# Réunion conjointe AFRALO/AfrICANN
# Réunion virtuelle de l'ICANN72

**Mardi 26 octobre (UTC)**

---

## Déclaration

---

# THÈME : SÉCURITÉ DES DONNÉES

---

Nous, membres de la communauté africaine de l'ICANN participant à l'AGM virtuelle de l'ICANN72 et assistant à la réunion conjointe AFRALO/AfrICANN, avons discuté de la sécurité des données, question importante pour l'AFRALO. Nous présentons par les présentes la position de l'Afrique en matière de sécurité des données au sein de l'ICANN. La discussion a été initiée par la majorité des membres de l'AFRALO suite à une demande formulée sur la liste de diffusion de l'AFRALO et visant à dégager des sujets de discussion pour l'ICANN72. Nous avons ensuite organisé un séminaire web de renforcement des capacités sur la sécurité des données qui a été animé par le personnel de l'ICANN.

La sécurité des données désigne un ensemble de processus et pratiques visant à protéger les principaux écosystèmes des technologies de l'information (IT). La sécurité des données et la confidentialité constituent les plus grands défis de cette ère de l'information. Parmi ces défis, on peut citer les attaques par rançongiciels qui ont fait les gros titres de la presse africaine. Pas plus tard que le mois dernier, le ministère de la Justice du gouvernement sud-africain a été confronté à une attaque par rançonlogiciel de grande ampleur. La communauté africaine a clairement fait de la question de la sécurité des données l'une des principales priorités de l'agenda de l'ensemble des parties prenantes.

Dans le cadre de l'ICANN, la sécurité des données revêt de multiples aspects. Elle inclut la sécurité et l'intégrité du système de nommage sur Internet, la sécurité des données des titulaires de noms de domaine et la sécurité des données d'utilisateurs eu égard au système des noms de domaine (DNS). La communauté de l'ICANN traite ces différents aspects de la sécurité des données via des pratiques et politiques auxquelles la communauté de l'AfrICANN apporte tout son soutien.

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.

Afin de régler la question de la sécurité des données des titulaires de noms de domaine et suite à l'adoption du règlement général sur la protection des données (RGPD), la communauté a élaboré une nouvelle politique pour les données d'enregistrement des gTLD. Pourtant, même si la politique protège les données des titulaires de noms de domaine, elle ne permet pas d'assurer une divulgation satisfaisante des données à des fins de protection de la communauté Internet. De plus, la sécurité des données des titulaires de noms de domaine reste problématique eu égard à la politique de transfert des noms de domaine, notamment concernant le code d'authentification envoyé aux titulaires de noms de domaine.

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. L'AFRALO 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.

À cette fin, l'AFRALO recommande à l'ICANN et à la communauté ce qui suit :

- Encourager le déploiement des DNSSEC et autres bonnes pratiques de sécurité afin de garantir l'intégrité et la sécurité des données du DNS
- Résoudre les problèmes liés à la sécurité des données et à l'utilisation malveillante du DNS avant de lancer une série de nouveaux gTLD
- Faire de la prévention et de l'atténuation de toutes les formes d'utilisation malveillante du DNS une priorité absolue pour l'ensemble de la communauté de l'ICANN
- Trouver le juste équilibre entre la confidentialité et la protection des données des titulaires de noms de domaine et la protection des données des internautes
- 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.

En outre, la communauté de l'AFRALO exhorte les internautes à prendre des mesures visant à protéger leurs données en ayant recours, entre autres, aux pratiques suivantes :

- Utiliser des outils de protection des données de messagerie et des outils de protection contre la perte de données afin de détecter toute activité suspecte.
- Protéger les données stockées en les rendant inutilisables et illisibles, ce qui permettrait d'assurer la sécurité des informations en cas de vol de données.
- Protéger les données lors de leur diffusion via une protection par mot de passe et le chiffrement, et en les diffusant par le biais de canaux sécurisés.
- Réduire au minimum le nombre de dispositifs contenant des données en n'autorisant l'accès aux fichiers uniquement sur des plates-formes sécurisées. Utiliser des données uniquement pour des tâches exigeant de telles données, et accorder un accès sélectif.
- Renforcer la surveillance de l'utilisation des données à l'aide du tatouage numérique et du contrôle des mouvements de 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 (scribe)
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 (scribe)
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, brighteduji h@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