*Module 4*

# Vie privée et protection des données

*Modules de synthèse sur les litiges relatifs aux droits numériques et à la liberté d'expression en ligne*

MEDIA DEFENCE

Publié par Media Defence : www.mediadefence.org
Ce module a été préparé avec l'aide d'ALT Advisory : https://altadvisory.africa/

**Décembre 2020**

Ce travail est sous licence Creative Commons Attribution-NonCommercial 4.0 International License. Cela signifie que vous êtes libre de partager et d'adapter ce travail à condition de mentionner le crédit approprié, de fournir un lien vers la licence et d'indiquer si des modifications ont été apportées. Tout partage ou adaptation de ce type doit être effectué à des fins non commerciales et doit être mis à disposition dans les mêmes conditions de « partage égal ». Les conditions de licence complètes sont disponibles à l'adresse https://creativecommons.org/licenses/by-ncsa/4.0/legalcode.

## TABLE DES MATIÈRES

**INTRODUCTION** ..... 1
**LE DROIT À LA VIE PRIVÉE** ..... 1
**PROTECTION DES DONNÉES** ..... 3
**« LE DROIT À L'OUBLI »** ..... 5
**LE CRYPTAGE ET L'ANONYMAT SUR L'INTERNET** ..... 8
**LA SURVEILLANCE NUMÉRIQUE DIRIGÉE PAR LE GOUVERNEMENT** ..... 10
**CONCLUSION** ..... 13

# MODULE 4

## CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

- **Le droit à la vie privée prend de plus en plus d'importance avec l'augmentation des flux de données et la nécessité concomitante de protéger les informations personnelles.**
- **Dans le contexte africain, il existe de multiples instruments, dont la Convention de l'UA sur la cyber-sécurité et la protection des données à caractère personnel (Convention de Malabo), qui régissent la protection des données.**
- **Il est important que les États veillent à ce que leur législation nationale détaille les principes du traitement légal des informations personnelles et qu'elle suive l'évolution de la protection des données.**
- **Les concepts de « droit à l'oubli », de cryptage et de surveillance gouvernementale sont associés à la protection des données.**
- **En particulier, la divulgation de sources journalistiques à la suite de la surveillance de l'État a un impact négatif sur la liberté d'expression et la liberté journalistique.**

## INTRODUCTION

Le droit à la vie privée et l'exigence concomitante de protection des informations personnelles ont suscité une attention considérable à l'aube de l'ère de l'information. Alors que l'échange d'informations et la collecte de données sur Internet et en ligne augmentent à un rythme exponentiel, les développements législatifs n'ont pas suivi le rythme et ne protègent pas suffisamment les informations personnelles. Toutefois, avec le temps, les États africains et les organismes régionaux et continentaux ont commencé à adopter des instruments et des règlements relatifs à la protection des données afin de remédier à la situation et de défendre le droit à la vie privée de leurs citoyens.

Ce module se concentre sur la protection des données en Afrique et les concepts connexes de « droit à l'oubli », de cryptage et de surveillance.

## LE DROIT À LA VIE PRIVÉE

Il est de plus en plus reconnu que le droit à la vie privée joue un rôle vital en soi et qu'il facilite le droit à la liberté d'expression. Par exemple, le recours au droit à la vie privée permet aux individus de partager des points de vue de manière anonyme dans des circonstances où ils peuvent craindre d'être censurés pour ces points de vue, il permet aux dénonciateurs de faire des divulgations protégées, et il permet aux membres des médias et aux militants de

communiquer en toute sécurité au-delà de la portée d'une interception gouvernementale illégale.

Le droit à la vie privée est contenu dans l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP), qui prévoit :

> « (1) Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.
> (2) Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Bien qu'il ne figure pas dans la Charte africaine des droits de l'homme et des peuples (CADHP), le droit à la vie privée des enfants est contenu dans l'article 10 de la Charte africaine des droits et du bien-être de l'enfant (CADBE), qui prévoit que :

> « Aucun enfant ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, son domicile ou sa correspondance familiale, ni d'atteintes à son honneur ou à sa réputation, étant entendu que les parents ou les tuteurs légaux ont le droit d'exercer une surveillance raisonnable sur la conduite de leurs enfants. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Le droit à la vie privée a également été reconnu dans d'autres instruments régionaux et sous-régionaux dans le contexte de la protection des données, qui est examiné plus loin. En outre, presque tous les États africains garantissent ce droit dans leur constitution nationale.[1]

Il est intéressant de noter qu'en 2017, la Cour suprême de l'Inde a déclaré que le droit à la vie privée est protégé en tant que partie intrinsèque du droit à la vie et à la liberté individuelle, et en tant que partie des libertés fondamentales garanties par la partie III de la Constitution indienne.[2] En tant que tel, bien que la Constitution indienne ne contienne pas expressément un droit à la vie privée, ce droit peut néanmoins être lu dans le contexte des autres droits et libertés qui sont garantis par la Constitution. Bien que cela n'ait pas été testé dans le contexte de la CADHP, il est possible d'interpréter le droit à la vie privée dans d'autres dispositions de la Charte africaine.

Comme pour le droit à la liberté d'expression, une limitation du droit à la vie privée doit satisfaire au test en trois parties pour une limitation justifiable. Selon la Cour constitutionnelle sud-africaine :[3]

---

[1] Au niveau national, plus de 50 constitutions africaines, y compris des amendements et des révisions récentes, font référence au droit à la vie privée. Singh and Power, « The privacy awakening: The urgent need to harmonise the right to privacy in Africa » Annuaire africain des droits de l'homme, volume 3 (2019) 202, page 202, accessible sur : http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf).

[2] « *Justice K.S. Puttaswamy and Another v Union of India and Others* », Demande nº 494/2012, 24 août 2017 (accessible en anglais sur : http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

[3] « *NM and Others v Smith and Others* », [2007] ZACC 6, 4 avril 2007 au paragraphe 33 (accessible en anglais sur : https://www.saflii.org/za/cases/ZACC/2007/6.html), citant avec approbation « *Bernstein and Others v Bester NNO and Others* », [1996] ZACC 2, 27 mars 1996 au paragraphe 77.

> « Un très haut niveau de protection est accordé à la sphère intime de la vie personnelle de l'individu et au maintien de ses conditions préalables de base et il existe une dernière sphère intouchable de la liberté humaine qui échappe à toute interférence de la part d'une autorité publique. À tel point que, en ce qui concerne ce noyau le plus intime de la vie privée, aucune limitation justifiable de celle-ci ne peut avoir lieu. Mais ce noyau le plus intime est interprété de façon étroite. Ce noyau inviolable est abandonné dès lors qu'un individu entre en relation avec des personnes situées en dehors de cette sphère intime la plus proche ; les activités de l'individu acquièrent alors une dimension sociale et le droit à la vie privée dans ce contexte devient sujet à limitation ».

Nous examinons ci-dessous les aspects spécifiques du droit à la vie privée et l'impact qu'Internet a eu sur la jouissance de ce droit.

## PROTECTION DES DONNÉES

Les lois sur la protection des données visent à protéger et à sauvegarder le traitement des informations personnelles (ou des données à caractère personnel). Il s'agit de toute information concernant une personne physique identifiée ou identifiable (à savoir la personne concernée) qui permet d'identifier cette personne, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Un gestionnaire de données, qui peut être un organisme public ou privé, désigne la personne ou l'entité responsable du traitement des informations personnelles concernant la personne concernée.

La protection des données est l'une des principales mesures par lesquelles le droit à la vie privée est mis en œuvre. Un certain nombre d'États africains ont déjà promulgué des lois sur la protection des données, et d'autres sont en train de le faire.[4] En plus de donner effet au droit à la vie privée, la législation sur la protection des données a également un rôle clé à jouer pour faciliter le commerce entre les États, car de nombreuses lois sur la protection des données limitent les transferts transfrontaliers de données dans les cas où l'État qui reçoit les informations n'assure pas un niveau de protection des données adéquat.

En ce qui concerne la protection des données à caractère personnel, l'Observation générale n° 16 sur l'article 17 du PIDCP (Observation générale n° 16) prévoit ce qui suit :[5]

> « La collecte et la conservation d'informations personnelles sur des ordinateurs, des banques de données et d'autres dispositifs, qu'elles soient le fait d'autorités publiques ou de personnes ou d'organismes privés, doivent être réglementées par la loi. Des mesures efficaces doivent être prises par les États pour garantir que les informations concernant

[4] À l'heure actuelle, 21 États de l'Union africaine (UA) ont promulgué des lois complètes sur la protection de la vie privée : Afrique du Sud, Angola, Bénin, Burkina Faso, Cap-Vert, Côte d'Ivoire, Égypte, Gabon, Ghana, Guinée équatoriale, Kenya, Lesotho, Madagascar, Mali, Maroc, Maurice, Sénégal, Seychelles, Tchad, République togolaise et Tunisie. Quatre autres États ont indiqué qu'ils étaient sur le point d'adopter une législation : Niger, Tanzanie, Ouganda et Zimbabwe. Voir https://dataprotection.africa/ pour plus d'informations.

[5] Observation générale nº 16 au paragraphe 10.

> la vie privée d'une personne ne parviennent pas entre les mains de personnes qui ne sont pas autorisées par la loi à les recevoir, les traiter et les utiliser, et qu'elles ne soient jamais utilisées à des fins incompatibles avec le Pacte. Afin de bénéficier de la protection la plus efficace de sa vie privée, toute personne devrait avoir le droit de savoir, sous une forme intelligible, si des données à caractère personnel sont stockées dans des fichiers automatisés, et dans l'affirmative, lesquelles, et à quelles fins. Chaque personne devrait également pouvoir savoir quelles autorités publiques ou quels particuliers ou organismes privés contrôlent ou peuvent contrôler ses dossiers. Si ces dossiers contiennent des données à caractère personnel incorrectes ou ont été collectés ou traités contrairement aux dispositions de la loi, toute personne devrait avoir le droit de demander leur rectification ou leur suppression. »

La plupart des lois sur la protection des données prévoient généralement les principes suivants :[6]

- Les informations personnelles doivent être traitées de manière loyale et licite, et ne doivent pas être traitées si les conditions stipulées ne sont pas remplies.
- Les informations personnelles doivent être obtenues dans un but (ou des buts) précis et ne doivent pas être traitées ultérieurement de manière incompatible avec ce but.
- Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard de la (ou des) finalité(s) pour laquelle (lesquelles) elles sont traitées.
- Les informations personnelles doivent être exactes et, le cas échéant, mises à jour.
- Les informations personnelles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire pour les besoins de la collecte.
- Les informations personnelles doivent être traitées conformément aux droits des personnes concernées prévus par la loi sur la protection des données.
- Des mesures techniques et organisationnelles appropriées doivent être prises contre le traitement non autorisé ou illicite de données à caractère personnel et contre la perte, la destruction ou la détérioration accidentelle de données à caractère personnel.
- Les données à caractère personnel ne doivent pas être transférées vers un autre pays qui n'assure pas un niveau de protection adéquat des droits et libertés des personnes concernées en ce qui concerne le traitement des informations à caractère personnel.

Il existe un certain nombre d'instruments régionaux africains qui traitent de la protection des données :

- **Convention de l'UA sur la cyber-sécurité et la protection des données à caractère personnelle de 2014**[7] (Convention de l'UA ou « Convention de Malabo ») : Cet instrument, qui vise un niveau continental, comprend des dispositions relatives à la protection des données, aux transactions électroniques, à la cybercriminalité et à la cybersécurité. Les dispositions relatives à la protection des données sont contenues dans le chapitre II, et contiennent les conditions du traitement licite des informations

[6] Information Commissioner's Office, « Data protection principles » (accessible sur : https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/).

[7] Accessible sur : https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_f.pdf. À l'heure actuelle, elle a été ratifiée par un État et signée par dix autres États.

personnelles, ainsi que les droits accordés aux personnes concernées. Bien qu'il ne soit pas encore entré en vigueur, il pourrait à l'avenir être un instrument juridique contraignant sur la protection des données en Afrique.

- **Projet de cadre juridique de la CAE pour les cyberlégislations de 2008** (Cadre juridique de la CAE) : Cet instrument couvre des sujets relatifs à la protection des données, au commerce électronique, à la sécurité des données et à la protection des consommateurs. Il n'est pas destiné à être une loi type, mais fournit plutôt des orientations et des recommandations aux États pour les aider à élaborer leurs lois en connaissance de cause. La protection des données est traitée brièvement au paragraphe 2.5 du cadre juridique de la CAE.
- **Acte additionnel sur la protection des données à caractère personnel au sein de la CEDEAO 2010** (Acte additionnel de la CEDEAO) : Cet instrument est conçu pour être directement transposé dans un contexte national et, à l'instar de la Convention de l'UA, il prévoit en détail les conditions de traitement licite des informations à caractère personnel et les droits des personnes concernées.
- **Loi type de la SADC pour la protection des données de 2013** (Loi type de la SADC) : Cet instrument est une loi type qui peut être utilisée dans un contexte national par les États membres. Elle cherche à assurer l'harmonisation des politiques en matière de technologies de l'information et des communications (TIC) et reconnaît que les développements des TIC ont un impact sur les droits et la protection des données à caractère personnel, y compris dans les activités gouvernementales et commerciales. Outre la définition des conditions de traitement licite des informations personnelles et des droits des personnes concernées, elle traite également de la dénonciation, en prévoyant que l'autorité chargée de la protection des données doit établir des règles autorisant et régissant le système de dénonciation qui préservent les principes de protection des données, notamment les principes d'équité, de licéité, de finalité, de proportionnalité et d'ouverture.

En plus de donner effet au droit à la vie privée, les lois sur la protection des données facilitent généralement le droit d'accès à l'information. À cet égard, la plupart des lois sur la protection des données prévoient que les personnes concernées peuvent demander et obtenir l'accès aux informations détenues à leur sujet par un responsable du traitement. Ce mécanisme peut permettre aux personnes concernées de vérifier si leurs informations personnelles sont traitées conformément aux lois applicables en matière de protection des données, et si leurs droits sont effectivement respectés.

## « LE DROIT À L'OUBLI »[8]

Le « droit à l'oubli » (qui est peut-être mieux décrit comme « le droit d'effacer » ou « le droit d'être rayé de la liste ») implique le droit de demander que les moteurs de recherche commerciaux ou d'autres sites web qui recueillent des informations personnelles à des fins lucratives, comme Google, suppriment les liens vers des informations privées lorsqu'on le leur

[8] Pour en savoir plus sur ce sujet, voir le « Manuel de formation sur les droits numériques et la liberté d'expression en ligne de Media Defence : litige sur les droits numériques et la liberté d'expression en ligne en Afrique de l'Est, de l'Ouest et du Sud » (accessible sur : https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

demande. Le droit à l'oubli progresse par rapport au droit des personnes concernées contenu dans de nombreuses lois sur la protection des données, selon lequel les informations personnelles détenues sur une personne doivent être effacées dans les cas où elles sont inadéquates, non pertinentes ou plus pertinentes, ou excessives par rapport aux objectifs pour lesquels elles ont été collectées.

En 2014, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt important dans l'affaire *« Google Espagne contre Gonzalez »*.[9] M. Gonzalez, un ressortissant espagnol, a déposé une plainte en 2010 auprès du régulateur espagnol de l'information. La cause de la plainte de M. Gonzalez était que, lorsqu'un internaute saisissait son nom dans le moteur de recherche de Google, il obtenait des liens vers des pages du journal espagnol de 1998 faisant référence à des procédures de saisie à son encontre pour le recouvrement de certaines créances. M. Gonzalez a demandé que les données à caractère personnel le concernant soient supprimées ou dissimulé, car la procédure engagée contre lui a été entièrement résolue et que la référence à lui est donc désormais sans objet.

Devant la CJUE, s'appuyant sur la législation de l'UE en matière de protection des données en vigueur à l'époque, la demande a été confirmée. La CJUE a noté que l'affichage même d'informations personnelles sur une page de résultats de recherche constitue un traitement de ces informations,[10] et qu'il n'y a aucune raison pour qu'un moteur de recherche ne soit pas soumis aux obligations et garanties prévues par la loi.[11] En outre, il a été noté que le traitement des informations personnelles effectué par un moteur de recherche peut affecter de manière significative les droits fondamentaux à la vie privée et à la protection des données à caractère personnel lorsqu'une recherche est effectuée à partir du nom d'une personne, car il permet à tout internaute d'obtenir un aperçu structuré des informations relatives à cette personne et d'établir un profil de celle-ci.[12] Selon la CJUE, l'effet de l'interférence « est renforcé compte tenu du rôle important joué par l'Internet et les moteurs de recherche dans la société moderne, qui rendent l'information contenue dans une telle liste de résultats omniprésente ».[13]

En ce qui concerne la radiation, la CJUE a estimé que la suppression des liens de la liste des résultats pourrait, selon les informations en cause, avoir des effets sur les internautes légitimes potentiellement intéressés à avoir accès à ces informations.[14] Il faudrait pour cela trouver un juste équilibre entre cet intérêt et les droits fondamentaux de la personne concernée, en tenant compte de la nature des informations, de leur sensibilité pour la vie privée de la personne concernée et de l'intérêt du public à disposer de ces informations, qui peut varier en fonction du rôle joué par la personne concernée dans la vie publique.[15]

La CJUE a ensuite estimé qu'une personne concernée est autorisée à demander que les informations la concernant ne soient plus mises à la disposition du grand public par leur

---

[9] *« Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another »*, Affaire N° C-131/12, 13 mai 2014 (accessible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62012CJ0131).

[10] Même endroit au paragraphe 57

[11] Même endroit au paragraphe 58

[12] Même endroit au paragraphe 80

[13] *Idem*

[14] Même endroit au paragraphe 81

[15] *Idem*

inclusion dans une liste de résultats de recherche lorsque, compte tenu de l'ensemble des circonstances, ces informations apparaissent inadéquates, non pertinentes ou non plus pertinentes, ou excessives au regard des finalités du traitement effectué par l'opérateur du moteur de recherche.[16] Dans ces circonstances, les informations et les liens concernés dans la liste des résultats doivent être effacés.[17]

Le droit à l'oubli a également été reconnu dans des contextes nationaux. Par exemple, la Cour suprême de cassation italienne a jugé que l'intérêt du public pour un article diminuait après deux ans et demi, et que les informations sensibles et privées ne devaient pas être accessibles au public indéfiniment.[18] L'affaire est actuellement en cours de litige devant la Cour européenne des droits de l'homme.[19] La Cour de cassation belge a également reconnu le droit à l'oubli.[20]

Il y a cependant des limites à la portée du droit à l'oubli. En 2017, la CJUE a été saisie d'une demande de décision préjudicielle dans l'affaire *« Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contre Salvatore Manni »*.[21] M. Manni, s'appuyant sur la décision *Gonzalez*, a demandé une ordonnance enjoignant à la Chambre de commerce d'effacer, d'anonymiser ou de bloquer toutes les données le liant à la liquidation de sa société contenues dans le registre des sociétés. La CJUE a refusé de faire droit à la demande de M. Manni et a estimé que, compte tenu de l'éventail des utilisations légitimes possibles des données figurant dans les registres des sociétés et des différents délais de prescription applicables à ces registres, il était impossible de déterminer une durée de conservation maximale appropriée. En conséquence, la CJUE a refusé de conclure qu'il existe un droit général à l'oubli des registres publics des sociétés.

En outre, d'autres juridictions ont refusé de défendre un droit à l'oubli face aux moteurs de recherche. Au Brésil, par exemple, il a été jugé que les moteurs de recherche ne peuvent être contraints de supprimer les résultats de recherche relatifs à un terme ou une expression spécifique ;[22] de même, la Cour suprême du Japon a refusé d'appliquer le droit d'être oublié

---

[16] Même endroit au paragraphe 94.

[17] Même endroit au paragraphe 94.

[18] *Plaintiff X v PrimaDaNoi*, Affaire nº 13161, 22 novembre 2015 (accessible sur : https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[19] Cour européenne des droits de l'homme, Demande nº 77419/16 (2020) (accessible en anglais sur : https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-201483%22%5D%7D).

[20] *P.H. v O.G.*, Affaire nº 15/0052/F, 29 avril 2016 (accessible sur : https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf). Pour une analyse de l'affaire, voir Hunton & Williams, « Belgian Court of Cassation rules on right to be forgotten », 1er juin 2016 (accessible en anglais sur : https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

Pour en savoir plus sur le droit à l'oubli, voir *« NT1 & NT2 v Google LLC »* au Royaume-Uni (2018) (accessible sur : https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf).

[21] Affaire nº C-385-15, 9 mars 2017 (accessible sur : https://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=446798).

[22] *« Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others »*, 2011/0307909-6, 26 juin 2012 (accessible sur : https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

à Google, estimant que la suppression « ne peut être autorisée que lorsque la valeur de la protection de la vie privée l'emporte largement sur celle de la divulgation d'informations ».[23]

Selon les Principes mondiaux pour la liberté d'expression et la protection de la vie privée (Principes mondiaux),[24] le droit (dans la mesure où il est reconnu dans une juridiction particulière) doit être limité au droit des personnes, en vertu de la législation sur la protection des données, de demander aux moteurs de recherche de retirer de la liste les résultats de recherche inexacts ou périmés produits sur la base d'une recherche de leur nom,[25] et doit être limité dans sa portée au nom de domaine correspondant au pays où le droit est reconnu et où la personne a établi un préjudice important.[26] Il précise en outre que les demandes de radiation devraient être soumises à un jugement final par un tribunal ou un organe juridictionnel indépendant ayant une expertise pertinente en matière de liberté d'expression et de législation sur la protection des données.[27]

## LE CRYPTAGE ET L'ANONYMAT SUR L'INTERNET[28]

Le cryptage est un processus mathématique consistant à convertir des messages, des informations ou des données sous une forme illisible par quiconque, sauf par le destinataire prévu, et à protéger ainsi la confidentialité et l'intégrité du contenu contre l'accès ou la manipulation par des tiers.[29] Avec un « cryptage à clé publique » (la forme dominante de sécurité de bout en bout pour les données en transit) l'expéditeur utilise la clé publique du destinataire pour crypter le message et ses pièces jointes, et le destinataire utilise sa propre

[23] The Japan Times, « Top court rejects 'right to be forgotten' demand », 1er février 2017 (accessible sur : https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[24] Les principes mondiaux (accessible sur : https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=53314e174#:~:text=Toute%20personne%20a%20droit%20%C3%A0,autre%20forme%20de%20m%C3%A9dias%20de) ont été élaborés par la société civile, sous la direction de l'ARTICLE19, en coopération avec des experts de haut niveau du monde entier.

[25] Principe 18(1) des Principes mondiaux.

[26] Même endroit au principe 18(4).

[27] Même endroit au principe 18(2).

[28] Pour en savoir plus sur ce sujet, voir le « Manuel de formation sur les droits numériques et la liberté d'expression en ligne de Media Defence : litige sur les droits numériques et la liberté d'expression en ligne en Afrique de l'Est, de l'Ouest et du Sud » (accessible sur : https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[29] Rapport du RSNU sur la liberté d'expression, « Rapport sur l'anonymat, le cryptage et le cadre des droits de l'homme », A/HRC/29/32, 22 mai 2015 (Rapport du RSNU sur l'anonymat et le cryptage), paragraphe 7 (accessible sur : https://digitallibrary.un.org/record/798709/files/A_HRC_29_32-FR.pdf). Pour plus de détails et de ressources, voir UCI Law International Justice Clinic, « Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression » (accessible en anglais sur : http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf).

clé privée pour les décrypter.[30] Il est également possible de crypter les données au repos qui sont stockées sur son appareil, tel qu'un ordinateur portable ou un disque dur.[31]

L'anonymat peut être défini soit comme le fait d'agir ou de communiquer sans utiliser ou présenter son nom ou son identité, soit comme le fait d'agir ou de communiquer d'une manière qui protège la détermination de son nom ou de son identité, soit comme le fait d'utiliser un nom inventé ou supposé qui n'est pas nécessairement associé à son identité légale ou coutumière.[32] On peut distinguer l'anonymat du pseudoanonymat : le premier consiste à ne pas prendre de nom du tout, tandis que le second consiste à prendre un nom d'emprunt.[33]

Le cryptage et l'anonymat sont des outils nécessaires à la pleine jouissance des droits numériques, et bénéficient d'une protection en vertu du rôle essentiel qu'ils jouent dans la garantie des droits à la liberté d'expression et à la vie privée. Tel que décrit par le rapporteur spécial des Nations unies (UNSR) sur la liberté d'expression :[34]

> « Le cryptage et l'anonymat, séparément ou ensemble, créent une zone de vie privée pour protéger les opinions et les croyances. Par exemple, ils permettent des communications privées et peuvent protéger une opinion d'un examen extérieur, ce qui est particulièrement important dans des environnements politiques, sociaux, religieux et juridiques hostiles. Lorsque les États imposent une censure illégale par le biais du filtrage et d'autres technologies, le recours au cryptage et à l'anonymat peut permettre aux individus de contourner les obstacles et d'accéder aux informations et aux idées sans l'intrusion des autorités. Les journalistes, les chercheurs, les avocats et la société civile ont recours au cryptage et à l'anonymat pour se protéger (ainsi que leurs sources, clients et partenaires) de la surveillance et du harcèlement. La possibilité de faire des recherches sur le web, de développer des idées et de communiquer en toute sécurité peut être le seul moyen pour beaucoup d'explorer les aspects fondamentaux de l'identité, comme le sexe, la religion, l'ethnicité, l'origine nationale ou la sexualité. Les artistes comptent sur le cryptage et l'anonymat pour sauvegarder et protéger leur droit à l'expression, en particulier dans les situations où ce n'est pas seulement l'État qui crée des limites, mais aussi la société qui ne tolère pas les opinions ou les expressions non conventionnelles ».

Le cryptage et l'anonymat sont particulièrement utiles pour le développement et le partage d'opinions en ligne, notamment dans des circonstances où des personnes peuvent craindre que leurs communications fassent l'objet d'interférences ou d'attaques par des acteurs étatiques ou non étatiques. Il s'agit donc de technologies spécifiques par lesquelles les individus peuvent exercer leurs droits. Par conséquent, les restrictions en matière de cryptage et d'anonymat doivent répondre au test en trois parties pour justifier la restriction.

Selon le RSNU sur la liberté d'expression, si le cryptage et l'anonymat peuvent frustrer les responsables de l'application des lois et de la lutte contre le terrorisme et compliquer la

---

[30] *Idem*

[31] *Idem*

[32] Electronic Frontier Foundation, « *Anonymity and encryption* », 10 février 2015 en page 3 (accessible en anglais sur : https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

[33] *Idem*

[34] Rapport du RSNU sur l'anonymat et le cryptage ci-dessus, point 29 au paragraphe 12.

surveillance, les autorités de l'État n'ont généralement pas réussi à fournir une justification publique appropriée pour soutenir la restriction ou à identifier les situations où la restriction a été nécessaire pour atteindre un objectif légitime.[35] L'interdiction pure et simple de l'utilisation individuelle de la technologie de cryptage restreint de manière disproportionnée le droit à la liberté d'expression, car elle prive tous les utilisateurs en ligne d'une juridiction particulière du droit de se tailler un espace d'opinion et d'expression, sans qu'il soit possible de prétendre que l'utilisation du cryptage est faite à des fins illégales.[36] De même, la réglementation étatique du cryptage peut équivaloir à une interdiction, par exemple en exigeant des licences pour l'utilisation du cryptage, en fixant des normes techniques faibles pour le cryptage ou en contrôlant l'importation et l'exportation d'outils de cryptage.[37]

Le RSNU sur la liberté d'expression a appelé les États à promouvoir un cryptage fort et l'anonymat, et a noté que les ordres de décryptage ne doivent être autorisés que lorsqu'ils résultent de lois transparentes et accessibles au public, appliquées uniquement de manière ciblée, au cas par cas, à des individus (et non à une masse de personnes), et sous réserve d'un mandat judiciaire et de la protection des droits des individus à une procédure régulière.[38]

## LA SURVEILLANCE NUMÉRIQUE DIRIGÉE PAR LE GOUVERNEMENT[39]

La surveillance des communications englobe la surveillance, l'interception, la collecte, l'obtention, l'analyse, l'utilisation, la préservation, la conservation, l'interférence, l'accès ou des actions similaires prises en ce qui concerne des informations qui incluent, reflètent, découlent ou concernent les communications d'une personne dans le passé, le présent ou l'avenir.[40] Cela concerne à la fois le contenu des communications et les métadonnées. En ce qui concerne ce dernier point, il a été noté que l'agrégation d'informations (communément appelées « métadonnées ») peut donner un aperçu du comportement, des relations sociales, des préférences privées et de l'identité d'un individu. Pris dans son ensemble, elle peut permettre de tirer des conclusions très précises concernant la vie privée de la personne.

L'Observation générale n° 16 prévoit que « [l]a surveillance, électronique ou autre, l'interception des communications téléphoniques, télégraphiques et autres, les écoutes téléphoniques et l'enregistrement des conversations devraient être interdits ».[41] La surveillance (qu'il s'agisse de la collecte massive (ou en masse) de données[42] ou de la collecte

[35] Même endroit au paragraphe 36.

[36] Même endroit au paragraphe 40.

[37] Même endroit au paragraphe 41.

[38] Même endroit aux paragraphes 59 à 60.

[39] Pour en savoir plus sur ce sujet, voir le « Manuel de formation sur les droits numériques et la liberté d'expression en ligne de Media Defence : litige sur les droits numériques et la liberté d'expression en ligne en Afrique de l'Est, de l'Ouest et du Sud » (accessible en anglais sur : https://www.mediadefence.org/resources/mldi-manual-on-freedom-of-expression-law/).

[40] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Principes de nécessité et de proportionnalité) en page 4 (accessible en anglais sur : https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[41] Observation générale nº 16 au paragraphe 8.

[42] Des révélations comme celle d'Edward Snowden ont révélé que l'Agence de sécurité nationale aux États-Unis et le quartier général des communications au Royaume-Uni avaient mis au point des technologies permettant d'accéder à une grande partie du trafic Internet mondial, aux relevés d'appels aux États-Unis, aux carnets d'adresses électroniques des particuliers et à d'énormes

ciblée de données) interfère directement avec la vie privée et la sécurité nécessaires à la liberté d'opinion et d'expression, et doit être considérée à la lumière du test en trois parties permettant d'évaluer la recevabilité de la restriction.[43] À l'ère numérique, les TIC ont renforcé la capacité des gouvernements, des entreprises et des particuliers à effectuer des opérations de surveillance, d'interception et de collecte de données, et ont permis de ne plus limiter l'efficacité de ces opérations par leur ampleur ou leur durée.[44]

Dans une résolution adoptée par l'Assemblée générale des Nations unies (AGNU) sur le droit à la vie privée à l'ère numérique, l'AGNU a souligné que la surveillance et/ou l'interception illégales ou arbitraires des communications, ainsi que la collecte illégale ou arbitraire de données personnelles sont des actes extrêmement intrusifs, qui violent le droit à la vie privée, peuvent interférer avec le droit à la liberté d'expression et peuvent être en contradiction avec les principes d'une société démocratique, y compris lorsqu'ils sont entrepris à grande échelle.[45] Elle a en outre noté que la surveillance des communications numériques doit être conforme aux obligations internationales en matière de droits de l'homme et doit être effectuée sur la base d'un cadre juridique, qui doit être accessible au public, clair, précis, complet et non discriminatoire.[46]

Afin de satisfaire à la condition de légalité, de nombreux États ont pris des mesures pour réformer leurs lois de surveillance afin de disposer des pouvoirs nécessaires pour mener les activités de surveillance. Selon les principes de nécessité et de proportionnalité, la surveillance des communications doit être considérée comme un acte hautement intrusif, et afin de respecter le seuil de proportionnalité, l'État doit être tenu au minimum d'établir les informations suivantes auprès d'une autorité judiciaire compétente avant de procéder à toute surveillance des communications :[47]

- Il existe un degré élevé de probabilité qu'un crime grave ou une menace spécifique à un objectif légitime ait été ou sera perpétré.
- Il est très probable que des éléments de preuve pertinents et matériels concernant une infraction aussi grave ou une menace spécifique à un objectif légitime soient obtenus en accédant aux informations protégées recherchées.
- D'autres techniques moins invasives ont été épuisées ou seraient futiles, de sorte que la technique utilisée est l'option la moins invasive.
- L'accès aux informations sera limité à celles qui sont pertinentes et importantes pour le crime grave ou la menace spécifique à un objectif légitime allégué.

---

volumes d'autres contenus de communication numérique. Ces technologies sont déployées par le biais d'un réseau transnational comprenant des relations de renseignement stratégique entre les gouvernements et d'autres acteurs. C'est ce qu'on appelle la surveillance de masse ou massive. Voir le rapport 2016 du HCDH au paragraphe 4.

[43] Rapport du RSNU sur la liberté d'expression de 2016, paragraphe 20.

[44] Rapport du HCDH, paragraphe 2.

[45] AGNU, « Résolution sur le droit à la vie privée à l'ère numérique », A/C.3/71/L.39/Rev.1, 16 novembre 2016 (Résolution de l'ONU sur la vie privée 2016) (accessible sur : https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1&Lang=F).

[46] *Idem*

[47] ci-dessus, au point 43, principe 5.

- Toute information excédentaire recueillie ne sera pas conservée, mais sera rapidement détruite ou renvoyée.
- Les informations ne seront accessibles qu'à l'autorité spécifiée et ne seront utilisées qu'aux fins et pour la durée pour lesquelles l'autorisation a été donnée.
- Les activités de surveillance demandées et les techniques proposées ne portent pas atteinte à l'essence du droit à la vie privée ou des libertés fondamentales.

La surveillance constitue une ingérence évidente dans le droit à la vie privée. En outre, elle constitue également une ingérence dans le droit à la liberté d'opinion sans entrave et dans le droit à la liberté d'expression. En ce qui concerne plus particulièrement le droit d'avoir des opinions sans interférence, les systèmes de surveillance, qu'ils soient ciblés ou de masse, peuvent porter atteinte au droit de former une opinion, car la crainte de la divulgation involontaire d'une activité en ligne, telles que la recherche et la navigation, dissuade probablement les individus d'accéder à des informations, en particulier lorsque cette surveillance conduit à des résultats répressifs.[48]

L'interférence avec le droit à la liberté d'expression est particulièrement évidente dans le contexte des journalistes et des membres des médias qui peuvent être placés sous surveillance en raison de leurs activités journalistiques. Comme l'a fait remarquer le Secrétaire général des Nations unies, cela peut avoir un effet paralysant sur la jouissance de la liberté des médias et rendre plus difficile la communication avec les sources, le partage et le développement des idées, ce qui peut conduire à l'autocensure.[49] L'utilisation du cryptage et d'autres outils similaires sont devenus essentiels au travail des journalistes afin de garantir qu'ils puissent mener leur travail sans interférence.

La divulgation de sources journalistiques et la surveillance peuvent avoir des conséquences négatives sur le droit à la liberté d'expression en raison d'une violation de la confidentialité des communications d'un individu.[50] Il en va de même pour les cas concernant la divulgation de données d'utilisateurs anonymes. Une fois que la confidentialité est compromise, celle-ci ne peut être rétablie. Il est donc de la plus haute importance que les mesures qui portent atteinte à la confidentialité ne soient pas prises arbitrairement.

L'importance de la protection des sources a été bien établie. Par exemple, dans l'affaire *« Bosasa Operation (Pty) Ltd v Basson and Another »*, la Haute Cour d'Afrique du Sud a estimé que les journalistes ne sont pas tenus de révéler leurs sources, sous réserve de certaines exceptions.[51] Le tribunal a déclaré à cet égard que :

---

[48] Rapport du RSNU sur l'anonymat et le cryptage au paragraphe 21.

[49] Rapport du Secrétaire général des Nations unies à l'Assemblée générale des Nations unies, « Rapport sur la sécurité des journalistes et la question de l'impunité », A/70/290, 6 août 2015 (Rapport du Secrétaire général des Nations unies de 2015), paragraphes 14 à 16 (accessible sur : https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session30/Documents/A_HRC_30_68_FRE.DOCX).

[50] Pour plus d'informations, voir « *Big Brother Watch v United Kingdom* in the ECtHR » (2018) (accessible en anglais sur : https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/) *et « amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa » (2019) (accessible en anglais sur : http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).

[51] [2012] ZAGPJHC 71, 26 avril 2012 (accessible en anglais sur : http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html).

> « Si la liberté de la presse est effectivement fondamentale et une *condition sine qua non* de la démocratie, il est essentiel que, dans l'exercice de ce devoir public pour le bien public, l'identité de leurs sources ne soit pas révélée, en particulier lorsque les informations ainsi révélées n'auraient pas été connues du public. Ce rôle essentiel et critique des médias, qui est plus prononcé dans notre démocratie naissante, fondée sur l'ouverture, où la corruption est devenue cancéreuse, doit être encouragé plutôt que dénudé ».[52]

Les activités de surveillance menées à l'encontre des journalistes risquent de compromettre fondamentalement la protection des sources à laquelle les journalistes ont par ailleurs droit.[53]

## CONCLUSION

À mesure que le monde se déplace en ligne, la protection des données devient de plus en plus nécessaire. Dans un contexte africain, des progrès ont été réalisés, 21 États africains ayant mis en place des lois sur la vie privée. Cependant, avec la croissance rapide de la collecte de données, les législateurs ont pris un certain retard dans la protection et la promotion de la confidentialité et de la protection des données. À mesure que nous progressons, les militants des droits numériques ont un rôle important à jouer en veillant à ce que les États suivent l'évolution de la protection des données et adoptent des cadres législatifs qui protègent et promeuvent pleinement le droit des personnes à la vie privée.

---

[52] Même endroit au paragraphe 38.

[53] Selon le principe 9 des Principes mondiaux, les États doivent prévoir la protection de la confidentialité des sources dans leur législation et garantir que :

- toute restriction du droit à la protection des sources est conforme au test en trois parties du droit international des droits de l'homme.
- le secret des sources ne doit être levé que dans des circonstances exceptionnelles et uniquement par une décision de justice, qui répond aux exigences d'un objectif légitime, de nécessité et de proportionnalité. Les mêmes protections doivent s'appliquer à l'accès au matériel journalistique.
- le droit de ne pas divulguer l'identité des sources et la protection du matériel journalistique exigent que la vie privée et la sécurité des communications de toute personne exerçant une activité journalistique, y compris l'accès aux données et métadonnées de ses communications, soient protégées. Les contournements, tels que la surveillance secrète ou l'analyse des données de communication non autorisée par les autorités judiciaires selon des règles juridiques claires et strictes, ne doivent pas être utilisés pour porter atteinte à la confidentialité des sources.
- toute décision de justice ne doit être rendue qu'après un procès équitable, si le journaliste en question a été prévenu suffisamment à l'avance, sauf en cas d'urgence réelle.