et procédure collective, dissertation, Cadi Ayyad University, Marrakech, 2022, p8.

[341] OSSAGOU Diane Loïca, op.cit, p31.

[342] Youssouf Adoum Youssouf, op.cit, p12.

[343] Thomas Clay, L'articulation harmonieuse de l'arbitrage et des procédures collectives, recueil Dalloz, 2004, p3184.

the dispute arises. In practice, arbitration and insolvency proceedings may overlap. In such cases, the rules governing collective proceedings as set out in the Uniform Act Organising Collective Proceedings for the Settlement of Debts (AUPC) must be complied with. The occurrence of insolvency proceedings is not without effect on arbitration proceedings.

The arbitration procedure is automatically interrupted. Although there is nothing to prevent the arbitrator from retaining his powers and making an award, the arbitration procedure is sometimes disrupted. This disruption is justified by the imperialistic nature of collective proceedings. The arbitrator must comply with this rule. In the name of this principle, the proceedings in progress are suspended. However, we must point out that the suspension of the current proceedings is only temporary.

The time for creditors to declare their claims. Once this stage has elapsed, the proceedings may resume their normal course[344] . It is with this in mind that article 75, paragraph 4 of the Ohada Uniform Act relating to collective proceedings for the settlement of debts provides: "Proceedings in progress shall be interrupted until the creditor pursuing the claim has produced his claim. They shall then be resumed ipso jure, with the liquidator duly summoned, but their sole purpose shall be to establish the claims and fix their amount". This legal position is endorsed by the Common Court of Justice and Arbitration (CCJA)[345] .

In Moroccan law, the Cherif legislator has opted for the same logic as that of the promoter of the Ohada Act, through Article 687 of the Commercial Code. This article states that proceedings are temporarily suspended, and this applies to all pending proceedings. The Moroccan Supreme Court has reinforced this rule of stay of proceedings. In a ruling, the Court of Cassation decided that: "The pronouncement of a court-ordered receivership decision suspends the formalities of execution on the movable and immovable property belonging to the company concerned"[346] .

The stay of individual proceedings is not only a rule of domestic public policy in both legislations, but also a rule of international public policy in collective proceedings. An international arbitration award that is to be enforced in the Ohada zone or in Morocco must comply with this principle.
In addition, arbitrators must ensure compliance with the principle of the prohibition on payment of prior debts, which is also a rule of domestic and international public policy in insolvency proceedings.

With the exception of wage claims, the judgment opening the collective proceedings automatically entails a prohibition on the payment of any claim arising prior to the judgment opening the proceedings[347] . When the arbitration proceedings are resumed and the claim is for the payment of a sum of money, the arbitrator must ensure that the rule of equality of creditors is respected. By virtue of this principle, the only purpose of the current proceedings is to establish claims and determine their amount. This prohibition also applies when insolvency proceedings are commenced prior to arbitration proceedings.

[344] Pierre M. Lecorre, Droit des entreprises en difficulté, 8th edition, Dalloz, p121.
[345] CCJA, 18 May 2017, No 128/2017.
[346] C. cass marocaine, chambre com.04 mars 2009, n° 335, dossier 203 /3/1/2007
[347] Article 690 of the Moroccan Commercial Code.

In the event of collective proceedings, the arbitrator is unable to order the debtor in collective proceedings to pay a sum of money. When a case is referred to arbitration, the award should not require the debtor to pay his previous debt. Instead, the arbitration proceedings will be limited to verifying and assessing the amount of the claim[348] .

An arbitration award that orders the debtor to pay a sum of money in the context of collective proceedings cannot be enforced because it violates the public policy rules governing collective proceedings.

D- The possibility of compromising during insolvency proceedings

While it is less complicated to talk about the arbitration procedure provided for prior to the insolvency proceedings, it is not so easy to talk about the arbitration procedure during the insolvency proceedings. After the commencement of insolvency proceedings, entering into an arbitration agreement is considered a serious act. The initiation of arbitration proceedings poses difficulties where collective proceedings have already been initiated. In principle, it is legally impossible to initiate arbitration proceedings during insolvency proceedings. However, there are a few exceptions to this prohibition.

In most cases, the opening of insolvency proceedings has the effect of altering the debtor's management powers. The prohibition on compromising is based both on legal provisions and on the very nature of the dispute. In Ohada insolvency law, this analysis is based on article 75, paragraph 1 of the AUPC. The provisions of the Moroccan Commercial Code relating to insolvency proceedings also prohibit recourse to arbitration by means of an arbitration agreement[349] .

Even though the provisions of Article 75(1) do not expressly mention arbitration, since arbitration is also a form of justice, it falls within the scope of these provisions. Centralizing disputes in the hands of the state judge seems to be the objective sought by collective proceedings. Giving creditors the opportunity to compromise will damage the cash position and undeniably undermine the equality of creditors[350] . It is in this sense that Professor Philippe Fouchard states that compromising after the opening judgment is not a simple "management operation"[351] .

Some Moroccan legal writers accept that: "If the arbitration agreement is concluded after the collective proceedings have been opened, it is null and void because the said proceedings concern public policy and substantial formalities, the implementation of which has been devolved by modern legislation to the exclusive jurisdiction of the national courts. Moroccan legislation is perfectly in line with this trend, having granted the commercial courts jurisdiction to hear disputes relating to collective proceedings"[352] .In this context, disputes arising from or closely related to collective proceedings may not be submitted to arbitration. As such, disputes relating to the opening of insolvency proceedings, suspect periods, the extension of proceedings to company directors, etc. are not arbitrable.

However, there are some exceptions to this legal prohibition. The legislator has

[348] Ossagou Diane Loïca, op.cit, p235.
[349] Article 686 of the Moroccan Commercial Code.
[350] Thomas Clay, L'arbitre, 1st edition, Dalloz, p175.
[351] Philippe Fouchard, op.cit, p493.
[352] Toumlilt, *op.cit*, p63.

authorised the liquidator to resort to arbitration despite the opening of collective proceedings. This authorisation is subject to the authorisation of the official receiver, and the dispute must be purely contractual in nature.

In this context, the Ohada and Moroccan legislators grant the official receiver the power to authorise the liquidator to compromise in the course of collective proceedings. The possibility of compromising is justified by articles 148 of the AUPC and 594 of the Moroccan Commercial Code.

By making arbitration possible despite the commencement of insolvency proceedings, the legislator aims to encourage the development of arbitration and demonstrate that the use of this alternative dispute resolution method cannot be impaired simply by the commencement of insolvency proceedings.

Finally, the dispute that is the subject of the compromise must be contractual in nature. Consequently, the dispute must have neither its origin nor any connection with the insolvency proceedings. For example, an action against a guarantor[353] may be the subject of an arbitration agreement.

However, the opening of future arbitration proceedings will be affected by the public policy rules of insolvency proceedings. Arbitration proceedings cannot be opened until the claimant creditor has declared its claim[354] .

IV- The resistance of arbitration to collective proceedings

Although subject to the rules of domestic and international public policy, the commencement of insolvency proceedings does not jeopardise the performance of an arbitration agreement for long. The commencement of insolvency proceedings does not in itself make it possible to disregard an arbitration clause entered into prior to the judgment of commencement or to prevent the conclusion of an arbitration agreement during the course of insolvency proceedings. Altering an arbitration agreement that complies with all the conditions for its validity is a fatal blow and a notorious violation of the autonomy of wills. To this end, we will see the persistence of arbitration in the face of collective proceedings(A).

Although recourse to arbitration presupposes that the parties wish to set aside the power of the State judge to hear the dispute, the State judge nevertheless appears when reviewing the arbitration award (B).

C- The persistence of arbitration in the face of insolvency proceedings

Given the clear intention of the parties to use arbitration as a means of settling their dispute, the occurrence of insolvency proceedings cannot be a reason for the debtor to avoid arbitration.

Given that the rules of public policy governing insolvency proceedings are complied with, the arbitration proceedings will be set up simply by the dispute that is the subject of the arbitration agreement. This argument is enshrined in Article 13 of the AUA. For this reason, an arbitration agreement, like any validly established act of

[353] Philippe Fouchard, *op.cit*, p480.

[354] Eric Loquin, *L'arbitrage du commerce international*, 1st edition, Issy-les Moulineaux, Joly édition, 2015, p. 56.

will, must imperatively be applied. By its positive effect, the arbitration agreement requires the parties to have recourse to private justice, i.e. to the arbitral tribunal, to the detriment of State justice[355] .

If the arbitrator retains jurisdiction despite the commencement of insolvency proceedings, the arbitration agreement will normally apply[356] .

While the positive effect of the arbitration agreement requires the parties to have recourse to arbitration, its negative effect excludes the power of the state judge to assess the dispute that is the subject of the arbitration agreement. The commissioning judge, in this case the state judge, declares that he has no jurisdiction and refers the parties to the arbitral tribunal, regardless of whether or not arbitration proceedings have been initiated[357] . It is therefore up to the arbitral tribunal to establish and assess the claim.

It should be emphasised that it is up to the parties to raise the existence of an arbitration agreement. The judge commissioner cannot, in principle, raise his lack of jurisdiction ex officio. In this context, it is advisable for the party hoping for an advantage in the arbitration to raise the existence of an arbitration agreement[358] .

In addition, the official receiver cannot rule on the jurisdiction of the arbitral tribunal. This is the jurisdiction-competence principle, which gives the arbitral tribunal full power to rule on its own jurisdiction and at the same time hear the dispute. This position is enshrined in both Ohada and Moroccan arbitration law.

If we understand the philosophy of the Ohada and Moroccan legislators, as long as the arbitration agreement is not manifestly null and void or manifestly inapplicable, it is not permissible to derogate from this principle.

D- Review of the arbitration award

If the parties, by their decision to resort to arbitration, have excluded the power of the state court to hear the dispute, this power will become apparent when the award made by the arbitral tribunal is reviewed.

This stage enables the national court to assess the effectiveness of the arbitration award with regard to the rules of domestic and international public policy governing insolvency proceedings. An arbitral tribunal wishing to have its award recognised by the national court must comply with the principles prohibiting individual lawsuits and the suspension of payment of prior debts.

In most cases, compliance with the rules of public policy governing insolvency proceedings in an arbitration award is verified through the exequatur procedure and the annulment proceedings.

Firstly, whether under Ohada or Moroccan arbitration law, the award can only be enforced by virtue of an exequatur order[359] .

The exequatur procedure enables the national court to ascertain the existence of an arbitration award and its compliance with the public policy rules governing insolvency proceedings. For this reason, exequatur is granted to any arbitral award made in compliance with the rules of domestic and

[355] Thomas Clay, *Articulation harmonieuse de l'arbitrage et des procédures collectives*, Dalloz, 2004, p. 3184.
[356] Ossagou Diane Loïca*, op.cit,* p173.
[357] Article 13, paragraph 2 of the AUA.
[358] C. cass marocain, ch.com, 09 /07/2008, n°59/3/1/2005, Réf 15834.
[359] Articles 30 of the AUA and 67 of Law 95-17 on arbitration and conventional mediation.

international public policy governing insolvency proceedings.

It goes without saying that the exequatur judge's control is limited. He is not allowed to carry out an in-depth review, to check whether the award was made pursuant to a valid arbitration agreement or to examine the composition of the arbitral tribunal.

While the judge granting the exequatur does not have sufficient means to assess the award in depth, the judge hearing the annulment proceedings does have the prerogatives to examine whether the arbitral tribunal has complied with the coordination between the arbitration and the collective proceedings[360] . The annulment proceedings are a way for the party that lost the case in the arbitral tribunal to erase the exequatur and, by extension, the arbitral award made against it. This remedy is available only in a limited number of cases. The Uniform Act on Arbitration recognises only six cases in which recourse is admissible. Moroccan arbitration law, on the other hand, recognises seven cases in which an action for annulment may be brought.

In insolvency proceedings, an action for annulment may be brought when the arbitral tribunal rules on disputes arising from the insolvency proceedings or which are affected by them. Such disputes cannot be arbitrated.

Epilogue

Although the arrival of collective proceedings has the effect of temporarily altering the progress of the arbitration proceedings, the latter soon take off.

At the end of this fascinating study, we conclude that despite the requirements of the public policy rules of collective proceedings, arbitration and collective proceedings, as described by legal writers as the two strong heads of business law, are reconcilable.

At first glance, it may seem that reconciling the two procedures is virtually impossible, but the results of this work show that it is possible. This difficult reconciliation inevitably involves respecting the fundamentals of each procedure.

This work highlights what must be followed by the arbitrator(s), the creditor(s) and even the defendant and defaulting party, in order to achieve unequivocal conciliation.

Reconciling these two major areas of business law requires great vigilance on the part of the parties. Arbitrators must comply with the domestic and international public policy rules governing insolvency proceedings, and the official receiver must relinquish jurisdiction in the event of an arbitration agreement, thereby demonstrating the parties' willingness to resort to arbitration.

Y.A.Y.

[360] Christophe Seraglini, L'affaire Thalès et le non-usage immodéré de l'exception d'ordre public, Gazette du palais, 2005, n°295, p419.

The CCJA and intellectual property or when litigants get tangled up

CCJA, 22 November 2022, Judgment No. 173/2022 of 24 November 2022

By Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

Messrs FATIME ASSILECK, ABDRAMAN AHMAT and HAROUN ADAM ABAKAR are ordered by the Court of Appeal of Abéché (Chad)[361] to pay Mr MAHAMAT ADAM ABAKAR the sum of one million FCFA as damages.

In order to recover the sum owed to him, Mr Abakar seized the assets of his adversaries held in the books of three banks. Mr AHMAT and Mr ABAKAR applied to the Supreme Court of Chad for a stay of execution of the decision of the Abéché Court of Appeal.

In a decision dated 12 July 2021, the Supreme Court of Chad[362] ordered a stay of execution of the Court of Appeal's decision.
The plaintiff then appealed to the OHADA Common Court of Justice and Arbitration (CCJA), which handed down its decision on 24 November 2022[363] .

This judgment is of threefold interest. Firstly, it concerns the jurisdiction of the CCJA in intellectual property disputes. Secondly, because it illustrates the issue of cohabitation between the CCJA and the supreme courts of the OHADA member states; and thirdly, insofar as it clarifies the application of the Uniform Act on enforcement procedures.

The only issue to be addressed here is the jurisdiction of the CCJA pursuant to Article 14 of the OHADA Treaty. This text provides that *"the Common Court of Justice and Arbitration shall ensure the interpretation and common application of the Treaty as well as of the regulations adopted for its application, uniform acts and decisions"*.
This question of the CCJA's jurisdiction is directly linked to that of the application of OHADA law when the dispute is related to a right governed by OAPI law. It illustrates the need to coordinate jurisdictional and normative powers between OHADA and OAPI[364] .

To contest the CCJA's jurisdiction, the debtor argued that the judgment that gave rise to the enforcement proceedings related to an intellectual property right. This is an erroneous interpretation of Article 14 of the OHADA Treaty.

A distinction needs to be made here. Either the dispute concerns a procedure specific to intellectual property rights governed by the OAPI (seizure for infringement, for example) or an aspect of substantive law provided for by the OAPI corpus, including those supplemented by national texts (mainly copyright law), in which case OHADA law is not applicable. In such cases, the CCJA does not have jurisdiction, as it has consistently pointed out[365] .
Or, as in the case reported here, it is a matter of enforcing a court decision by applying the relevant legislation. In this case, unless there are special rules, the applicable law (including in sixteen of the seventeen OAPI States) is

[361] Ruling no. 001/2021 of 27 April 2021
[362] Ruling no. 74/CS/CJ/SC/2021
[363] Ruling No. 173/2022
[364] L.Y. Ngombé, "Droit OHADA et Droit OAPI : actualité et virtualités d'une concurrence normative", *Mélanges Dorothée Sossa,* Editions du CREDIJ, 2021, pp. 397.
[365] See for example Ngombé, "Les plaideurs insistent, la Cour persiste...et signe, CCJA, 1ère ch.,17 February 2022, pourvoi n°261/2021 *":* *RSPIA* 2023, n°3, p.65.

OHADA law, and more specifically the Uniform Act Organising Simplified Debt Collection Procedures and Enforcement Measures.

Unsurprisingly, therefore, in a decision that can only be approved, the CCJA granted the petitioner's request, pointing out that it had *"consistently held that where the decision of a national court of cassation may have a direct impact on the implementation of the Uniform Acts, it is consequently one of those 'not subject to appeal' handed down by any court of the Contracting States"*. This was indeed the case here, since the dispute, which was the subject of an appeal decision, concerned the attachment of a debt. It does not matter whether the claim originates from an infringement of an intellectual property right[366] .

Y.L.N.

[366] In the same vein, Cour d'appel de Niamey, Niger, Judgment No. 2 of 5 March 2008, *Société Rothmans of Pall Mall Limited v La Société Adil Compagny SA: Cahier de la propriété Intellectuelle,* Volume 26, Number 3, October 2014, p. 786, obs. Ngombé.

- **BEYOND AFRICA**
  - **UNITED STATES/EUROPE**

The work of AIs in the scales of justice or the legal purgatory of "A Recent Entry into Paradise".

United States District Court, District of Columbia. Stephen Thaler v. Shira Perlmutter, Register of Copyrights and Director of the United States Copyright Office, et al, Defendants. Civil Action No. 22-1564 (BAH), August 18, 2023

By Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

An artistic creation entitled "A Recent Entrance to Paradise". (is generated by an Artificial Intelligence. The publisher of the artificial intelligence wanted to register it with the Copyright Office.

In its application for registration, the publisher stated that the author was a creative machine and that the work had been "created autonomously by a computer algorithm running on a computer". It also stated that it was acting as the assignee of the work owned by the artificial intelligence that had autonomously generated the creation.

The application for registration was refused by the Copyright Office on the grounds that the creation in question was not the work of a human being. Faced with this refusal, the publisher, Mr Thaler, unsuccessfully requested a re-examination of the case, confirming that the creation in question was generated by an artificial intelligence. The Copyright Office's decision is, in fact, in line with the guidelines adopted in March 2023[367]

Since this work has been refused copyright protection, the publisher of the artificial intelligence that generated "Une entrée récente au paradis" has decided to take the matter to court.

The case was then brought before the *United States District Court, District of Columbia* (the Court), which had to answer the question of whether a creation generated by artificial intelligence could be protected by copyright.

In a lengthy, reasoned and didactic judgment, the court recalled that copyright has never extended to the point of protecting works generated by new forms of technology operating without human intervention. The court added that one of the foundations of copyright lies in the fact that an author can only be a natural person, a human being.

This American decision may have an echo both in French law and in African countries. It is reminiscent of what René Savatier wrote seventy years ago, when he observed that the subject of copyright can only be a natural person, insofar as the work is "that divine keyboard on which inspiration plays, and which the law protects precisely as an attribute of its personality"[368] . Since artificial intelligence has no personality, it cannot be

[367] *U.S. Copyright Office, Library of Congress, Copyright Registration Gudance: Works Containing, Material Generated by Artificial Intelligence*, March 10, 2023, CFR part 202

[368] R. Savatier, Le droit de l'art et des lettres. Les travaux des muses dans les balances de la justice, LGDJ, 1953, n 146, p.109

the owner of copyright. And in the absence of an author, there is no protectable creation.

In an identical situation, would the application of the laws of African States be different? If we look at the different laws of the African States, an identical solution should impose itself on the judges. For example, in the OAPI area, Article 4 of Annex VII of the Bangui Agreement, which constitutes a minimum normative framework, provides that a work protected by copyright is an original intellectual creation[369]

In the majority of the laws of the Member States, original creation is understood to be the imprint of the author's personality or that which makes it possible to identify the author[370] . It would be futile to look for an imprint of the personality of an artificial intelligence. The personalistic dimension of copyright makes the notion of originality incompatible with that of automated creation[371] .

However, the door remains ajar when a human contribution can be detected in the creation generated by Artificial Intelligence. The question will then be to what extent such an input exists. The question will then be to what extent the *prompts* (instructions) dictated to the artificial intelligence have been decisive[372] .

The "Une récente entrée au Paradis" case illustrates the difficulty there would be in admitting, even under the Copyright system (as adopted in English-speaking African countries), the protection of a creation generated by artificial intelligence. Indeed, the requirement of originality would not be met in the ARIPO countries, for example, which apply the criteria of *skill, labour and effort.* When faced with a creation generated by artificial intelligence, it seems difficult to consider that there is a creative effort on the part of an author (which by definition would not exist).

In any event, as the Court pointed out in this case, the creation must come from an individual, a physical person, a being of flesh and blood. Only an extension of the notion of author to automated systems could open the door of copyright to creations generated by artificial intelligences. In the case in point, "Une entrée récente au paradis", rejected by the Copyright Office, had no chance of success in the scales of justice.

Legal provisions, through the voice of judges, have confined this creation to what resembles a legal purgatory... pending an entry, no doubt a long way off, into the Paradise... of copyright.

Y.L.N.

[369] Bangui Agreement, Annex VII, Article 4

[370] Y.L. Ngombé, *Droit(s) africain(s) de la propriété littéraire et artistique,* PUAM 2022, n°58

[371] A. Lucas, A. Lucas-Schloetter and C. Bernault, *Traité de la propriété littéraire et artistique,* 5ème edition, LexisNexis, 2017, n°59

[372] For example, is Fabio Comparelli the author of the history of art told by the Artificial Intelligence to which he has given instructions?

A tax haven is not necessarily a digital haven

The case leclrec.com, Association des Centres Distributeurs E. Leclerc - ACD Lec, v. W S, WIS INC Case no. D2023-2315, WIPO Arbitration and Mediation Center, 15 September 2023

By Yvon Laurier Ngombé,
Lawyer, Doctor of Law
Lecturer
Chairman of APIA

In September 2023, the WIPO Mediation and Arbitration Center handed down some interesting decisions relating to typosquatting cases involving well-known trademarks. This was the case, for example, with the domain name *Lambroghini*, which infringed the rights of the company that owns the famous *Lamborghini trademark*.

Ten days after ordering the transfer of the domain name *Lambroghini* to the Lamborghini company[373] , the Centre d'arbitrage et de Médiation has handed down a decision following a complaint from the Association des Centres Distributeurs E. Leclerc.

The complaint stems from the reservation of the domain name *leclrec.com* by a company based in the Cayman Islands, a territory reputed to be a tax haven. The complainant considers that this domain name creates confusion with the *Leclerc* brand, over which it has legitimacy. In view of what is nothing less than typosquatting, the complainant successfully requested the transfer of the disputed domain name.

The Administrative Panel of the WIPO Arbitration and Mediation Centre based its decision on the fact that the disputed domain name is "confusingly similar" to the LECLERC trademark in which the complainant has rights. The inversion of the letters "e" and "r", according to the panel, is insufficient to dispel this confusion.

The Panel then found that the respondent (which did not send any observations to the Panel) has no rights or legitimate interests in the disputed domain name and that it had not proved that it was authorised by the trade mark owner to make any use of it.

Finally, the Panel considers that the documents submitted by the Complainant prove that the Respondent was aware of the LECLERC trademark at the time it reserved the disputed domain name, and that it acted in bad faith. The Complainant notes that the Respondent intentionally attempted to attract, for commercial purposes, Internet users to its website or any other online site, by creating a likelihood of confusion with the LECLERC trademark.

Faced with this clear act of typosquatting, the defendant, although based in a tax haven, could only have the UDRP[374] rules for resolving domain name disputes applied to it. So some tax havens are a long way from tax law, but no way of escaping digital law.

Y.L.N.

---

[373] Automobili Lamborghini S.p.A. v. Jinsoo, Yoon Case No. D2023-2655, WIPO Arbitration and Mediation Center, 5 September 2023

[374] Uniform Domain Name Dispute Resolution Policy. These rules are those applied by the WIPO Mediation and Arbitration Centre. Some African States' Naming Charters refer to them (see Ngombé, "Propriétés intellectuelles et commerce électronique dans l'espace OAPI et dans l'espace OHADA", *Recueil Penant* April-June 2021, p. 277).

Trademark originality: when the courts play *false friends off against each other*

General Court, Case T-324/22, Ecoalf Recycled Fabrics v. EUIPO, Decision of 13 September 2023

By Christian Kpolo
Member of the Paris Bar
Doctor of Law - Associate Researcher
University of Lorraine and University of Abidjan

On 15 December 2020 Ecoalf Recycled Fabrics, SL (the applicant) applied to the EUIPO for registration of the word sign BECAUSE THERE IS NO PLANET B as a European Union trade mark. The mark applied for designated goods in Classes 3, 16, 18 and 21.

By decision of 24 September 2021, the EUIPO examiner rejected the application for registration of that trade mark on the basis of Article 7(1)(b) of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark.

On 18 November 2021, the applicant lodged an appeal with the EUIPO against the examiner's decision. In the contested decision, the Board of Appeal dismissed the appeal on the ground that the trade mark applied for was devoid of distinctive character. In particular, it held that the mark would be perceived by the relevant public as a slogan of a purely promotional nature, and not as an indication of the commercial origin of the goods in question.

In its decision of 13 September 2023, the EU Court upheld the rejection of the trade mark application on the basis that, since the expression 'because there is no planet B' has a clear meaning and complies with the rules of English grammar and, moreover, is well known to be used in the context of the fight against climate change, it does not possess any originality or salience, does not require a minimum effort of interpretation, and does not trigger a cognitive process in the relevant public. In addition, the Court of First Instance - Board of Appeal correctly considered that the trade mark applied for will be perceived by the relevant public as a mere promotional slogan.

The Court's response is not surprising in itself, but what is intriguing is that, in reaching its decision, the court followed the argument that *"the expression 'planet B' lacks originality". This is* enough to make intellectual property law purists wince, for whom the term originality should only be used strictly when analysing the criteria for protecting a work of the mind (under copyright law)[375] . Moreover, it would be unfortunate to confine oneself to the formula used by the court, because on the other hand, the originality to which it refers should not be considered in the sense of copyright law but rather ... in the sense of everyday language, namely *"Character of a person whose behaviour deviates from common usage; singularity, oddity".*[376]

An original approach, isn't it?

Ch.K.

[375] S. Hans, *L'originalité au sens du droit d'auteur: contribution à l'étude de la notion*, thesis, Université Paris 1 Sorbonne, 1991.

[376] V° "Originality", Dictionnaire de l'Académie française, 9e edition.

Clarification by the *Cour de cassation* of the deadline for filing a second-generation divisional application

Court of Cassation, Commercial Division, 30 August 2023, no. 20-15.480

By Christian Kpolo
Member of the Paris Bar
Doctor of Law - Associate Researcher
University of Lorraine and University of Abidjan

In a recent case brought before the French Supreme Court on 30 August, Kubota Corporation found itself at the heart of a complex issue relating to its patent applications. To understand the context, let's look at the chronology of these applications. It all began with the initial filing of a patent application by Kubota Corporation. After seven years, the company filed its first divisional application. Later, in 2018, it submitted a second divisional application. However, the latter application was rejected by the Director General of the Institut national de la propriété industrielle (INPI).

The ensuing dispute concerned the deadline by which a patent applicant is entitled to submit a new divisional application. To resolve this delicate issue, the Cour de cassation referred to Article L. 612-4 of the French Intellectual Property Code. This article states that a patent application may only relate to one invention or a group of closely related inventions, thus forming a single general inventive concept. Any application that does not comply with this provision must be divided within a prescribed period. Divisional applications benefit from the filing date of the initial application, as well as the priority date, where applicable.

The Court of Cassation's response was based on an in-depth analysis of European practice in relation to divisional applications. It noted that the guidelines in force at the European Patent Office (EPO) since 1 November 2018 define the term "earlier application" as referring to the closest application on which the divisional application is based. This terminology has replaced that of "original application" which previously appeared in Article 76 of the Munich Convention on the Grant of European Patents.

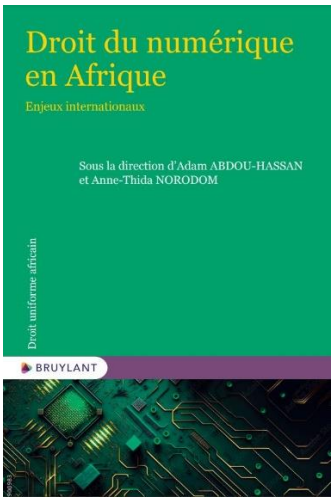
Prior to 2011, the INPI accepted the filing of a new divisional application until the date of payment of the costs of granting and printing the patent specification resulting from the first divisional application. The Court of Cassation therefore overturned the decision of the Court of Appeal, which had rejected the patent applicant's appeal. It pointed out that in Article R 612-34 of the French Intellectual Property Code, the term "patent" refers to the expression "initial patent application" in the same sentence.

This provision refers to the first patent application before any division and thus sets a filing date applicable to all subsequent divisional applications, without the possibility of a different interpretation. Consequently, the second divisional application submitted by the company after payment of the costs of granting and printing the patent specification was deemed inadmissible.

Ch.K.

BIBLIOGRAPHY

Publications



The first book on digital law in Africa was published in September 2023 by Bruylant, edited by Adam ABDOU-HASSAN, doctor of public law, and Anne-Thida NORODOM, professor of public law at Université Paris Cité.

The book brings together contributions from academics and practitioners, in French and English, on international organisations involved in Internet governance, state transformations, cybersecurity, digital taxation, data protection, and access to the Internet and its content. There are also articles on economic development, space activities, education and culture, and human rights.

This book on international law is undoubtedly a welcome addition to the global economy.

I.R.

Five years of research into business law in the face of digitalisation, in collaboration between the Institut François Gény, the Confluence Sciences & Humanités research unit, the Transversales Humanités research unit, the Transversales laboratory and the Centre de recherches juridiques de l'Université Grenoble Alpes, has resulted in the publication of a collective work *Droit des affaires et intelligence artificielle*, edited by Iony Randrianirina (UGA), Michel Cannarsa (UCLy), Jean-Luc Piotraut (Université de Lorraine) and Alexandre Quiquerez (Université Lumière Lyon 2).

Contributions from academics and practitioners cover blockchain, *smart contracts*, the DSA and DMA directives, AI-generated products, new banking practices, cybercrime, start-ups, financial law and international arbitration.

I.R.

Baudin L., *Cyberattaques et droit international public : de la négociation entre états à l'intégration des acteurs privés pour parvenir à la cyberpaix*, Coll. " Logiques Juridiques ", L'Harmattan, 2023, 418 pages

Brandre L., *Protection des données à caractère personnel en côte d'ivoire : comprendre les textes de loi*, Éd. Le livre en papier, 2023

Brandre L., *Protection des données à caractère personnel en côte d'ivoire : les bases légales en droit positif ivoirien*, Éd. Le livre en papier, 2023

Cluzel-Métayer L. et Sée A. (ss dir.), *Eléments de droit public du numérique*, Coll. " Logiques Juridiques ", L'Harmattan, 2023, 176 pages

Demay S., *La charge de travail à l'ère du numérique : Réflexion sur la santé au travail, ?* coll. "Le Droit aujourd'hui", L'Harmattan, 2023, 306 pages

Fotso E. D., *Droit des affaires en Afrique - Recueil de jurisprudence 2022 : Cour commune de Justice et d'Arbitrage (CCJA-OHADA), cours d'appel, tribunaux de commerce*, LegiAfrica, 2023, 478 pages

Kianguebeni U. K., *Droits linguistiques et patrimoine immatériel au Congo*, Edilivre, 2019, 218 pages

Konaté M. K., *Contentieux du droit communautaire africain : Le juge national et le contentieux des normes communautaires de l'UEMOA*, Coll. "Harmattan Mali", L'Harmattan, 2023, 140 pages

Kutnjem A. M., *Introduction générale au droit camerounais du sport*, Coll. "Etudes africaines", L'Harmattan, 2023, 356 pages

Mpakam R. E., *Des brevets en droit congolais : Recherche d'informations et systèmes juridiques de leur protection,* Éd. Academia, 2023, 256 pages

Mvomo Ela P., *La protection de la culture au Cameroun : Enjeux et perspectives,* L'Harmattan, 2023, 232 pages

Sall A., *Singularités juridiques africaines: Ce que l'Afrique apporte au droit*, L'Harmattan, 2023, 322 pages

Semo Miekountima V. F. M., *Le juge et la cybercriminalité au Congo*, Coll. "JAMA", L'Harmattan, 2023, 224 pages

Traoré M., *Le règlement des litiges commerciaux en Afrique de l'Ouest*, Coll. "Etudes africaines", L'Harmattan, 2023, 368 pages

Articles and case law reviews

Johnson-Ansah A., "Commerce électronique et épuisement du droit des marques dans l'espace OAPI", *Penant* 2023, n° 922, p. 167

Ngombé Y. L. (under the dir. of), Ch. Kpolo, J.-P. Koso Omambondi, R. Mabouana, "Contentieux des signes distinctifs et de la concurrence déloyale en Afrique", *Propr. Industr.* 2023, n°6, study 7.

Savom Ambara R., "Étude comparée des mesures probatoires de la contrefaçon des œuvres de l'esprit dans l'accord de Bangui de 2015 et la loi n°2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins", *RFPI* n°17, October 2023, p. 31.

Sawadogo F. M., "La construction d'un modèle de droit d'auteur pour l'OAPI : analyse de la technique légistique", *Penant* 2023, No. 922, p. 255.

I.R., A.N., Y.L.Y., F.K. & Ch.K.

Semi-Annual Review of the Intellectual Property in Africa

Journal of the Association for the Promotion of Intellectual Property in Africa (APIA)

Association registered under n° W912014459

www.apia-asso.org

Semi-Annual Review of the Intellectual Property in Africa

PROVISIONAL SCHEDULE OF APIA 2023 ACTIVITIES

Podcast | Le Balafon	*March 2023*
BSPIA no. 3	*April 2023*
Podcast | Le Balafon	
Podcast | Le Balafon	*May |June |July | August 2023*
Scientific Research Day	*September 2023*
RSPIA no. 4	*October 2023*
APIA's Palaver Tree	*December 2023*
Annual General Meeting	*December 2023*

ISSN 3000-0025