MINISTERE DE L'ECONOMIE NUMERIQUE
ET DE LA TRANSFORMATION DIGITALE

MINISTERE DE LA SECURITE
ET DE LA PROTECTION CIVILE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRÊTÉ N° 006 /24/MENTD/MSPC

Portant mécanisme de blocage des sites et contenus illégaux ou malveillants

---

LE MINISTRE DE L'ECONOMIE NUMERIQUE ET DE LA TRANSFORMATION DIGITALE,

LE MINISTRE DE LA SECURITE ET DE LA PROTECTION CIVILE,

Vu la Constitution togolaise du 06 mai 2024 ;

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n°2013-003 du 19 février 2013 ;

Vu la loi n° 2014-004 du 08 mai 2014 relative à la répression des infractions de chèques ;

Vu la loi n°2012-018 sur les communications électroniques, telle que modifiée par la loi n°2013-003 ;

Vu la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;

Vu la loi n°2017-006 du 22 juin 2017 d'orientation de la société de l'information au Togo ;

Vu la loi n°2017-017 du 22 juin 2017 relative aux transactions électroniques telle que modifiée par la loi n°2023-012 du 19 juillet 2023 ;

Vu la loi n°2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité telle que modifiée par la loi n°2022-009 du 24 juin 2022 ;

Vu la loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n°2015-091/PR du 27 novembre 2015 portant organisation et fonctionnement de l'Autorité de régulation des communications électroniques et des postes ;

Vu le décret n°2018-062/PR du 20 octobre 2016 portant règlementation des transactions et services électroniques au Togo ;

Vu le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société Cyber Defense Africa tel que modifié par le décret n°2020-034/PR du 11 mai 2020 ;

Vu le décret n°2024-040/PR du 1er août 2024 portant nomination du Premier ministre ;

Vu le décret n°2024-041/PR du 20 août 2024 portant composition du gouvernement ;

Considérant la nécessité de protéger le cyberespace togolais contre les sites internet et les contenus manifestement illégaux ou malveillants,

ARRETENT :

Article 1er : Objet

Le présent arrêté a pour objet de mettre en place un mécanisme permettant le signalement et le blocage des sites et contenus manifestement illégaux ou malveillants accessibles sur le territoire national.

Article 2 : Définitions

Au sens du présent arrêté, on entend par :

CERT : le centre national d'alerte et de réaction aux attaques informatiques placé sous l'autorité de l'Agence nationale de cybersécurité.

Personne qualifiée : une ou plusieurs personnes désignée(s) par son président au sein de l'Agence nationale de cybersécurité et au sein du CERT.

Plateforme : le système informatique utilisé par le CERT en vue de permettre le signalement de sites ou contenus manifestement illégaux ou malveillants et leur traitement conformément aux dispositions du présent arrêté.

Sites ou contenus manifestement illégaux : sites internet ou contenus accessibles sur internet, à l'exception des correspondances privées, manifestement utilisés pour commettre les infractions ou actes suivants :

- la fourniture illégale de services, y compris la vente de biens illégaux ;
- Les infractions relatives aux jeux d'argent et de hasard en ligne prévues aux articles 636 à 638 de la loi n° 2015-10 du 24 novembre 2015 portant nouveau code pénal.
- les infractions de production, d'importation, exportation, ou possession d'une image ou d'une représentation à caractère pornographique infantile visées aux articles 111, 112 et 113 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- l'infraction de facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur visée à l'article 114 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité :
- l'infraction d'incitation au suicide prévue à l'article 24 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- l'infraction de menace par le biais d'un système informatique visée à l'article 16 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- l'infraction de violation du secret de la défense nationale visée aux articles 644 à 648 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;

- l'infraction de mercenariat visée aux articles 648 à 653 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- les infractions relatives aux atteintes à la sécurité extérieure de l'Etat visées aux articles 654 à 662 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- les infractions relatives aux atteintes à la sécurité intérieure de l'Etat visées aux articles 663 à 666 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- les infractions relatives au terrorisme visées au Titre V de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- les infractions de traite des personnes et du trafic illicite de migrants par terre, air et mer visées aux articles 317 à 334 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;

Sites ou contenus manifestement malveillants : sites internet ou contenus accessibles sur internet, à l'exception des correspondances privées, utilisés pour commettre les infractions ou actes suivants :

- les infractions d'abus de confiance ou escroquerie prévues aux article 429 et suivants et 448 et suivants de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- les infractions en matière d'accès frauduleux à un système informatique ou d'entrave au fonctionnement d'un système informatique prévues aux articles 8 et 9 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- les infractions en matière de vol d'informations ou de données prévue à l'article 19 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- les infractions d'atteinte en matière de données et de systèmes d'informations prévues à l'article 474 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal et à l'article 10 de la loi n°2018-026 en date du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité ;
- les infractions d'usage frauduleux d'un moyen de paiement électronique et de fraude à la carte bancaire prévues par la loi n° 2014-004 du 8 mai 2014 relative à la répression des infractions de chèques, de cartes bancaires et d'autres instruments et procédés électroniques de paiement ;
- l'infraction de traitement frauduleux des données à caractère personnel prévue à l'article 84 de la loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- l'infraction d'extorsion prévue à l'article 463 de la loi n°2015-10 du 24 novembre 2015 portant nouveau code pénal ;
- tout acte de prospection directe interdit visé aux articles 35 et 36 de la loi n°2017-017 du 22 juin 2017 relative aux transactions électroniques telle que modifiée par la loi n°2023-012 du 19 juillet 2023 ;
- tout acte d'usurpation d'identité ;

Site miroir : désigne tout site internet hébergeant une copie, totale ou substantielle, d'un site internet principal.

Les autres termes et expressions employés dans le présent arrêté ont le sens qui leur est attribué par la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n° 2013-003 du 19 février 2013, la loi n°2017-017 du 22 juin 2017 relative aux transactions électroniques telle que modifiée par la loi n°2023-012 du 19 juillet 2023 et la loi n°2018-026 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité telle que modifiée par la loi n°2022-009 du 24 juin 2022.

Article 3 : Plateforme

Le CERT met en place et assure le bon fonctionnement et la maintenance de la plateforme dédiée au blocage des sites et contenus illégaux ou malveillants et leurs sites miroirs.

Cette plateforme permet à toute personne de signaler des sites et contenus manifestement illégaux ou malveillants en vue d'obtenir leur blocage et d'assurer la coordination entre toutes les parties prenantes chargées d'exécuter les obligations prévues dans le présent arrêté.

Article 4 : Compétences et missions du CERT

Le CERT est chargé, à l'aide de la plateforme, de :

- assurer la communication et la sensibilisation de l'ensemble des personnes, entreprises et administrations sur la plateforme, notamment ses fonctionnalités et les modalités de signalements ;
- fournir aux utilisateurs un accès à la plateforme, les former à l'utilisation de la plateforme et les assister en cas de difficultés rencontrées dans le cadre de l'utilisation de la plateforme ;
- assurer une veille active en vue d'identifier les sites et contenus qui pourraient être considérés comme illégaux ou malveillants ;
- analyser les signalements soumis sur la plateforme ;
- procéder à une catégorisation des sites et contenus signalés conformément aux dispositions de l'article 7 du présent arrêté ;
- établir des propositions de blocage de sites et contenus illégaux ou malveillants ou de rejet des signalements et les transmettre aux personnes visées aux articles 8 et 9 du présent arrêté.

Article 5 : Personnes qualifiées

Les personnes qualifiées sont des agents assermentés de l'Agence nationale de cybersécurité.

Dans le cas où les personnes qualifiées n'auraient pas déjà prêté serment dans le cadre de l'exercice de leurs missions au sein de l'Agence nationale de cybersécurité, les personnes qualifiées prêtent serment devant la chambre administrative de la cour d'appel de Lomé selon la formule suivante : « *Je jure de remplir avec conscience, probité et loyalisme, mes fonctions en me conformant à la loi, tout en observant les devoirs et les réserves qu'elles m'imposent. Je m'engage à garder scrupuleusement en tout temps, en tout lieu et en toute circonstance, le secret des informations dont j'aurai connaissance dans l'exercice de mes fonctions. En cas de parjure, que je subisse la rigueur de la loi* ».

Les personnes qualifiées ont l'obligation de réserve et de respect du secret professionnel pour les faits, actes et renseignements dont elles ont pu avoir connaissance du fait de leurs

fonctions. Elles sont tenues au respect strict du secret d'État. Toute violation de ce secret les expose aux sanctions pénales prévues par les lois en vigueur.

Article 6 : Signalement des sites et des contenus manifestement malveillants et illégaux

Toute personne peut signaler un site ou un contenu qu'elle estime manifestement malveillant ou illégal sur la plateforme.

Dans le cadre de la veille qu'il assure, le CERT signale les sites et contenus manifestement malveillants et illégaux qu'il identifie sur la plateforme.

Le signalement doit permettre la communication des informations suivantes :

- l'identité et les coordonnées de l'auteur du signalement ;
- l'adresse URL du site ou contenu signalé ou le moyen permettant d'y accéder ;
- les motifs du signalement ;
- le cas échéant, les éléments de preuve disponibles.

Le CERT accuse réception du signalement dans un délai de trente minutes.

La confidentialité de l'identité de toute personne réalisant un signalement sur la plateforme et du contenu de ce signalement est garantie.

Article 7 : Vérification et classification des signalements

Le CERT procède à la vérification et à la catégorisation des signalements dans un délai d'une heure. Il peut demander à l'auteur du signalement de fournir des informations complémentaires si nécessaire.

Le CERT catégorise les signalements de la façon suivante :

- Catégorie A : site ou contenu manifestement illégal ;
- Catégorie B : site ou contenu manifestement malveillant.

Si le signalement est jugé infondé, le CERT propose à l'Agence nationale de cybersécurité de le rejeter.

Dès la catégorisation des sites et contenus, les personnes concernées visées aux articles 8 et 9 du présent arrêté en sont immédiatement informées à travers la plateforme.

Article 8 : Traitement du blocage des sites manifestement illégaux par l'Agence Nationale de Cybersécurité

Lorsqu'un signalement est classé dans la catégorie A, les personnes qualifiées au sein de l'Agence nationale de cybersécurité en sont immédiatement notifiées à travers la plateforme. Elles disposent d'un délai maximal de quatre heures pour :

- décider du blocage du site ou du contenu ;
- rejeter la demande de blocage du site ou du contenu ;
- modifier la catégorisation proposée par le CERT sur la plateforme.

La demande de blocage est immédiatement notifiée aux opérateurs de communications électroniques à travers la plateforme.

Article 9 : Traitement du blocage des sites ou contenus manifestement malveillants par le personnel qualifié du CERT

Lorsqu'un signalement est classé dans la catégorie B les personnes qualifiées au sein du CERT en sont immédiatement notifiées à travers la plateforme. Elles disposent d'un délai maximal de quatre heures pour :

- décider du blocage du site ou du contenu ;
- rejeter la demande de blocage du site ou du contenu ;
- modifier la catégorisation proposée sur la plateforme.

La demande de blocage est immédiatement notifiée aux opérateurs de communications électroniques à travers la plateforme.

Article 10 : Mise en œuvre des décisions de blocage

Toute décision de blocage est immédiatement notifiée aux opérateurs de communications électroniques, au ministre chargé de l'économie numérique et à l'auteur du signalement à travers la plateforme.

Toute décision de rejet d'une demande de blocage est immédiatement notifiée à l'auteur du signalement à travers la plateforme.

Article 11 : Blocage des sites et contenus par les opérateurs de communications électroniques

Les opérateurs de communications électroniques doivent se conformer à l'injonction de blocage qui leur est notifiée à travers la plateforme dans l'heure suivant la notification visée aux articles 8 et 9 du présent arrêté.

Les opérateurs doivent mettre en œuvre tous les moyens utiles permettant de bloquer les sites et contenus illégaux et malveillants (et tout site miroir) ou les rendre inaccessibles sur le territoire national, sans affecter le fonctionnement normal du réseau ou la qualité du service offert aux utilisateurs.

L'Autorité de régulation des communications électroniques et des postes est chargée d'assurer le suivi de l'exécution par les opérateurs des obligations mises à leur charge en application du présent arrêté. L'Autorité de régulation des communications électroniques et des postes peut prononcer des sanctions à l'encontre des opérateurs de communications électroniques ne respectant pas les obligations mises à leurs charges dans les conditions prévues à l'article 31 de la loi n°2012-018 sur les communications électroniques.

Article 12 : Information de l'auteur du signalement

Les décisions suivantes sont immédiatement notifiées à travers la plateforme, selon le cas, à l'auteur de signalement :

- le rejet du signalement ;

- la décision de blocage du ou des sites ou contenus visés dans le signalement.

L'absence de toute notification dans un délai de sept (07) jours équivaut à un rejet de la demande.

Article 13 : Mise à disposition de la liste des sites et contenus malveillants ou illégaux

Avant la fin du mois de février de chaque année, l'Agence nationale de cybersécurité adresse à ses ministères de tutelle un rapport d'activité présentant le bilan de l'exécution du présent arrêté et publie sur son site internet une version confidentialisée de ce rapport.

L'Agence nationale de cybersécurité met à disposition et actualise sur la plateforme la liste des sites et contenus illégaux ou malveillants dont le blocage a été ordonné.

Article 14 : Connexion à la plateforme et notification

L'Agence nationale de cybersécurité et en son sein le CERT désignent chacun une ou plusieurs personne(s) qualifiée(s) dans un délai de vingt jours à compter de la date de l'entrée en vigueur du présent arrêté.

Dans un délai de trois mois à compter de la date de l'entrée en vigueur du présent arrêté, le CERT :

- met à disposition des personnes qualifiées et du personnel désigné par le ministre chargé de l'économie numérique, l'Agence nationale de cybersécurité, l'Autorité de régulation des communications électroniques et des postes et les opérateurs de communications électroniques, les moyens techniques leur permettant d'accéder à la plateforme en vue d'exécuter leurs obligations au titre du présent arrêté ;
- leur dispense les formations nécessaires à l'utilisation de la plateforme.

Le CERT apporte aux personnes visées à l'alinéa précédent l'assistance nécessaire en cas de difficultés liées à l'utilisation de la plateforme.

Toute notification prévue en application du présent arrêté est valablement adressée par voie électronique à travers la plateforme.

Article 15 : Interruption des blocages

Toute personne intéressée peut demander à l'Agence nationale de cybersécurité l'interruption d'une mesure de blocage d'un site ou d'un contenu si elle démontre que le contenu litigieux a été définitivement supprimé.

L'Agence nationale de cybersécurité dispose d'un délai de trente jours pour répondre à la demande par une décision motivée. Ce délai est prorogé en cas de demande d'information supplémentaire adressée à l'auteur du recours. L'absence de toute réponse dans ce délai équivaut à un rejet de la demande.

Article 16 : Recours

Les décisions de blocage visées au présent arrêté peuvent faire l'objet d'un recours gracieux auprès du ministre chargé de l'économie numérique et d'un recours contentieux devant la chambre administrative du tribunal de grande instance de Lomé dans un délai de deux mois.

En cas de recours gracieux, le Ministre chargé de l'économie numérique dispose d'un délai de trente jours pour répondre à la demande par une décision motivée. Ce délai est prorogé en cas de demande d'information supplémentaire adressée à l'auteur du recours. Le recours n'est pas suspensif de la décision de blocage. Le silence pendant un délai de trente jours équivaut à un rejet de la demande.

Article 17 : Exécution

Le secrétaire général du ministère de l'économie numérique et de la transformation digitale, le secrétaire général du ministère de la sécurité et de la protection civile, le directeur général de l'Agence nationale de cybersécurité et le directeur général de l'Autorité de régulation des communications électroniques et des postes sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté qui sera publié au journal officiel de la République Togolaise.

Fait à Lomé, le 06 SEPT 2024

Le Ministre de la Sécurité
et de la Protection Civile

SIGNE

Amb. Calixte Batossie MADJOULBA

Le Ministre de l'Economie Numérique
et de la Transformation Digitale

SIGNE

Cina LAWSON

AMPLIATIONS

CAB/MENTD 1
CAB/ MSPC..... 1
ARCEP..... 1
ANCy..... 1
CERT 1
OPERATEURS 1
JORT..... 1

Pour ampliation,
Le Secrétaire général

Tidjani KASSIME