# Réunion conjointe AFRALO-AfrICANN
# Réunion Virtuelle de l'ICANN 72
# Mardi 26 octobre (GMT)

---

## Déclaration

---

## SUJET : SÉCURITÉ DES DONNÉES

---

Nous, membres de la Communauté Africaine de l'ICANN participant à la Réunion de l'Assemblée Générale virtuelle de l'ICANN 72, ayant assisté à la réunion conjointe **AFRALO-AfrICANN**, avons discuté de la sécurité des données en tant que sujet important pour AFRALO.

Par la présente, nous présentons la position de l'Afrique concernant la sécurité des données au sein de l'ICANN. Cette discussion a été recommandée par la majorité des membres d'AFRALO suite à un appel sur la liste de diffusion interne pour des propositions de sujets à discuter durant la réunion ICANN72. A cet effet, un webinaire de renforcement des capacités a été organisé par AFRALO sur ce sujet. Celui-ci a été facilité par le personnel de l'ICANN.

La sécurité des données est un ensemble de processus et de pratiques conçus pour protéger les écosystèmes critiques des technologies de l'information (TI). La sécurité des données et la confidentialité sont les défis les plus importants de l'ère de l'information. Des exemples de ce type de défis incluent les attaques de **"Ransomwares"** que nous avons constatées à la une des journaux africains. Le mois dernier, le ministère sud-africain de la justice a été confronté à une attaque massive de Ransomware.

La communauté africaine estime explicitement que le sujet de la sécurité des données doit être une priorité l'une des principales priorités de l'agenda de toutes les parties prenantes.

Dans le contexte de l'ICANN, la sécurité des données revêt des multiples facettes, elle inclut la sécurité et l'intégrité du système de nommage sur Internet, la sécurité des données des titulaires de nom de domaine et la sécurité des données des utilisateurs, eu égard au système de noms de domaine (DNS). La communauté de l'ICANN traite ces différents aspects de la sécurité des données par le biais de pratiques et de politiques, que la communauté AFRLO-AfrICANN soutient pleinement.

Afin de garantir la sécurité et la stabilité d'Internet, il est essentiel d'assurer la sécurité et l'intégrité des données du DNS. Le DNS peut être utilisé en tant qu'outil permettant de

commettre des actes malveillants qui menacent la sécurité des données des internautes, prennent pour cible bon nombre d'entre eux et réduisent la confiance qu'ils ont en Internet.

Dans la mesure où la sécurité des données du DNS a un impact direct sur la sécurité des internautes, elle a aussi un impact direct sur les activités des registres et des bureaux d'enregistrement. De ce fait, la prévention et l'atténuation de toutes les formes d'utilisation malveillante du DNS qui modifient les données du DNS ou les utilisent afin de cibler des millions d'individus doivent être une priorité absolue de l'ensemble de la communauté de l'ICANN. Parmi les techniques visant à protéger l'intégrité des données du DNS, on peut citer le déploiement des DNSSEC, qui renforce la sécurité du DNS à l'aide de signatures numériques. Mais les DNSSEC ne sont pas déployées à grande échelle. Les méthodes de résolution, telles que les protocoles DNS sur HTTPS (DoH) et DNS sur TLS, tous deux fondés sur la sécurité de la couche transport et le chiffrement, renforcent également la confidentialité et la sécurité des utilisateurs. En outre, les politiques de l'ICANN sont aussi affectées par la question de la sécurité des données, par exemple la nouvelle série de gTLD, les services d'annuaire de données d'enregistrement anciennement connus sous le nom de WHOIS, et les politiques de transfert des noms de domaine. Le lancement d'une nouvelle série de gTLD sans résoudre les difficultés liées à la sécurité des données entraînerait une augmentation des actes malveillants touchant l'ensemble de la communauté Internet Pour résoudre le problème de la sécurité des données des titulaires et suite à la promulgation du règlement général européen sur la protection des données (RGPD), la communauté a développé une nouvelle politique pour les données d'enregistrement des gTLD. Cependant, malgré le fait que les politiques protègent les données du titulaire, elles ne permettent pas efficacement la divulgation des données dans le but de protéger la communauté Internet. De plus, la sécurité des données du titulaire reste une préoccupation de la politique de transfert de nom de domaine, notamment en ce qui concerne le code d'authentification envoyé au titulaire.

Après avoir analysé les pratiques en matière de sécurité des noms de domaine, nous avons noté que le verrouillage des registres est actuellement utilisé afin d'empêcher le détournement de noms de domaine et les modifications non autorisées du DNS. Sans ce verrouillage, les attaques pourraient entraîner la clôture d'un site web ou rediriger les utilisateurs vers du contenu malveillant. Il se peut que de nombreux domaines soient actuellement déverrouillés étant donné que tous les bureaux d'enregistrement ne proposent pas ce service.

La communauté AFRALO-AfrICANN recommande par les présentes d'obliger les bureaux d'enregistrement à proposer des services de verrouillage de domaine en tant que mesure de sécurité des données pour les noms de domaine. Une politique de verrouillage des registres pourrait prévenir les transferts de domaines initiés par les bureaux d'enregistrement.

C’est à ce titre qu’AFRALO-AfrICANN recommande à l'ICANN et à la communauté les actions suivantes :

- Encourager le déploiement de DNSSEC et d'autres bonnes pratiques de sécurité pour garantir l'intégrité et la sécurité des données DNS,
- Résoudre les problèmes liés à la sécurité des données et aux abus DNS avant d'aller de l'avant avec un nouveau cycle de gTLD,
- Considérer la prévention et l'atténuation de toutes les formes d'abus du DNS comme une priorité élevée pour l'ensemble de la communauté de l'ICANN,
- Trouver le juste équilibre entre la confidentialité et la protection des données des déclarants et la protection des données des utilisateurs finaux d'Internet,
- Exiger des bureaux d'enregistrement qu'ils proposent des services de verrouillage de domaine comme mesure de sécurité des données pour les noms de domaine.

En outre, la communauté AFRALO-AfrICANN exhorte les utilisateurs finaux d'Internet à prendre des mesures de protection de leurs données à travers des pratiques qui incluent :

- Utiliser des outils de protection des données de messagerie et des outils de protection contre la perte de données pour détecter toute activité suspecte.
- Protéger les données stockées en les rendant inutilisables et illisibles, cela permettrait de garder les informations en sécurité en cas de vol de données.
- Protéger les données lorsqu'elles celles-ci sont distribuées via une protection par mot de passe et un cryptage, ainsi que la distribution via des canaux sécurisés.
- Minimiser les appareils contenant des données en autorisant l'accès aux fichiers uniquement sur des plates-formes sécurisées. Utiliser les données uniquement pour les tâches qui nécessitent les données et accorder un accès sélectif.
- Améliorer la surveillance de l'utilisation des données grâce au tatouage numérique et à la vérification du mouvement des données sur le réseau.

Équipe de rédaction :


1. Gabriel Bombambo Boseko, gbombambo@gmail.com
2. Raymond Mamattah, mamattah.raymond@gmail.com
3. Tijani BEN JEMAA, tijani.benjemaa@topnet.tn
4. Hadia EL Miniawi, Hadia@tra.gov.eg (Pen-holder)
5. Mary Uduma, mnuduma@yahoo.com
6. Emmanuel K Asare , kaku.asare@gmail.com
7. Joshua Ayayi, ayayijoshua@gmail.com
8. DANIEL Nanghaka , dndannang@gmail.com (Pen-holder)
9. Remmy Nweke, remmyn@gmail.com
10. Musa Stephen Honlue, stephen.honlue@afrinic.net
11. Bamba Vassindou , vassb2017@gmail.com
12. Arthur Carindal, arthur@afrinic.net
13. Michel Tchonang Linze, capdasiege@gmail.com
14. Sarah T. Kiden, skiden@gmail.com
15. Bright Kuleke, brightedujih@gmail.com
16. Dave Kissoondoyal, dkissoondoyal@gmail.com
17. Olévié Kouami, olivierkouami@gmail.com
18. Bram Fudzulani, beatblam@hotmail.com
19. Brahim Ousmane, braoust@gmail.com
20. Fanny Saliou, salyoufanny@gmail.com
21. Sarata Omane, somane@egigfa.org
22. Robert Nkambwe, rnkambwe@yahoo.com
23. Fatimata Seye Syll, fsylla@gmail.com
24. Aziz Hilali hilaliaziz@yahoo.fr