Les dix principaux termes fondamentaux pour les journalistes couvrant les droits de l'Internet

Présenté par African Internet Rights Alliance (AIRA)

1. **Perturbations du réseau (arrêts, pannes de courant, anti-démarreurs):** il s'agit de la perturbation des communications électroniques sur un réseau, les rendant inaccessibles ou effectivement inutilisables pour une population spécifique ou dans un endroit particulier[1]. Les perturbations du réseau peuvent être intentionnelles ou non et / ou affecter une partie ou la totalité des services, les rendant inaccessibles ou effectivement inutilisables souvent pour exercer un contrôle sur le flux d'informations[2]. Cela se produit lorsqu'un acteur (généralement un gouvernement), perturber intentionnellement Internet ou des applications mobiles (telles que WhatsApp ou Telegram) pour contrôler ce que les gens disent en ligne[3] [4]

2. **Surveillance et traçage:** cette notion fait référence à la surveillance de l'activité numérique et des données stockées ou transmises sur des réseaux tels qu'Internet et les communications mobiles. La surveillance et le traçage sont souvent effectués secrètement et peuvent être effectués par des gouvernements[5], des entreprises, des groupes criminels ou même des individus[6]. Ils peuvent être légaux ou non et exiger ou non l'autorisation d'un tribunal ou d'autres agences gouvernementales indépendantes. Lorsqu'une telle surveillance est exercée abusivement, en plus de la violation de la vie privée, il s'établit une relation directe entre la surveillance et le suivi et la liberté d'expression. Si la surveillance ne conduit pas directement à la censure, la perception de la surveillance peut conduire à l'autocensure[7].

3. **Violation de données:** il s'agit de la divulgation intentionnelle ou non intentionnelle d'informations sécurisées ou privées et confidentielles à partir d'un système à l'insu ou sans l'autorisation du propriétaire du système[8].

4. **Protection des données:** La protection des données (confidentialité des données ou confidentialité des informations) est le processus de protection des données contre la corruption, la compromission ou la perte[9]. L'importance de la protection des données augmente à mesure que la quantité de données créées et stockées continue d'augmenter à un rythme sans précédent[10]. Lorsque des données sont collectées, il est essentiel que des garanties soient mises en place pour garantir que l'utilisation des données est conforme aux normes des droits de l'homme. Se prémunir contre les abus qui peuvent survenir lorsque des données sont stockées par des organisations, des entreprises ou le gouvernement nécessite des systèmes et des garanties[11] [12].

5. **Responsabilité des intermédiaires:** Un intermédiaire est un fournisseur de services Internet, qui fournit à ses utilisateurs une plate-forme pour télécharger et partager tous les types de contenu, allant du texte aux vidéos[13]. Certains des exemples les plus

---

1 Disconnected Report 2018. Initiative de Global Network.

2 Étude de cas: Cameroun: 93 jours d'arrêt d'Internet. Paradigm Initiative (PIN).

3 Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa. CIPESA.

4 Building trust between the state and citizens: A Policy Brief on Internet shutdowns and elections in Kenya 2017. KICTANet.

5 Digital Rights in Africa Report 2019. Paradigm Initiative (PIN).

6 Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy. CIPESA.

7 Trends in transition from classical censorship to Internet censorship: selected country overviews. IFLA.

8 Definition of "data breach". TechTarget.

9 ARTICLE 19 Data Protection Policy. ARTICLE 19.

10 The Data Protection Act as a tool for permitting innovation and consumer safety in Kenya's digital finance market. CIPIT.

11 Policy Brief: Tanzania's EPOCA and Cybercrimes Laws Offer No Protection for Citizen's Data. Paradigm Initiative (PIN).

12 Data protection in Kenya: Policy Brief examining the current state of data protection in Kenya. KICTANet.

13 Internet intermediaries: The dilemma of liability in Africa. APC.

populaires d'intermédiaires sont Facebook, YouTube, Twitter, WordPress et Blogspot. Le concept de responsabilité intermédiaire lui-même repose sur des incitations économiques. Si les individus sont incités à dire ce qu'ils veulent dire et à faire des efforts pour s'assurer qu'il est correctement diffusé, un intermédiaire n'a pas une telle incitation. Ainsi, d'une part, l'individu fera tout son possible pour s'assurer que ce qu'il dit est entendu, peut-être même au péril de sa vie. Mais d'un autre côté, les intermédiaires ne sont généralement pas incités à promouvoir la liberté d'expression de leurs abonnés et utilisateurs[14] [15].

6. **Fake News (fausses informations):** Les fausses nouvelles sont un type de journalisme ou de propagande jaune qui consistent en des informations délibérément fausses ou trompeuses diffusées via les médias traditionnels imprimés et télévisés ou en ligne. Les fausses nouvelles sont écrites et publiées dans l'intention d'induire en erreur afin de nuire à une agence, une entité ou une personne, et / ou à gagner financièrement ou politiquement. Les créateurs de fausses nouvelles utilisent souvent des titres sensationnalistes, malhonnêtes ou carrément fabriqués pour augmenter le lectorat, le partage en ligne ou les revenus du trafic Internet[16].

7. **Sécurité numérique:** la sécurité numérique est la protection des identités et des actifs en ligne[17]. Les criminels trouvent de nouvelles façons de fonctionner et de voler des informations aux utilisateurs numériques pour leur propre gain personnel. La sécurité numérique est un terme général qui comprend les outils utilisés pour sécuriser les appareils, les communications et les données dans le monde en ligne et mobile.

8. **Cybercriminalité:** également appelée criminalité informatique, la cybercriminalité est l'utilisation d'un ordinateur comme instrument à d'autres fins illégales, telles que la fraude, le trafic de pornographie enfantine et de propriété intellectuelle, le vol d'identité ou la violation de la vie privée[18]. La cybercriminalité, en particulier via Internet, a pris de l'importance à mesure que l'ordinateur est devenu un élément central de commerce, de divertissement et de gouvernement.

9. **Accès à l'information en ligne:** L'accès à l'information en ligne est la liberté ou la capacité d'identifier, d'obtenir et d'utiliser efficacement des données ou des informations. Le droit à l'information permet au public d'accéder aux informations détenues par les autorités publiques ou par des autorités privées exerçant des fonctions publiques. La liberté d'information implique également l'accès à l'information dont une personne a besoin pour jouir de ses droits humains[19]. Il le fait de deux manières: les pouvoirs publics sont tenus de publier certaines informations sur leurs activités; et les membres du public ont le droit de demander des informations aux autorités publiques. Le droit à l'information est essentiel pour instaurer la confiance entre les gouvernements et le public[20].

10. **Liberté d'expression en ligne:** Il s'agit du droit de s'exprimer en ligne et d'accéder aux informations, aux opinions et aux expressions d'autrui. Cela comprend les discours politiques, les opinions religieuses, les opinions et les expressions qui sont accueillies favorablement ou considérées comme inoffensives, mais aussi celles qui peuvent offenser, choquer ou déranger les autres[21]. Dès le début, la liberté d'expression est un droit fondamental qui n'est pas seulement exercé hors ligne, mais également en ligne via Internet et via d'autres technologies numériques habilitantes. Dans l'exercice de la liberté d'expression, il convient de tenir dûment compte des restrictions strictes énoncées dans le droit international des droits de l'homme, ainsi que d'autres droits qui se renforcent mutuellement, tels que le droit à la vie privée. Les organisations, les entreprises et les gouvernements doivent respecter la liberté d'expression en ligne en offrant un environnement propice à l'expression libre[22]. Cette liberté est menacée par la censure d'Internet, qui est utilisée pour contrôler ou supprimer ce qui peut être consulté, publié ou consulté sur Internet[23].

---

[14] Global Expression Report 2018/19: Intermediary Liability. ARTICLE 19.

[15] Which Intermediaries Have Your Back?: How Kenyan Intermediaries Protect Human Rights Online. KICTANet.

[16] "Fake News" and Internet Shutdowns in Africa – What is to be Done? CIPESA.

[17] Digital Security. CcHub.

[18] Cybercrime: The World's New Social Problem. CcHub.

[19] Universal Access to Information in Africa: What Governments Need to Do. CIPESA.

[20] Ensuring the Public's Right to Know in the COVID-19 Pandemic. ARTICLE 19

[21] The Universal Declaration of Human Rights. United Nations.

[22] Coronavirus: ARTICLE 19 briefing on tackling misinformation. ARTICLE 19.

[23] Digital Activism and the Right to Online Free Speech and Assembly [Case Study]. Paradigm Initiative (PIN).