



QUATRE-VINGT-SEIZIEME SESSION ORDINAIRE DU CONSEIL DES MINISTRES

Freetown, 16 - 17 juillet 2026.

DIRECTIVE C/DIR.2/7/26 RELATIVE À LA LUTTE CONTRE LA CYBERCRIMINALITÉ

LE CONSEIL DES MINISTRES,

VU le Traité révisé de la CEDEAO tel qu'amendé, notamment en ses articles 10, 11 et 12 portant création du Conseil des Ministres et définissant sa composition et ses fonctions ;

VU ledit Traité en ses articles 27, 32 et 33 relatifs à la science et à la technologie, et aux domaines des communications et des télécommunications;

VU le Traité révisé en son article 57 relatif à la coopération judiciaire et juridique qui prescrit que chaque Etat membre s'engagent à promouvoir la coopération judiciaire en vue d'harmoniser les systèmes judiciaires et juridiques;

VU la Convention A/P1/7/92 relative à l'entraide judiciaire en matière pénale ;

VU la Convention A/P1/8/94 relative à l'extradition ;

VU l'Acte additionnel A/SA.1/01/07 de la CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication (TIC);

VU l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO;

VU l'Acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO ;

CONSIDÉRANT la coopération existante entre chaque Etat membre de la CEDEAO en matière de police pénale, qui prévoit la mise en commun des expertises et le partage des expériences par les services de sécurité en vue d'établir des méthodes efficaces d'enquête et de répression ;

CONSIDÉRANT EGALEMENT que les développements technologiques rapides, notamment l'évolution des systèmes informatiques, des réseaux et des services numériques, ont créé de nouvelles formes de conduite criminelle et amplifié les menaces existantes à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes ;

NOTANT que les meilleures pratiques régionales et mondiales en matière de lutte contre la cybercriminalité ont considérablement progressé depuis l'adoption de la Directive C/DIR.1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, nécessitant que la CEDEAO mette à jour son cadre en fonction de ces évolutions ;

CONSCIENT de la nécessité de doter la Communauté d'outils juridiques modernes, harmonisés et robustes afin de prévenir, détecter, enquêter et poursuivre efficacement la cybercriminalité, et de renforcer la confiance dans les technologies numériques ;

DESIREUX de veiller à ce que le cadre juridique de la CEDEAO reste aligné sur l'évolution des normes internationales, tout en reflétant les besoins et priorités spécifiques de la région ;

SUR RECOMMANDATION de la réunion des Ministres en charge des télécommunications / TIC et de la Digitalisation tenue à Freetown en Sierra Leone le 27 mars 2026.

APRES AVIS du Parlement lors de sa première session ordinaire tenue à Abuja du 04 au 17 mai 2026.

PRESCRIT :

CHAPITRE PREMIER – DÉFINITIONS

Article 1^{er} - Définitions

Aux fins de la présente Directive, on entend par :

1. « **accès** » obtenir l'accès à tout ou partie d'un système informatique, que ce soit ou non en permettant l'entrée, le contrôle ou le droit d'utiliser tout ou partie de ce système informatique ;
2. « **accès à un programme informatique ou à des données informatiques** » l'accès à tout programme informatique ou à toute donnée informatique stockés dans un système informatique, obtenu en amenant ce système à exécuter une fonction quelconque permettant à une personne :
 - a. altère, modifie ou efface le programme informatique ou les données informatiques, ou tout aspect ou attribut lié au programme informatique ou aux données informatiques ; ou
 - b. copies, transferts ou déplacements vers-
 - i. tout système informatique, appareil ou support de stockage de données informatiques autre que celui qui le contient ; ou
 - ii. à un autre emplacement dans le même système informatique, appareil ou support de stockage de données informatiques dans lequel il est stocké ; ou
 - c. l'utilise ; ou
 - d. le fait sortir du système informatique dans lequel il est stocké, que ce soit par affichage ou de toute autre manière ;

et les références à l'accès à un programme informatique ou à des données informatiques (et à une intention de sécuriser un tel accès) doivent être interprétées en conséquence.

Aux fins du paragraphe (c) ci-dessus, une personne utilise un programme si la fonction qu'elle fait exécuter au système informatique :

- i. provoque l'exécution du programme informatique ; ou
- ii. est elle-même une fonction du programme informatique.

Aux fins du paragraphe (d) ci-dessus :

- i. Un programme informatique est considéré comme produit si les instructions qui le composent sont produites ; et
 - ii. La forme sous laquelle ces instructions ou toutes autres données informatiques sont produites (et en particulier la question de savoir si elles représentent ou non une forme sous laquelle, dans le cas des instructions, elles peuvent être exécutées ou, dans le cas des données, elles peuvent être traitées par un système informatique) est sans importance ;
3. « **infrastructure critique** » tout système informatique, programme informatique, donnée informatique ou actif informatique, physique ou virtuel, d'une importance telle pour l'État membre que son indisponibilité ou sa destruction aurait des conséquences graves sur la sécurité intérieure ou frontalière, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou toute combinaison de ces éléments. Elle inclut également tout autre système informatique, programme informatique, donnée informatique ou actif informatique désigné comme infrastructure d'information critique par l'autorité compétente en vertu de la législation de l'État membre. Les infrastructures critiques peuvent inclure des infrastructures d'information critiques.
4. « **enfant** » : tout être humain âgé de moins de dix-huit (18) ans.
5. « **données informatiques** » désigne toute représentation de faits, d'informations ou de concepts sous une forme adaptée au traitement dans un système informatique ;
6. « **Support de stockage de données informatiques** » désigne tout dispositif, physique ou virtuel, contenant, conçu pour contenir ou permettant le stockage de données, disponibles sous une forme unique, distribuée ou décentralisée, destinées à être utilisées par un système informatique, à partir duquel des informations peuvent être extraites ou reproduites ; toute référence à un programme informatique ou à des données informatiques contenues dans un système informatique inclut les références à tout programme informatique ou à toute donnée informatique contenue sur un support de stockage amovible qui se trouve temporairement dans le système informatique ; et un système informatique est

considéré comme contenant tout programme informatique ou toute donnée informatique contenue sur un tel support.

7. « **programme informatique** » désigne des données informatiques représentant des instructions ou des déclarations qui, lorsqu'elles sont exécutées dans un système informatique, amènent ce système informatique à exécuter une fonction, et les références à un programme informatique incluent les références à une partie d'un programme informatique ;
8. « **système informatique** » désigne tout appareil ou groupe d'appareils interconnectés ou liés, dont un ou plusieurs, conformément à un programme informatique, effectuent un traitement automatique de données informatiques ;
9. « **confiscation** », qui comprend la déchéance le cas échéant, désigne la privation permanente de biens par ordre d'un tribunal ou d'une autre autorité compétente ;
10. « **données de contenu** » désigne la substance, la portée ou la signification d'une communication spécifiée qui est interceptée en vertu des articles 33 et 43 de la présente Directive ;
11. « **appareil** » comprend :
 - i. dispositif physique ou virtuel ;
 - ii. tout outil électronique ou virtuel qui n'est pas sous forme physique ;
 - iii. tout programme informatique ou données informatiques conservées sous forme électronique ;
 - iv. un mot de passe, un code d'accès ou des données similaires, sous forme électronique ou autre, permettant d'accéder à tout ou partie d'un système informatique ; ou
 - v. dispositifs, programmes informatiques ou systèmes informatiques automatisés, auto-exécutables, adaptatifs ou autonomes ;
12. « **urgence** » une situation dans laquelle il existe un risque important et imminent pour la vie ou la sécurité de toute personne physique ;
13. « **intercepter** », aux fins de :
 - i. Article 3, écouter ou enregistrer une fonction d'un système informatique, ou en acquérir la substance, la signification ou la portée ; et
 - ii. Articles 33 et 43, collecte, enregistrement ou acquisition de données de contenu ;
14. « **gel** » ou « **saisie** » signifie interdire temporairement le transfert, la conversion, la disposition ou le déplacement de biens ou prendre temporairement la garde ou le contrôle de biens sur la base d'une ordonnance émise par une autorité judiciaire ou autre autorité compétente ;

15. « **produits du crime** » désigne tout bien provenant ou obtenu, directement ou indirectement, par la commission d'une infraction ;
16. « **édition** » comprend :
- i. distribuer, transmettre, diffuser, faire circuler, livrer, afficher, exposer, prêter à but lucratif, échanger, troquer, vendre ou proposer à la vente, louer ou proposer à la location, offrir de toute autre manière, ou mettre à disposition de toute manière ;
 - ii. imprimer, copier ou fabriquer de toute autre manière (de même nature ou de nature différente) dans le but d'accomplir l'un des actes visés au sous-paragraphe (i).
17. « **infraction sous-jacente** » toute infraction ayant généré des produits susceptibles de faire l'objet d'une infraction au sens de l'article 21 de la présente Directive ;
18. « **Contenu raciste et xénophobe** » désigne tout document écrit (qu'il soit numérique, électronique ou sous toute autre forme), toute image ou toute autre représentation d'idées ou de théories, qui prône, promeut ou incite à la haine, à la discrimination ou à la violence contre un individu ou un groupe d'individus, en raison de leur race, couleur, ascendance ou origine nationale ou ethnique, ainsi que de leur religion si celle-ci est utilisée comme prétexte pour l'un de ces facteurs.
19. « **Saisir** » le pouvoir de :
- i. saisir ou sécuriser de manière similaire un système informatique ou une partie de celui-ci, ou un support de stockage de données informatiques ;
 - ii. faire et conserver une copie d'un programme informatique ou de données informatiques,
 - iii. maintenir l'intégrité du programme informatique ou des données informatiques stockées concernées ;
 - iv. rendre inaccessibles ou supprimer des programmes informatiques ou des données informatiques dans le système informatique consulté ; et
 - v. obtenir les données de sortie d'un système informatique.
20. « **fournisseur de services** » :
- i. une entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; et
 - ii. toute autre entité qui traite ou stocke des données informatiques pour le compte de cette entité ou de ces utilisateurs.
21. « **Informations sur l'abonné** » désigne toute information contenue sous forme de données informatiques ou sous toute autre forme détenue par un fournisseur de

services, relative aux abonnés de ses services, autre que les données de trafic ou les données de contenu, permettant d'établir :

- i. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la durée du service ;
- ii. l'identité de l'abonné, son adresse postale, son adresse électronique géographique, son numéro de téléphone et autres numéros d'accès, ses informations de facturation et de paiement, disponibles sur la base du contrat ou de l'accord de service ; ou
- iii. toute autre information relative au site d'installation des équipements de communication, disponible sur la base du contrat ou de l'accord de service ; et

22. « **données de trafic** » toutes les données informatiques relatives à une communication effectuée au moyen d'un système informatique, générées par un système informatique faisant partie de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille, la durée ou le type de service sous-jacent de la communication.

CHAPITRE II – INFRACTIONS CYBERCRIMINELLES

Article 2 – Accès non autorisé

1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national, l'acte intentionnel d'amener un système informatique à exécuter une fonction quelconque dans le but d'obtenir l'accès à tout ou partie d'un système informatique, d'un programme informatique ou de données informatiques, ou de permettre qu'un tel accès soit obtenu, lorsque :
 - a. l'accès que l'on souhaite sécuriser, ou que l'on peut rendre possible, n'est pas autorisé ; et
 - b. au moment où la personne fait exécuter la fonction au système informatique, elle sait que l'accès qu'elle entend sécuriser, ou permettre de sécuriser, n'est pas autorisé.
2. Aux fins du paragraphe 1 du présent article, tout accès, de quelque nature que ce soit, par toute personne à un système informatique, à un programme informatique ou à des données informatiques est considéré comme non autorisé si :
 - a. cette personne n'est pas autorisée à contrôler l'accès de ce type particulier au système informatique, au programme informatique ou aux données informatiques ; et

- b. cette personne ne dispose pas du consentement de la personne habilitée à accorder ce consentement, pour le type d'accès en question ; ou
 - c. si cette personne a outrepassé l' autorisation , le droit ou le consentement visées au paragraphe 2 alinéas a. et b. du présent article.
- 3. L'intention visée au paragraphe 1 du présent article n'a pas à se rapporter à, ni à être dirigée vers :
 - a. tout programme informatique ou données informatiques particuliers ;
 - b. un programme informatique ou des données informatiques de toute nature ; ou
 - c. un programme informatique ou des données informatiques stockées dans un système informatique particulier.
- 4. Le paragraphe 1 du présent article ne s'applique pas lorsque l'accès est effectué en vertu d'une autorité légale, d'une ordonnance judiciaire, d'un mandat ou de l'exercice légitime des pouvoirs prévus par le droit national.
- 5. Aux fins du présent article, l'absence d'autorisation comprend les cas où il peut exister une autorisation générale d'accès à un système informatique, mais où un type, une nature ou une méthode d'accès spécifique n'est pas autorisé.

Article 3 – Interception non autorisée

- 1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national, l'acte intentionnel et non autorisé d'intercepter ou de provoquer l'interception, de manière temporaire ou permanente et de manière directe ou indirecte, par des moyens techniques de tout moyen non public :
 - a. transmission de données informatiques vers, depuis ou au sein d'un système informatique ; ou
 - b. Émissions électromagnétiques d'un système informatique transportant de telles données informatiques.
- 2. Aux fins du présent article, une interception est considérée comme non autorisée lorsque la personne qui intercepte ou provoque l'interception :
 - a. n'est pas la personne responsable du système informatique concerné ;
 - b. n'est pas la personne habilitée à déterminer si une telle interception peut avoir lieu ;
 - c. n'a pas le consentement d'une personne habilitée à donner ce consentement ; et
 - d. si cette personne a outrepassé l' autorisation , le droit ou le consentement.
- 3. L'intention visée au paragraphe 1 du présent article n'a pas à se rapporter à, ni à être dirigée vers :

- a. tout système informatique , programme informatique ou donnée informatique particulier ;
 - b. un programme informatique ou des données informatiques de toute nature ; ou
 - c. un programme informatique ou des données informatiques stockées dans un système informatique particulier.
4. Aux fins du présent article, il importe peu qu'une interception non autorisée, ou tout effet escompté d'une telle interception, soit permanente ou temporaire.
5. Le paragraphe 1 du présent article ne s'applique pas lorsque l'interception est effectuée en vertu d'une autorité légale, d'une ordonnance judiciaire, d'un mandat ou de l'exercice légitime des pouvoirs prévus par le droit national.

Article 4 – Interférence non autorisée avec un programme informatique ou des données informatiques

1. Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national , l'acte d'ingérence intentionnel et non autorisé ou en provoquant une interférence non autorisée avec un programme informatique ou des données informatiques, que ce soit de manière temporaire ou permanente.
2. Aux fins du paragraphe 1 du présent article, « atteinte à un programme informatique ou à des données informatiques » signifie :
- a. l'endommagement, l'effacement, la détérioration, l'altération, l' effacement ou suppression d'un programme informatique ou des données informatiques ;
 - b. ajouter un programme informatique ou des données informatiques au contenu d'un système informatique ;
 - c. empêcher ou entraver l'accès à, ou la disponibilité de, tout programme informatique ou données informatiques ;
 - d. altérer le fonctionnement de tout programme informatique ou la fiabilité de toute donnée informatique ;
 - e. altérer l'intégrité ou le contenu de tout programme informatique ou de toute donnée informatique ;
 - f. altérer la fiabilité, la disponibilité ou la sécurité de tout programme informatique ou de toute donnée informatique ;
 - g. permettre l'exécution de l'un quelconque des actes mentionnés au paragraphe 2 alinéas a) à f) du présent article
3. Aux fins du présent article, une ingérence est considérée comme non autorisée si la personne qui la commet ou la provoque :
- a. n'est pas habilitée à déterminer si l'intervention peut être entreprise ;
 - b. n'a pas obtenu le consentement d'une personne habilitée à donner ce consentement ; et
 - c. a dépassé l' autorisation , le droit ou le consentement.

4. Toute ingérence dans les données effectuée conformément à une autorité légale, à une décision judiciaire ou à l'exercice légitime des pouvoirs prévus par le droit national sera considérée comme autorisée.
5. L'intention visée au paragraphe 1 du présent article n'a pas à se rapporter à, ni à être dirigée vers :
 - a. tout système informatique , programme informatique ou donnée informatique particulier ;
 - b. un programme informatique ou des données informatiques de toute nature ; ou
 - c. un programme informatique ou des données informatiques stockées dans un système informatique particulier.
6. Aux fins du présent article, il importe peu qu'une intervention non autorisée dans les données ou tout effet escompté d'une telle intervention soit permanente ou temporaire.
7. Le paragraphe 1 du présent article ne s'applique pas lorsque l'intervention sur les données est effectuée en vertu d'une autorité légale, d'une ordonnance judiciaire, d'un mandat ou de l'exercice légitime des pouvoirs prévus par le droit national .

Article 5 – Interférence non autorisée avec un système informatique

1. Chaque Etat membre adopte les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national, l'acte intentionnel et non autorisé d'interférer avec un système informatique ou de provoquer une interférence avec celui-ci, que ce soit de manière temporaire ou permanente.
2. Aux fins du présent article, « atteinte à un système informatique » désigne le fait de l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression d'un programme informatique ou des données informatiques de manière à provoquer :
 - a. l'entrave au fonctionnement d'un système informatique, en tout ou en partie ;
 - b. l'altération du fonctionnement, de la fiabilité ou de la sécurité d'un système informatique ;
 - c. l'entrave ou obstruction de l'accès à un système informatique ; ou
 - d. permettant l'exécution de l'un quelconque des actes visés au paragraphe 2 alinéas a) à c) du présent article .
3. Aux fins du présent article, toute intervention sur un système informatique est considérée comme non autorisée si la personne qui effectue ou provoque cette intervention :
 - a. n'est pas habilitée à déterminer si l'intervention peut être entreprise ;

- b. n'a pas obtenu le consentement d'une personne habilitée à donner ce consentement ; et
 - c. si cette personne a outrepassé l' autorisation , le droit ou le consentement.
- 4. Aucune disposition du présent article n'oblige chaque Etat membre à ériger en infraction pénale un comportement qui ne constitue qu'une ingérence mineure dans un système informatique, c'est-à-dire un comportement dont les effets sont si insignifiants ou négligeables qu'il ne cause pas, ou ne crée pas de risque de causer d'un préjudice matériel.
- 5. L'intention visée au paragraphe 1 du présent article n'a pas à se rapporter à, ni à être dirigée vers :
 - a. tout système informatique , programme informatique ou donnée informatique particulier ;
 - b. un programme informatique ou des données informatiques de toute nature ; ou
 - c. un programme informatique ou des données informatiques stockées dans un système informatique particulier.
- 6. Aux fins du présent article, il importe peu qu'une intervention non autorisée dans un système informatique, ou tout effet escompté d'une telle intervention, soit permanente ou temporaire.
- 7. Le paragraphe 1 du présent article ne s'applique pas lorsque l'intervention dans un système informatique est effectuée en vertu d'une autorité légale, d'une ordonnance judiciaire, d'un mandat ou de l'exercice légitime des pouvoirs prévus par le droit national.

Article 6 – Utilisation abusive des dispositifs

- 1. Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national , l' acte intentionnel et non autorisé de :
 - a. soit :
 - i. la fabrication, la production, la génération, l'adaptation, le transfert, l'importation, l'exportation, la distribution, le partage, la fourniture, l'offre de fourniture, la vente ou la mise à disposition de toute autre manière d'un dispositif, principalement destiné à être utilisé, dans l'intention ou la conviction qu'il soit principalement utilisé, pour commettre ou contribuer à la commission d'une infraction établie en vertu des articles 2, 3, 4 ou 5 de la présente Directive ; ou
 - ii. acquérir, obtenir ou se procurer tout dispositif, principalement destiné à être utilisé, dans l'intention ou la conviction qu'il soit principalement

utilisé, pour commettre ou aider à commettre une infraction en vertu des articles énumérés au paragraphe 1 a. (i) du présent article..

- b. posséder un nombre d'appareils déterminé par l'État membre en vertu de sa législation nationale, dans l'intention que ces appareils soient utilisés pour commettre ou aider à commettre une infraction visée aux articles énumérés au paragraphe 1 a. (i) du présent article.
2. Aux fins du présent article, le terme « dispositif » comprend :
- a. un système informatique ou une partie de celui-ci ;
 - b. un mot de passe informatique, un code d'accès ou des données similaires permettant d'accéder à tout ou partie d'un système informatique ;
 - c. tout programme informatique, y compris les logiciels malveillants, conçu ou adapté principalement dans le but de commettre une infraction établie conformément à la présente Directive.
3. Ne constitue pas une infraction au sens du présent article, la fabrication, la production, la génération, l'adaptation, le transfert, l'acquisition, l'importation, la distribution, la possession ou la mise à disposition d'un tel dispositif :
- a. non principalement conçu ou adapté dans le but de commettre une infraction établie conformément à la présente Directive;
 - b. entrepris à des fins de formation autorisée , de tests, d'analyse de réseau, de protection d'un système informatique, de recherche et développement, ou pour toute autre utilisation légitime similaire ; ou
 - c. entrepris conformément à un mandat judiciaire, à une autorisation légale ou à tout autre exercice légitime de pouvoir en vertu du droit national.

Article 7 – Faux et usage de faux informatiques

1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national , l'acte intentionnel et non autorisé de l'introduction, l'altération, l'effacement et la suppression ou dissimulation des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient considérées ou utilisées à des fins juridiques comme si elles étaient authentiques, que les données soient ou non directement lisibles ou intelligibles.
2. Chaque État membre peut prendre des mesures pour garantir la prise en compte des circonstances aggravantes, notamment lorsque l'infraction établie conformément au paragraphe 1 du présent article est commise de manière malhonnête ou avec une intention similaire en vue d'un gain illicite, d'une perte illicite ou d'un avantage économique pour soi-même ou pour autrui.

Article 8 – Fraude informatique

1. Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national, le comportement de toute personne, par un acte non autorisé qui entraîne, en tout ou en partie, la perte de données, de programmes, de biens, de valeurs mobilières, de contreparties ou de systèmes informatiques, qui, avec une intention frauduleuse ou malhonnête, procure :
 - a. un gain illicite ;
 - b. une perte injustifiée; ou
 - c. tout avantage économique pour soi-même ou pour une autre personne.
2. Aux fins du paragraphe 1 du présent article, le terme « acte » comprend notamment :
 - a. tout accès non autorisé à un système informatique, à un programme informatique ou à des données informatiques ;
 - b. toute l'introduction, l'altération, l'effacement, la suppression ou génération de tout programme informatique ou de données informatiques ;
 - c. toute interférence, entrave, altération ou obstruction au fonctionnement d'un système informatique ; ou
 - d. copier, transférer ou déplacer des données informatiques ou un programme informatique vers un système informatique, un appareil ou un support de stockage autre que celui dans lequel il est légalement détenu, ou vers un emplacement différent au sein de ce système, appareil ou support de stockage ; ou
 - e. en utilisant ces données informatiques ou ce programme informatique ; ou
 - f. obtenir toute donnée informatique ou tout résultat de programme informatique provenant du système informatique qui la contient, que ce soit par affichage ou par tout autre moyen ; ou
 - g. toute tromperie relative à des circonstances factuelles commise au moyen d'un système informatique et qui amène une personne à faire ou à omettre de faire quelque chose qu'elle n'aurait pas fait ou omis de faire autrement.

Article 9 – Infractions contre les infrastructures critiques

Chaque État membre prend des mesures pour garantir que des circonstances aggravantes s'appliquent lorsqu'une infraction prévue au Chapitre II de la présente Directive, ou tout autre comportement prescrit par chaque État membre, y compris toute action entraînant des dommages matériels, est commise contre une infrastructure critique.

Article 10 - Infractions liées à la diffusion en ligne de contenus pédopornographiques ou d'exploitation sexuelle d'enfants

1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national, l'acte intentionnel de :
 - a. publier du matériel d'abus sexuels ou d'exploitation sexuelle d'enfants par le biais d'un système informatique ;
 - b. produire du matériel d'abus ou d'exploitation sexuelle d'enfants en vue de sa publication par le biais d'un système informatique ;
 - c. posséder ou contrôler du matériel pédopornographique ou d'exploitation sexuelle d'enfants dans un système informatique ou sur un support de stockage de données informatiques
 - d. solliciter, se procurer ou accéder à du matériel d'abus sexuels ou d'exploitation sexuelle d'enfants par le biais d'un système informatique ;
 - e. diffuser, distribuer ou rendre accessible de toute autre manière du matériel relatif à la maltraitance ou à l'exploitation sexuelle d'enfants par le biais d'un système informatique ; ou
 - f. financer les infractions établies conformément au paragraphe 1 alinéas a. à e. du présent article.
2. Aux fins du présent article , « matériel d'abus sexuel ou d'exploitation sexuelle d'enfants » comprend le matériel visuel et peut comprendre du contenu écrit ou audio qui décrit ou représente :
 - a. un enfant se livrant à une conduite sexuellement explicite réelle ou simulée ;
 - b. un enfant en présence d'une personne se livrant à une activité sexuelle quelconque ;
 - c. un enfant ou une personne qui s'avère être un enfant dont les parties sexuelles sont exposées à des fins principalement sexuelles ;
 - d. un enfant soumis à la torture ou à des traitements ou peines cruels, inhumains ou dégradants et dont le contenu est de nature sexuelle ;
 - e. une personne qui s'avère être un enfant et qui se livre à des actes sexuels explicites ; ou
 - f. images réalistes représentant un enfant se livrant à une activité sexuelle explicite.
3. Chaque État membre peut exiger que les matières visées au paragraphe 2 du présent article soient limitées aux matières qui :
 - a. représente, décrit ou illustre une personne existante ; ou
 - b. représente visuellement des abus sexuels ou de l'exploitation sexuelle d'enfants.
4. Conformément à son droit national et aux obligations internationales applicables, chaque État membre peut prendre des mesures pour ne pas pénaliser :
 - a. la conduite des enfants concernant du contenu auto-produit les représentant ;
ou

- b. la production, la transmission ou la possession consensuelles de matériel décrit au paragraphe 2 alinéas (a) à (c) du présent article, lorsque la conduite sous-jacente décrite est légale telle que déterminée par le droit national, et lorsque ce matériel est conservé exclusivement pour l'usage privé et consensuel des personnes concernées.
- 5. Aucune disposition de la présente Directive ne porte atteinte aux obligations internationales qui sont plus favorables à la protection des droits de l'enfant.

Article 11 – Sollicitation ou incitation en vue de commettre une infraction sexuelle contre un enfant

Chaque État membre adopte les mesures nécessaires pour ériger en infractions pénales, en vertu de leur droit national, l'acte intentionnel de communiquer, de solliciter, d'approcher ou de prendre des dispositions, au moyen d'un système informatique, avec un enfant, dans le but de commettre une infraction sexuelle à l'encontre de ce mineur, y compris la commission de toute infraction établie conformément à l'article 10 de la présente Directive.

Article 12 – Diffusion non consensuelle d'images intimes

1. Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale le fait de publier intentionnellement, au moyen d'un système informatique, une image intime d'une personne, sans le consentement de la personne représentée sur l'image.
2. Aux fins du paragraphe 1 du présent article, « image intime » désigne tout enregistrement visuel d'une personne, qu'il s'agisse d'une photographie, d'une vidéo ou d'une autre représentation réalisée par quelque moyen que ce soit, qui est de nature sexuelle ou dans lequel la personne est nue, partiellement nue, se livre à une activité sexuelle ou est représentée dans des circonstances où une attente raisonnable de vie privée existait au moment de l'infraction.
3. Chaque État membre prévoit que la responsabilité pénale exige les éléments intentionnels suivants :
 - a. la divulgation a été faite intentionnellement ou par imprudence quant au préjudice émotionnel et à la détresse qui pourraient être causés à la victime ; ou
 - b. La divulgation a été faite dans l'intention d'obtenir un gain indu ou de causer un préjudice indu.
4. Chaque État membre reconnaît comme moyens de défense ou exceptions lorsque :
 - a. la personne représentée a consenti volontairement à la divulgation ;
 - b. la divulgation a été faite de bonne foi à des fins d'application de la loi, judiciaires ou médicales ; ou
 - c. L' image a été légalement mise à disposition dans un contexte commercial.

5. Chaque État membre étend l'infraction aux menaces de diffusion d'une image intime sans consentement.

CHAPITRE III - AUTRES INFRACTIONS

Article 13 – Cyberharcèlement

1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale le fait de poursuivre intentionnellement, au moyen d'un système informatique, une conduite qui s'apparente à du harcèlement d'une autre personne.
2. Aux fins du paragraphe 1 du présent article, une « ligne de conduite » peut comprendre un ou plusieurs des actes suivants, qu'ils soient commis directement ou indirectement, et lorsqu'ils sont exécutés de façon répétée ou systématique.
 - a. contacter, ou tenter de contacter, une personne par tout moyen électronique, y compris le courrier électronique, les SMS, les médias sociaux ou les communications par Internet ;
 - b. publier ou faire publier tout document relatif à une personne ou censé s'y rapporter, ou censé provenir d'une personne ;
 - c. surveillance de l'utilisation par une personne d'un système informatique ou de toute forme de communication électronique ;
 - d. interférer avec, endommager ou accéder à un bien en possession d'une personne; ou
 - e. transmettre ou laisser, directement ou indirectement, des documents offensants ou menaçants à une personne.
3. Aux fins du paragraphe 2 du présent article, chaque État membre détermine, conformément à son droit national, le nombre d'occurrences ou les circonstances qui constituent un comportement « répété » ou « systématique ».
4. Chaque État membre prévoit que la responsabilité pénale exige les éléments intentionnels suivants :
 - a. ce comportement a été adopté dans l'intention de harceler, d'intimider, de tourmenter ou d'embarrasser ;
 - b. la personne savait, ou aurait dû savoir, que sa conduite constituerait un harcèlement; et

- c. Ce comportement visait à susciter la crainte pour la sécurité de la personne concernée ou de toute personne de son entourage.
- 5. Chaque État membre Chaque Etat membre veille à ce que l'infraction établie en application du paragraphe 1 du présent article produise les effets suivants :
 - a. amener raisonnablement la personne, compte tenu de toutes les circonstances, à craindre pour sa sécurité ou celle d'autrui ;
 - b. provoquer chez la personne l'appréhension ou la crainte de violences à son encontre, à l'encontre d'une autre personne ou à l'encontre de ses biens ; ou
 - c. causer un préjudice, raisonnablement dû compte tenu de toutes les circonstances, à la santé, à la réputation, aux relations ou à la carrière de la personne.
- 6. Chaque État membre Chaque Etat membre reconnaît comme moyens de défense ou exceptions lorsque :
 - a. cette conduite a été entreprise dans le but de prévenir ou de détecter un crime ;
 - b. la conduite était autorisée par la loi ou effectuée conformément à une exigence légale ;
 - c. la conduite était raisonnable dans les circonstances ; ou
 - d. la conduite a été raisonnable dans le cadre d'un commerce, une activité professionnelle ou une occupation licite, ou aux fins d'obtenir ou de fournir des informations dans lesquelles la personne a un intérêt légitime.
- 7. Chaque État membre Chaque Etat membre peut prévoir que des circonstances aggravantes sont établies lorsque :
 - a. la victime est un enfant ;
 - b. l'infraction a été commise dans le cadre d'une relation intime ou fondée sur la confiance ; ou
 - c. Ce comportement a causé un préjudice important à la santé, à la sécurité ou au bien-être de la victime.

Article 14 – Cyberintimidation

- 1. Chaque État membre adopte les mesures nécessaires pour ériger en infraction pénale le fait de se livrer intentionnellement, au moyen d'un système informatique, à des actes d'intimidation, de harcèlement ou de brimades à l'encontre d'une autre personne, lorsque ces actes sont commis de manière répétée ou systématique.
- 2. Aux fins du présent article, chaque État membre détermine, conformément son droit national, le nombre d'occurrences ou les circonstances qui constituent un comportement « répété » ou « systématique ».

3. Chaque État membre veille à ce que la responsabilité pénale comprenne des éléments moraux liés aux éléments suivants :
 - a. la personne savait, ou aurait dû savoir, que ce comportement causerait du harcèlement ou une détresse émotionnelle importante ;
 - b. le comportement a été adopté de manière imprudente, sans se soucier de savoir s'il causerait du harcèlement, de l'intimidation ou de la détresse ; ou
 - c. Ce comportement visait à susciter la crainte pour la sécurité de la personne ou d'autrui.
4. Chaque État membre exige, en application du paragraphe 1 du présent article que produise les effets suivants, tout acte qui :
 - a. amène cette autre personne, compte tenu de toutes les circonstances, à craindre raisonnablement pour sa sécurité ou celle de toute personne qu'elle connaît ;
 - b. cause à cette autre personne ou à toute autre personne du harcèlement, de l'inquiétude ou de la détresse; ou
 - c. amène cette autre personne, de manière raisonnable compte tenu de toutes les circonstances, à craindre des violences ou des dommages à une personne ou à un bien.
5. Chaque État membre reconnaît comme moyens de défense ou exceptions lorsque la conduite :
 - a. a été entreprise dans le but de prévenir ou de détecter un crime ;
 - b. était autorisée par la loi ou effectuée conformément à une exigence légale ;
 - c. était raisonnable dans les circonstances; ou
 - d. a été raisonnable dans le cadre d'un commerce, une activité professionnelle ou une occupation licite , ou aux fins d'obtenir ou de fournir des informations dans lesquelles la personne a un intérêt légitime.
6. Chaque État membre peut prévoir que des circonstances aggravantes sont établies lorsque :
 - a. la victime est un enfant ;
 - b. l'infraction a été commise dans le cadre d'une relation intime ou fondée sur la confiance; ou
 - c. Ce comportement a causé un préjudice important à la santé, à la sécurité ou au bien-être de la victime.

Article 15 – Divulgateion non autorisée

Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national, la divulgation intentionnelle et non autorisée, au moyen d'un système informatique, de toute information :

- a. données informatiques; ou
- b. tout mot de passe, code d'accès ou tout autre moyen permettant d'accéder à un programme informatique ou à des données informatiques stockées dans un système informatique.

Article 16 – Diffusion de contenus racistes et xénophobes par le biais de systèmes informatiques

Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de leur droit national, le comportement de toute personne qui diffuse intentionnellement ou met autrement à la disposition du public, par le biais d'un système informatique, des contenus racistes ou xénophobes.

Article 17 – Menace à motivation raciste et xénophobe

1. Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national, le comportement de toute personne qui, intentionnellement, au moyen d'un système informatique, menace de commettre une infraction grave à l'encontre d'une personne ou d'un groupe de personnes au motif qu'elles appartiennent à un groupe caractérisé par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ainsi que par la religion, lorsque la religion est utilisée comme prétexte pour l'un de ces facteurs.
2. Aux fins du présent article, chaque État membre peut déterminer ce qui constitue une « infraction grave » en vertu de son droit national.

Article 18 – Insulte à caractère raciste et xénophobe

Chaque État membre peut adopter les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national, le comportement de toute personne qui, intentionnellement et publiquement, par le biais d'un système informatique, insulte une personne ou un groupe de personnes au motif qu'elles appartiennent à un groupe distingué par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ainsi que par la religion, lorsque la religion est utilisée comme prétexte pour l'un de ces facteurs.

Article 19 – Nier, minimiser grossièrement, approuver ou justifier le génocide ou les crimes contre l'humanité

Chaque État membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de son droit national, le comportement de toute personne qui, dans l'intention

d'inciter à la haine, à la discrimination ou à la violence contre un individu ou un groupe d'individus pour des raisons de race, de couleur, d'ascendance, d'origine nationale ou ethnique, ou de religion lorsque celle-ci est utilisée comme prétexte pour l'un de ces facteurs, diffuse ou met à la disposition du public, par le biais d'un système informatique, tout contenu qui nie, minimise grossièrement, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité tels que définis par le droit international.

Article 20 – Violation du droit d’auteur et des droits voisins

Chaque Etat membre prend les mesures nécessaires pour ériger en infractions pénales, en vertu de son droit national, la violation du droit d'auteur et de tout droit voisin, tel que défini par le droit de l'Etat membre, lorsque ces actes sont commis intentionnellement, à une échelle commerciale et au moyen d'un système informatique, conformément à leurs obligations internationales.

Article 21 – Blanchiment des produits du crime

1. Chaque Etat membre adopte, conformément aux principes fondamentaux de droit national son droit national, les mesures nécessaires pour ériger en infractions pénales les actes commis intentionnellement :

- a. la conversion ou le transfert de biens, sachant que ces biens proviennent d'un crime, dans le but de dissimuler ou de masquer l'origine illicite des biens ou d'aider toute personne impliquée dans la commission de l'infraction sous-jacente à se soustraire aux conséquences juridiques des actes de cette personne ;
- b. le fait de dissimuler ou de masquer la véritable nature, la source, l'emplacement, la disposition, le mouvement ou la propriété d'un bien, ou les droits s'y rapportant, en sachant que ce bien provient d'un crime.

2. Sous réserve des principes fondamentaux de son système juridique :

- a. l'acquisition, la possession ou l'utilisation d'un bien, sachant, au moment de sa réception, que ce bien provient d'un crime ;
- b. la participation à, l'association à ou le complot en vue de commettre, les tentatives de commettre et le fait d'aider, d'encourager, de faciliter et de conseiller la commission de l'une des infractions établies conformément au présent article.

3. Aux fins de la mise en œuvre ou de l'application du paragraphe 1 du présent article :

- a. Chaque Etat membre doit établir comme infractions sous-jacentes les infractions pertinentes établies conformément au Chapitre II de la présente Directive ;

- b. Dans le cas des États membres dont la législation établit une liste d'infractions sous-jacentes spécifiques, ils doivent, à tout le moins, inclure dans cette liste un éventail complet d'infractions établies conformément au Chapitre II de la présente Directive ;
- c. Aux fins du paragraphe 3 alinéa b. du présent article, les infractions sous-jacentes comprennent les infractions commises tant à l'intérieur qu'à l'extérieur du territoire de l'État membre concerné.
- d. les infractions commises hors du territoire d'un État membre ne constituent des infractions sous-jacentes que si :
 - i. le comportement en question constitue une infraction pénale en vertu du droit national de l'État où il est commis
 - ii. et constitue une infraction pénale en vertu du droit national de l'État membre qui met en œuvre ou applique le présent article, s'il y avait été commis ;
- e. Chaque Etat membre fournit à la Commission de la CEDEAO une copie de ses lois donnant effet au présent article et de toute modification ultérieure de ces lois ou une description de celles-ci ;
- f. Si les principes fondamentaux du droit national d'un État membre l'exigent, il peut être prévu que les infractions visées au paragraphe 1 du présent article ne s'appliquent pas aux personnes qui ont commis l'infraction sous-jacente ;
- g. La connaissance, l'intention ou le but requis comme élément constitutif d'une infraction énoncée au paragraphe 1 du présent article peuvent être déduits de circonstances factuelles objectives.

Article 22 – Catégories particulières de cybercriminalité impliquant des technologies émergentes

1. Chaque Etat membre peut adopter les mesures nécessaires pour garantir que les infractions de cybercriminalité commises au moyen ou facilitées par les technologies émergentes, notamment l'intelligence artificielle, les systèmes d'apprentissage automatique, l'informatique quantique, les plateformes blockchain, les technologies deepfake et les systèmes autonomes, soient reconnues et criminalisées en vertu du droit national.
2. Chaque Etat membre peut qualifier d'infraction aggravée et l'exposer à des peines renforcées, conformément à son droit national, toute infraction prévue au Chapitre II de la présente Directive lorsqu'elle est commise au moyen de technologies émergentes qui sont conçus ou adaptés principalement pour faciliter la commission d'une infraction prévue au Chapitre II de la présente Directive, de la manière suivante qui :
 - a. masque l'identité ou le lieu où se trouve l'auteur des faits ;
 - b. amplifie l'ampleur, la vitesse ou l'impact de l'infraction
 - c. cible les infrastructures critiques, les institutions démocratiques ou les populations vulnérables ; ou

- d. implique des systèmes automatisés ou autorépliatifs capables de causer des dommages considérables.
- 3. Chaque Etat membre peut mettre en place des mécanismes pour suivre l'évolution des technologies émergentes, actualiser en conséquence sa législation nationale en matière de cybercriminalité et les protocoles d'application pertinents, et veiller à ce que les autorités chargées de l'application de la loi et les autorités judiciaires reçoivent une formation appropriée en matière de détection, d'enquête et de poursuite des infractions impliquant ces technologies.
- 4. Les Etats membres peuvent coopérer pour harmoniser les définitions, les normes d'enquête et les approches de poursuite relatives à l'utilisation criminelle des technologies émergentes, et échangent des informations, des bonnes pratiques et une expertise technique par le biais des mécanismes de coopération de la CEDEAO.

Article 23 – Tentative et complicité

Chaque Etat membre prend les mesures nécessaires pour ériger en infraction pénale, en vertu de droit national son droit national, le comportement de toute personne qui, intentionnellement :

- a. encourage la commission de toute infraction établie conformément à la présente Directive ;
- b. aide une autre personne à commettre une telle infraction ;
- c. tente de commettre une telle infraction ; ou
- d. entreprend tout acte préparatoire ou visant à faciliter la commission d'une telle infraction.

Article 24 – Responsabilité pénale des personnes morales

- 1. Chaque Etat membre adopte les mesures nécessaires pour garantir que les personnes morales puissent être tenues responsables des infractions établies conformément à la présente Directive, lorsque ces infractions sont commises à leur profit par toute personne physique, agissant soit individuellement, soit au sein d'un organe de la personne morale, qui y occupe une position dominante, sur la base :
 - a. d'un pouvoir de représentation de la personne morale ;
 - b. d'un pouvoir de prendre des décisions au nom de la personne morale ; ou
 - c. d'une autorité permettant d'exercer un contrôle au sein de la personne morale.
- 2. Chaque Etat membre adopte les mesures nécessaires pour garantir qu'une personne morale puisse également être tenue responsable lorsque le manque de surveillance ou de contrôle exercé par une personne physique visée au paragraphe 1 du présent article a rendu possible la commission d'une infraction établie conformément à la présente Directive, au profit de cette personne morale, par une personne physique agissant sous son autorité.

3. Chaque Etat membre veille à ce que les personnes morales visées au présent article n'excluent pas les poursuites pénales contre les personnes physiques qui sont auteurs, instigateurs ou complices des infractions concernées.

Article 25 – Poursuites, jugement et sanctions

1. Chaque Etat membre veille à ce que les infractions constatées conformément à la présente Directive soient soumises à des sanctions effectives, proportionnées et dissuasives, compte tenu de la gravité de l'infraction.
2. Chaque Etat membre peut, conformément à droit nationalson droit national, prévoir des circonstances aggravantes pour de telles infractions, notamment lorsque des infrastructures critiques sont touchées.
3. Chaque Etat membre veille à ce que les poursuites et les mesures d'exécution soient menées efficacement et de manière à dissuader la commission d'infractions, tout en respectant les droits de la défense et le droit à un procès équitable.
4. Chaque Etat membre prend les mesures appropriées pour protéger les enfants accusés d'infractions établies conformément à la présente Directive, dans le respect de la Convention relative aux droits de l'enfant et des autres obligations internationales applicables.
5. Aucune disposition de la présente Directive ne porte atteinte au principe selon lequel la définition des infractions et des moyens de défense , ainsi que les règles régissant les poursuites et les sanctions, sont déterminées par le droit national .

CHAPITRE IV – DISPOSITIONS PROCÉDURALES

Article 26 – Portée des dispositions procédurales

1. Chaque Etat membre prend les mesures nécessaires pour garantir que les pouvoirs et dispositions procédurales adoptés en vertu de la présente Directive s'appliquent à :
 - a. l'enquête et la poursuite des infractions pénales établies en vertu de la présente Directive ;
 - b. l'enquête et la poursuite des autres infractions pénales commises au moyen d'un système informatique en vertu droit nationaldu droit national; et
 - c. la collecte de preuves sous forme électronique en relation avec toute infraction pénale relevant de la présente Directive ou d'une autre loi nationale.
2. Chaque Etat membre veille à ce que les preuves ne soient pas exclues au seul motif qu'elles ont été générées, transmises, saisies ou identifiées au moyen d'un système informatique.

3. Aucune disposition du présent Chapitre ne doit être interprétée comme portant atteinte ou limitant l'application des dispositions législatives existantes des États membres qui habilitent les autorités compétentes à conserver, recueillir ou utiliser des éléments de preuve, électroniques ou autres, au cours d'enquêtes et de poursuites.

Article 27 – Conditions et garanties

Chaque Etat membre veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures visés dans le présent chapitre soient soumis à des conditions et des garanties, notamment :

- a. La protection des droits de l'homme et des libertés tels que garantis par les instruments régionaux et internationaux applicables ;
- b. La supervision judiciaire ou autre supervision indépendante ;
- c. Les motifs justifiant l'application des mesures; et
- d. Les limitations quant à la portée et à la durée de ces pouvoirs.

Article 28 – Conservation accélérée des données informatiques stockées

1. Chaque Etat membre adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner ou d'obtenir par tout autre moyen la conservation rapide de données informatiques stockées, y compris les données de trafic, qui sont pertinentes aux fins d'une enquête ou d'une procédure pénale , en particulier lorsqu'il existe des raisons de croire que ces données peuvent être vulnérables à la perte ou à la modification .
2. Lorsqu'une injonction est émise en vertu du paragraphe 1 du présent article, chaque Etat membre veille à ce que le prestataire de services ou toute autre personne en possession ou contrôlant les données informatiques stockées spécifiées soit tenu de préserver et de maintenir l'intégrité de ces données pendant une période déterminée par le droit national, suffisante pour permettre aux autorités compétentes d'en demander la communication.
3. Chaque Etat membre peut prévoir que les ordonnances de conservation visées au paragraphe 2 s'appliquent pour une durée maximale de quatre-vingt (90) jours, renouvelable conformément à la législation nationale.
4. Chaque Etat membre adopte les mesures nécessaires pour obliger les prestataires de services ou autres personnes tenues de conserver des données informatiques stockées en vertu du présent article à garder confidentiel l'engagement de cette conservation pendant la période prévue par le droit national.

Article 29 – Conservation accélérée et divulgation partielle des données de trafic

1. Chaque Etat membre adopte les mesures nécessaires, en ce qui concerne les données de trafic qui doivent être conservées en vertu de l'article 28 de la présente Directive, pour garantir la conservation rapide de ces données de trafic, qu'un ou plusieurs fournisseurs de services soient impliqués ou non dans la transmission d'une communication.
2. Chaque Etat membre adopte les mesures nécessaires pour assurer la communication rapide aux autorités compétentes, ou à une personne désignée par ces autorités, d'une quantité suffisante de données de trafic permettant l'identification des fournisseurs de services et du chemin par lequel la communication ou les informations indiquées ont été transmises.

Article 30 – Ordres de production

1. Chaque Etat membre adopte les mesures nécessaires pour habilitier les autorités judiciaires ou autres autorités compétentes à ordonner à toute personne en possession ou ayant le contrôle de données informatiques spécifiées stockées dans un système informatique ou sur un support de stockage de données informatiques de produire ces données.
2. Chaque Etat membre adopte les mesures nécessaires pour habilitier les autorités judiciaires ou autres autorités compétentes à ordonner aux fournisseurs de services offrant des services sur leur territoire de fournir les informations sur les abonnés en leur possession ou sous leur contrôle.
3. Chaque Etat membre prend les mesures nécessaires pour garantir qu'une injonction de production ne puisse être délivrée que sur demande exposant, lorsque cela est raisonnable et possible, les raisons pour lesquelles il est estimé que :
 - a. Les données informatiques ou les informations sur les abonnés recherchées sont susceptibles d'être disponibles auprès d'une personne ou d'un fournisseur de services mentionné au paragraphe 1 du présent article ;
 - b. Une enquête peut être entravée ou gravement compromise si les données informatiques spécifiées ou les informations sur l'abonné ne sont pas produites ;
 - c. le type de preuve que l'on soupçonne d'être susceptible d'être produit par une personne ou un fournisseur de services mentionné au paragraphe 1 du présent article ;
 - d. Les abonnés, utilisateurs ou identifiants uniques qui font l'objet d'une enquête ou de poursuites peuvent être divulgués à la suite de la production des données informatiques ou des informations sur les abonnés spécifiées ;
 - e. une infraction identifiée est une infraction pour laquelle l'ordonnance de production est demandée ;
 - f. Les mesures prises doivent garantir que les données informatiques ou les informations sur les abonnés spécifiées seront produites tout en préservant la confidentialité des autres utilisateurs, clients et tiers.

4. Chaque Etat membre peut prendre les mesures nécessaires pour accorder aux prestataires de services le droit exprès de contester devant l'autorité judiciaire ou compétente une ordonnance de production pour des raisons de pertinence, de privilège ou d'autres objections légales à l'ordonnance ou autrement protégées contre la divulgation par la loi, ou de non-respect des exigences du présent article.

Article 31 – Perquisition et saisie de données informatiques stockées

1. Chaque Etat membre adopte les mesures nécessaires pour habilitier les autorités judiciaires ou autres autorités compétentes à ordonner ou à obtenir de manière similaire la recherche, l'accès, la saisie ou la sécurisation rapides de données, de programmes ou de systèmes informatiques, lorsqu'il existe des motifs raisonnables de croire que ces données, programmes ou systèmes informatiques sont pertinents aux fins d'une enquête ou d'une procédure pénale spécifique.
2. Chaque Etat membre adopte les mesures nécessaires pour garantir que, lorsque leurs autorités judiciaires ou autres autorités compétentes recherchent ou accèdent à un système informatique spécifique ou à une partie de celui-ci, et ont des raisons de croire que les données ou programmes informatiques recherchés sont stockés dans un autre système informatique ou une autre partie de celui-ci, et que ces données sont légalement accessibles depuis ou disponibles pour le système initial, ces autorités soient en mesure d'étendre rapidement la recherche pour obtenir l'accès à cet autre système informatique.
3. Chaque Etat membre veille à ce que ces pouvoirs soient exercés sous réserve de garanties appropriées, notamment un contrôle judiciaire ou autre contrôle indépendant, le principe de proportionnalité et des limitations à l'utilisation des données à des fins licites.
4. Chaque Etat membre prend les mesures nécessaires pour garantir qu'une ordonnance de recherche, d'accès, de saisie ou de mise en sécurité de données, de programmes ou de systèmes informatiques puisse être délivrée sur demande comportant les éléments suivants, lorsque cela est raisonnable et possible :
 - a. une explication des raisons pour lesquelles on peut croire que les éléments recherchés seront trouvés lors de l'exercice du pouvoir procédural ;
 - b. identification et description précise du type de preuves que l'on soupçonne d'être trouvées ;
 - c. identification et description précise du programme informatique ou des données informatiques recherchés, et les motifs raisonnables de soupçonner que ce programme informatique ou ces données informatiques sont disponibles sur chaque système informatique, appareil ou support de stockage de données informatiques ;
 - d. identification et description précise des systèmes informatiques, appareils ou supports de stockage de données informatiques individuels à fouiller ou à saisir,

- ainsi que les motifs raisonnables de soupçonner qu'ils contiennent le programme, les données ou les preuves pertinents ;
- e. une description des mesures techniques à prendre pour garantir que la perquisition ou la saisie soit effectuée par des méthodes médico-légales appropriées, telles que la mise en miroir ou la copie des données informatiques pertinentes, plutôt que par le retrait physique des systèmes ou appareils informatiques, sauf en cas de stricte nécessité ;
 - f. l'identification de toute personne proposée pour accompagner l'officier d'exécution, ainsi que les raisons justifiant leur présence ; et
 - g. une demande, le cas échéant, pour que l'autorité judiciaire ou compétente accompagne l'agent d'exécution lors de l'exercice du pouvoir procédural.
5. Chaque Etat membre prend les mesures nécessaires pour garantir que l'agent d'exécution, lorsqu'il exerce ce pouvoir procédural puisse :
- a. agir en toutes circonstances avec proportionnalité ;
 - b. prendre toutes les précautions nécessaires pour maintenir l'intégrité du système informatique, du programme informatique et des données informatiques faisant l'objet de la perquisition ou de la saisie ;
 - c. ne pas perturber ni entraver l'intégrité ou le fonctionnement de tout système informatique, programme informatique ou donnée informatique qui n'est pas l'objet des infractions identifiées dans la demande ;
 - d. éviter toute perturbation des activités commerciales légitimes et des locaux susceptibles d'être soumis au pouvoir procédural ;
 - e. tenir en toutes circonstances dûment compte des droits des tiers ;
 - f. éviter toute perturbation de tout système informatique, programme informatique ou donnée informatique non lié au système informatique, au programme informatique ou aux données informatiques qui ne font pas l'objet des infractions identifiées dans la demande ou qui ne sont pas nécessaires à l'enquête sur l'infraction spécifiée ; et
 - g. Ne saisir un système informatique ou un support de stockage de données informatiques que lorsqu'il est impossible de saisir ou de sécuriser de la même manière les données informatiques, ou lorsqu'il est nécessaire de garantir que les données informatiques ne seront pas détruites, altérées ou altérées de quelque manière que ce soit.
6. Chaque Etat membre prend les mesures nécessaires pour que l'agent d'exécution, lors de l'exercice de ce pouvoir procédural ou dès que possible après la perquisition :
- a. dresse une liste de ce qui a été saisi ou mis en sécurité de manière similaire, en indiquant la date et l'heure de la saisie ou de la mise en sécurité ; et
 - b. Remet une copie de cette liste à la personne qui contrôle le système informatique, le programme informatique ou les données informatiques.
7. Chaque Etat membre prend les mesures nécessaires pour garantir qu'un agent d'exécution puisse, sur demande, autoriser une personne à accéder aux données informatiques du système et les copier, ou en fournir une copie à une personne :
- a. qui a la garde ou le contrôle d'un système informatique ;

- b. qui a droit à un programme informatique ou à des données informatiques saisis ou sécurisés de manière similaire en vertu du présent article; ou
 - c. qui agit au nom d'une personne visée au paragraphe 7 alinéas a. ou b. du présent article, pour accéder et copier le programme informatique ou les données informatiques sur le système informatique ou donner à cette personne une copie du programme informatique ou des données informatiques ;
- 8. Un officier d'exécution peut refuser de donner accès aux documents saisis ou obtenus de manière similaire en application du présent article ou d'en fournir des copies s'il a des motifs raisonnables de croire que l'accès ou la fourniture de copies pourrait :
 - a. Constituer une infraction pénale; ou
 - b. porter préjudice à :
 - i. une enquête; ou
 - ii. toute poursuite.
- 9. Dans ce cas, la personne lésée peut s'adresser au tribunal compétent pour obtenir cet accès ou des copies.

Article 32 – Collecte en temps réel des données de trafic

1. Chaque Etat membre adopte les mesures nécessaires pour habilitier les autorités judiciaires ou autres autorités compétentes à :
 - a. collecter ou enregistrer, par l'application de moyens techniques sur leur territoire, des données de trafic en temps réel associées à des communications spécifiques.
 - b. contraindre un fournisseur de services, dans la limite de ses capacités techniques existantes, à :
 - i. collecter ou enregistrer, par l'application de moyens techniques sur le territoire de l'État membre, des données de trafic en temps réel associées à des communications spécifiques ; ou
 - ii. coopérer avec les autorités judiciaires ou autres autorités compétentes et leur apporter une assistance dans la collecte ou l'enregistrement de ces données de trafic.
2. Lorsque, en raison des principes de son système juridique national, un État membre ne peut adopter les mesures visées au paragraphe 1 du présent article, il peut adopter en revanche les mesures nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données de trafic associées à des communications spécifiques transmises sur son territoire, par l'application de moyens techniques sur ce territoire.
3. Chaque Etat membre prend les mesures nécessaires pour obliger les prestataires de services à garder confidentiels le fait de l'exercice de tout pouvoir prévu au présent

article, ainsi que toute information s'y rapportant, pendant la période prévue par la loi nationale.

4. L'application des mesures prévues au présent article est soumise à des conditions et garanties, notamment une autorisation judiciaire ou indépendante, la proportionnalité, la nécessité et des limitations quant à l'utilisation et à la conservation des données de trafic.
5. Chaque Etat membre prend les mesures nécessaires pour garantir qu'une ordonnance de collecte ou d'enregistrement de données de trafic ne puisse être délivrée que sur demande exposant, lorsque cela est raisonnable et possible, les raisons pour lesquelles il est estimé que :
 - a. les données de trafic recherchées seront obtenues si ce pouvoir procédural est exercé ;
 - b. le type de données de trafic que l'on soupçonne d'être trouvées ;
 - c. L'infraction identifiée est l'infraction pour laquelle le mandat est demandé ;
 - d. des divulgations supplémentaires sont nécessaires pour atteindre l'objectif pour lequel l'autorisation d'exercer ce pouvoir procédural est requise, lorsqu'une autorisation de collecte ou d'enregistrement à plus d'une occasion est nécessaire ;
 - e. Les mesures prises doivent garantir que la collecte ou l'enregistrement est effectué tout en préservant la vie privée des autres utilisateurs, clients et tiers, sans divulgation d'informations et de données de toute partie non impliquée dans l'enquête ;
 - f. L'enquête risque d'être entravée ou gravement compromise si la collecte ou l'enregistrement n'est pas autorisé ;
 - g. Pour atteindre l'objectif pour lequel l'autorisation est demandée, la collecte ou l'enregistrement des données de trafic est nécessaire.
6. Chaque Etat membre prend les mesures nécessaires pour que l'autorisation de collecte ou d'enregistrement des données de trafic ne dépasse pas la durée strictement nécessaire et, en tout état de cause, pas plus de quatre-vingt (90) jours, cette période pouvant être prolongée par notification à l'autorité judiciaire ou compétente de l'Etat membre.
7. Chaque Etat membre prend les mesures nécessaires pour accorder aux prestataires de services le droit exprès de contester devant l'autorité judiciaire ou compétente une injonction de procéder à la collecte en temps réel de données de trafic, pour des motifs de pertinence, de privilège ou d'autres objections légales à l'encontre de l'injonction ou autrement protégée contre la divulgation par la loi, ou de non-respect des exigences du présent article.

Article 33 – Interception des données de contenu

1. Chaque Etat membre adopte les mesures nécessaires, concernant un ensemble d'infractions pénales graves à déterminer en vertu du droit national de son droit national, afin d'habiliter les autorités judiciaires ou autres autorités compétentes à :
 - a. intercepter, collecter ou enregistrer, par l'application de moyens techniques sur leur territoire, les données de contenu associées à des communications spécifiques en temps réel ; et
 - b. contraindre un prestataire de services, dans les limites de ses capacités techniques existantes à :
 - i. intercepter, collecter ou enregistrer, par l'application de moyens techniques sur le territoire de l'Etat membre, les données de contenu associées à des communications spécifiées en temps réel ; ou
 - ii. coopérer et assister les autorités judiciaires ou autres autorités compétentes dans l'interception, la collecte ou l'enregistrement de ces données de contenu.
2. Lorsque, en raison des principes de son système juridique national, un Etat membre ne peut adopter les mesures visées au paragraphe 1 alinéa a. du présent article, il peut adopter à la place les mesures nécessaires pour assurer l'interception, la collecte ou l'enregistrement des données de contenu de communications spécifiées transmises sur son territoire, par l'application de moyens techniques sur ce territoire.
3. Chaque Etat membre prend les mesures nécessaires pour obliger les prestataires de services à garder confidentiels le fait de l'exercice de tout pouvoir prévu au présent article, ainsi que toute information s'y rapportant, pendant la période prévue par la loi nationale.
4. L'application des mesures prévues au présent article est soumise à des conditions et garanties, notamment une autorisation judiciaire ou indépendante, la proportionnalité, la nécessité et des limitations quant à l'utilisation et à la conservation des données de contenu.
5. Chaque Etat membre prend les mesures nécessaires pour garantir qu'une ordonnance d'interception, de collecte ou d'enregistrement de données de contenu ne puisse être délivrée que sur demande exposant, lorsque cela est raisonnable et possible, les raisons pour lesquelles il est estimé que :
 - a. les données de contenu recherchées seront obtenues si ce pouvoir procédural est exercé ;
 - b. le type de données de contenu que l'on soupçonne d'être trouvées ;
 - c. L'infraction identifiée est l'infraction pour laquelle le mandat est demandé ;
 - d. Les divulgations supplémentaires sont nécessaires pour atteindre l'objectif pour lequel l'autorisation d'exercer ce pouvoir procédural est requise, lorsqu'une autorisation de demander une interception, une collecte ou un enregistrement à plus d'une occasion est nécessaire ;

- e. Les mesures prises doivent garantir que l'interception, la collecte ou l'enregistrement soient effectués tout en préservant la vie privée des autres utilisateurs, clients et tiers, sans divulgation d'informations et de données d'aucune partie ne faisant pas partie de l'enquête ;
 - f. L'enquête risque d'être entravée ou gravement compromise si l'interception, la collecte ou l'enregistrement ne sont pas autorisés ;
 - g. Pour atteindre l'objectif pour lequel l'autorisation est demandée, l'interception, la collecte ou l'enregistrement des données de contenu est nécessaire.
6. Chaque Etat membre prend les mesures nécessaires pour garantir que l'autorisation d'interception, de collecte ou d'enregistrement de données de contenu ne soit pas accordée pour une durée supérieure à celle strictement nécessaire et, en tout état de cause, pas plus longue que celle déterminée par le droit national.
 7. Chaque Etat membre prend les mesures nécessaires pour accorder aux prestataires de services le droit exprès de contester devant l'autorité judiciaire ou compétente une injonction d'interception de données de contenu pour cause de pertinence, de privilège ou autre objection légale à l'injonction ou autrement protégée contre la divulgation par la loi, ou pour non-respect des exigences du présent article.

Article 34 – Gel, saisie et confiscation du produit du crime

1. Chaque Etat membre adopte, dans toute la mesure permise par leur système juridique national, les mesures nécessaires pour permettre la confiscation de :
 - a. produits du crime provenant d'infractions établies conformément à la présente Directive ou biens dont la valeur correspond à celle de ces produits ;
 - b. biens, équipements ou autres instruments utilisés ou destinés à être utilisés dans le cadre d'infractions établies conformément à la présente Directive.
2. Chaque Etat membre adopte les mesures qui peuvent être nécessaires pour permettre l'identification, le traçage, le gel ou la saisie de tout élément visé au paragraphe 1 du présent article en vue d'une éventuelle confiscation.
3. Chaque Etat membre adopte, conformément à son droit national, les mesures nécessaires pour réglementer l'administration par les autorités judiciaires ou autres autorités compétentes des biens gelés, saisis ou confisqués visés aux paragraphes 1 et 2 du présent article.
4. lorsque le produit d'un crime a été transformé ou converti, en partie ou en totalité, en d'autres biens, ces biens sont soumis aux mesures visées au présent article à la place du produit du crime.

5. lorsque des produits du crime ont été mélangés à des biens acquis de sources légitimes, ces biens seront, sans préjudice des pouvoirs relatifs au gel ou à la saisie, passibles de confiscation à concurrence de la valeur estimée des produits mélangés.
6. Les revenus ou autres avantages provenant du produit du crime, de biens dans lesquels le produit du crime a été transformé ou converti, ou de biens avec lesquels le produit du crime a été mêlé, sont également soumis aux mesures visées au présent article, de la même manière et dans la même mesure que le produit du crime.
7. Aux fins du présent article et de l'article 47 de la présente Directive, Chaque Etat membre habilite ses autorités judiciaires ou autres autorités compétentes à ordonner que les documents bancaires, financiers ou commerciaux soient mis à disposition ou saisis .
8. Chaque Etat membre ne peut refuser d'agir conformément aux dispositions du présent article au motif du secret bancaire.
9. Chaque Etat membre peut envisager la possibilité d'exiger d'un contrevenant qu'il démontre l'origine licite du produit présumé du crime ou d'autres biens susceptibles de confiscation, dans la mesure où une telle exigence est compatible avec les principes du droit national et avec la nature des procédures judiciaires et autres.
10. Les dispositions du présent article ne doivent pas être interprétées comme portant atteinte aux droits des tiers de bonne foi.
11. Aucune disposition du présent article ne porte atteinte au principe selon lequel les mesures auxquelles il se rapporte doivent être définies et mises en œuvre conformément aux dispositions du droit national d'un État membre.

Article 35 – Responsabilité des prestataires de services

1. Chaque Etat membre prend les mesures nécessaires pour garantir que les prestataires de services ne soient pas soumis à une responsabilité civile ou pénale pour les informations transmises, acheminées, relayées, mises en cache, stockées ou autrement mises à disposition par le biais de leurs services, à moins qu'il ne soit établi que le prestataire de services avait :
 - a. une notification effective et une connaissance précise de l' activité ou de l'information illicite ; et
 - b. l'intention délibérée et malveillante de faciliter, d'aider ou d'encourager une telle activité illégale, au-delà d'une simple omission ou d'un défaut d'agir.
2. La charge de la preuve pour établir la responsabilité en vertu du paragraphe 1 du présent article incombe à la partie qui allègue une telle notification, connaissance ou intention.

3. Chaque Etat membre exige que toute allégation de ce type à l'encontre d'un prestataire de services identifie clairement et précisément le contenu, le matériel ou la conduite donnant lieu à la responsabilité alléguée.
4. Chaque Etat membre veille à ce que les prestataires de services ne soient en aucun cas tenus responsables uniquement du maintien ou de la mise à disposition de leurs services.
5. Chaque Etat membre veille à ce que les prestataires de services ne soient pas responsables de la divulgation de données ou d'autres informations lorsque cette divulgation n'est effectuée que dans la mesure requise par le droit national ou en application d'une ordonnance légale rendue conformément aux dispositions du présent Chapitre.
6. Chaque Etat membre adopte les mesures nécessaires pour garantir que les prestataires de services ne soient pas soumis à des obligations générales de surveillance proactive, d'enquête ou de recherche de faits ou de circonstances relatifs au contenu ou aux informations qu'ils transmettent, acheminent, mettent en cache, stockent ou mettent autrement à disposition.
7. Chaque Etat membre adopte les mesures nécessaires pour garantir que les fournisseurs de services mettent en place des mécanismes de signalement accessibles et transparents et informent les utilisateurs de leurs droits et recours.

Article 36 – Assistance aux victimes

1. Chaque Etat membre reconnaît l'importance d'assurer la protection et l'assistance effective des victimes de la cybercriminalité, en accordant une attention particulière aux cas impliquant un enfant.
2. Chaque Etat membre doit envisager de mettre en place des mécanismes appropriés pour remédier aux préjudices physiques, psychologiques et économiques subis par les victimes.
3. Chaque Etat membre doit envisager de mettre en œuvre des procédures efficaces pour :
 - a. préserver la vie privée et l'identité des victimes, y compris la protection de leurs données personnelles ;
 - b. offrir des possibilités d'indemnisation, notamment par le biais de fonds d'aide aux victimes, lorsque de tels fonds existent.
4. Les Etats membres doivent s'engager dans une coopération internationale visant à prévenir, atténuer et réparer les préjudices subis par les victimes de la cybercriminalité.

CHAPITRE V – COOPÉRATION RÉGIONALE ET INTERNATIONALE

Article 37 – Principes généraux relatifs à l'assistance mutuelle

1. Chaque Etat membre désigne une autorité centrale chargée de :
 - a. envoyer et répondre aux demandes d'entraide judiciaire ;
 - b. assurer l'exécution de ces demandes ou leur transmission aux autorités compétentes pour leur exécution ; et
 - c. exercer les fonctions et les pouvoirs conférés par la présente Directive en matière de coopération internationale.
2. Chaque Etat membre communique à la Commission de la CEDEAO les noms et adresses des autorités désignées en application du présent article.
3. La Commission de la CEDEAO établit et tient à jour un registre des autorités centrales désignées par les États membres. Chaque État membre veille à ce que les informations figurant dans ce registre soient exactes en permanence .
4. Chaque Etat membre veille à ce que l' autorité centrale fournisse une assistance juridique mutuelle dans toute la mesure du possible aux fins d'enquêtes ou de poursuites concernant des infractions pénales relevant du champ d'application défini à l'article 26 de la présente Directive.
5. Chaque Etat membre veille à ce que, dans des circonstances urgentes, l'autorité centrale puisse formuler ou recevoir des demandes d'entraide judiciaire, ou des communications connexes, par des moyens de communication accélérés, y compris par voie électronique, à condition que des niveaux appropriés de sécurité et d'authentification soient maintenus, notamment par le recours au chiffrement lorsque cela est nécessaire. Une confirmation formelle est ensuite fournie lorsque l'État membre requis ou requérant l'exige.
6. Sauf disposition contraire expresse des articles du présent chapitre, l'entraide judiciaire est soumise aux conditions prévues par la législation de l'État membre requis, par les traités d'entraide judiciaire applicables ou par un accord des États membres concernés fondé sur la présente Directive, y compris les motifs pour lesquels l'État membre requis peut refuser de coopérer.

7. L'État membre requis ne peut exercer son droit de refuser l'entraide judiciaire en ce qui concerne les infractions visées aux articles 2 à 11 de la présente Directive au seul motif que la demande porte sur une infraction qu'il considère comme une infraction fiscale.
8. Lorsque l'entraide judiciaire est subordonnée à l'existence d'une double incrimination, chaque Etat membre veille à ce que cette condition soit réputée remplie, indépendamment du fait que son droit national classe ou désigne l'infraction dans la même catégorie ou par la même terminologie que l'État membre requérant, si le comportement à l'origine de l'infraction constitue une infraction pénale en vertu de son droit national.
9. Les demandes d'entraide judiciaire présentées au titre du présent Chapitre sont exécutées conformément aux procédures fixées par les États membres requérants, sauf en cas d'incompatibilité avec la législation des États membres requis.
10. Sauf indication contraire, l'État membre requis peut refuser son assistance si :
 - a. la demande concerne une infraction que l'État membre requis considère comme une infraction politique ou une infraction liée à une infraction politique, ou
 - b. l'État membre requis considère que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.
 - c. la demande n'est pas faite conformément aux dispositions du présent article ;
 - d. il y a absence de double criminalité ;
 - e. Les autorités de l'État membre requis sont empêchées par droit national son droit national de prendre les mesures demandées à l'égard de toute infraction similaire, si celle-ci avait fait l'objet d'une enquête, de poursuites ou de procédures judiciaires relevant de leur propre juridiction ;
 - f. son assistance est contraire au système juridique de l'État membre requis en matière d'entraide judiciaire que la demande soit acceptée ; ou
 - g. L'État membre requis a des motifs sérieux de croire que la demande a été faite dans le but de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politiques, ou que le fait de donner suite à la demande porterait préjudice à la situation de cette personne pour l'une de ces raisons.
 - h. si, au moment de la communication, il apparaît par la suite clair à l'État membre requis que la demande concerne l'un des paragraphes 10 alinéas b., c., d. et g. du présent article.
11. Tout refus d'entraide judiciaire doit être motivé.
12. L'Etat membre requis exécute la demande d'entraide judiciaire dans les meilleurs délais et tient compte autant que possible des délais suggérés par l'État membre requérant et dont les raisons sont données, de préférence dans la demande.

13. L'État membre requis répond aux demandes raisonnables de l'État membre requérant concernant l'état d'avancement et les progrès réalisés dans le traitement de la demande.
14. L'État membre requis peut reporter toute action relative à une demande si cette action est susceptible de porter préjudice aux enquêtes ou procédures pénales menées par ses autorités.
15. Avant de refuser ou de reporter son assistance, l'État membre requis examine, le cas échéant après avoir consulté l'État membre concerné, si la demande peut être accordée partiellement ou sous réserve des conditions qu'il juge nécessaires.
16. L'État membre requis informe sans délai l'État membre requérant du résultat de l'exécution de la demande d'assistance. Tout refus ou report de la demande est motivé. L'État membre requis informe également l'État membre requérant de tout motif rendant impossible l'exécution de la demande ou susceptible de la retarder sensiblement.
- 17.
- a. L'État membre requérant peut demander à l'État membre requis de garder confidentielle l'existence même de toute demande formulée en vertu du présent chapitre, ainsi que son objet, sauf dans la mesure nécessaire à son exécution. Si l'État membre requis ne peut se conformer à cette demande de confidentialité, il en informe sans délai l'État membre requérant, lequel détermine alors s'il convient néanmoins d'exécuter la demande.
 - b. L'État membre requis peut subordonner la fourniture d'informations ou de documents en réponse à une demande à la condition qu'elle soit :
 - i. maintenue confidentielle lorsque la demande d'entraide judiciaire ne peut être satisfaite en l'absence d'une telle condition, ou
 - ii. non utilisée pour des enquêtes ou des procédures autres que celles mentionnées dans la demande.
 - c. Si l'État membre requérant ne peut satisfaire à une condition visée au paragraphe 17 alinéa b. du présent article, il en informe sans délai l'autre État membre, lequel détermine alors s'il convient néanmoins de fournir les informations. Lorsque l'État membre requérant accepte la condition, il y est lié.
 - d. Tout État membre qui fournit des informations ou du matériel soumis à une condition visée au paragraphe 17 alinéa b. du présent article peut exiger de l'autre Partie qu'elle explique, en relation avec cette condition, l'utilisation faite de ces informations ou de ce matériel.
- 18.
- a. En cas d'urgence, les demandes d'entraide judiciaire ou les communications s'y rapportant peuvent être adressées directement par les autorités judiciaires des États membres requérants aux autorités judiciaires de l'État membre requis. Dans ce cas, une copie est simultanément transmise à l'autorité centrale de l'État

- membre requis par l'intermédiaire de l'autorité centrale de l'État membre requérant.
- b. Toute demande ou communication peut être transmise par l'intermédiaire de l'Organisation Internationale de la Police Criminelle (INTERPOL) ou du Système d'Information de la Police Ouest-Africaine (SIPAO).
 - c. Lorsqu'une demande est adressée directement à une autorité judiciaire de l'État membre requis qui n'est pas compétente pour la traiter, l'autorité judiciaire de l'État membre requis transmet la demande à l'autorité centrale de l'État membre requis et en informe l'autorité judiciaire qui a formulé la demande.
 - d. Les demandes ou communications qui n'impliquent pas de mesures coercitives peuvent être transmises directement par l'autorité judiciaire de l'État membre requérant à l'autorité judiciaire de l'État membre requis.
 - e. L'autorité judiciaire de l'État membre requis ne peut mettre en œuvre les mesures prévues au présent paragraphe que si le droit national de cet État membre le permet.
 - f. L'autorité judiciaire d'un État membre requis ne peut communiquer à l'autorité judiciaire de l'État membre requérant, sur la base d'une demande d'entraide judiciaire, qu'après approbation de l'autorité centrale.

Article 38 – Information spontanée

1. Chaque Etat membre prend les mesures nécessaires pour permettre à son autorité compétente de transmettre, sans demande préalable, à un pays tiers les informations obtenues dans le cadre de ses propres enquêtes, lorsqu'elle estime qu'une telle divulgation peut :
 - a. aider l' le pays tiers à engager ou à mener des enquêtes ou des procédures; ou
 - b. conduire à une demande de coopération au titre de la présente Directive ou d'autres instruments internationaux applicables auxquels un État membre est partie.
2. Chaque Etat membre veille à ce que l'autorité compétente puisse, avant de fournir de telles informations, demander qu'elles soient tenues confidentielles ou utilisées sous réserve de conditions spécifiques.
3. Chaque Etat membre veille à ce que, lorsque l'État destinataire ne peut se conformer à ces conditions, il en informe l'autorité émettrice, laquelle détermine alors si les informations doivent néanmoins être fournies. Lorsque l'État destinataire accepte les informations sous conditions, il est lié par celles-ci.
4. Chaque Etat membre veille à ce que les preuves ou informations reçues en application du présent article ne soient pas irrecevables dans le cadre de poursuites pénales au seul motif qu'elles ont été transmises sans demande formelle d'entraide judiciaire.
5. Chaque Etat membre veille à ce que la réception d'informations spontanées conformément au présent article n'empêche pas l'État destinataire de présenter

ultérieurement des demandes d'entraide judiciaire portant sur les mêmes faits, comportements ou éléments de preuve.

Article 39 – Conservation accélérée des données informatiques stockées

1. Chaque Etat membre prend les mesures nécessaires pour permettre à son autorité compétente de, à la demande d'un pays tiers ou d'une organisation multilatérale compétente, ordonner ou obtenir par tout autre moyen la conservation rapide de données informatiques stockées spécifiées situées sur leur territoire ou sous leur contrôle, lorsque l'autorité requérante entend présenter une demande d'entraide judiciaire en vue de la recherche, de l'accès, de la saisie, de la sécurisation ou de la communication de ces données informatiques.
2. Chaque Etat membre veille à ce qu'une demande de conservation comprenne, dans la mesure du possible :
 - a. l'identité de l'autorité qui demande la préservation ;
 - b. l'infraction qui fait l'objet de l'enquête ou des poursuites, y compris un bref résumé des faits pertinents ;
 - c. les données informatiques stockées à préserver et leur lien avec l'infraction ;
 - d. toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou l'emplacement du système informatique ;
 - e. la nécessité de la préservation ; et
 - f. la confirmation que l'autorité requérante a l'intention de soumettre une demande d'entraide judiciaire relative à la recherche, à l'accès, à la saisie, à la sécurisation ou à la divulgation des données informatiques.
3. Chaque Etat membre veille à ce que son autorité compétente prenne les mesures appropriées pour préserver rapidement les données informatiques spécifiées, conformément aux procédures et aux pouvoirs prévus par le droit national transposant la présente Directive.
4.
 - a. Un Etat membre ne peut refuser la conservation, au titre du présent article, d'une infraction visée au Chapitre I de la présente Directive au seul motif que la condition de double incrimination n'est pas remplie.
 - b. Pour toute autre infraction, lorsqu'un Etat membre qui exige la double incrimination comme condition pour répondre à une demande d'entraide judiciaire en matière de recherche ou d'accès similaire, de saisie ou de mise en sécurité similaire, ou de communication de données conservées, cet Etat membre peut se réserver le droit de refuser la demande de conservation, au titre

du présent article, pour toute autre infraction s'il a des raisons de croire qu'au moment de la communication, la condition de double incrimination ne peut être remplie.

5. De plus, une demande de conservation ne peut être refusée que si :
 - a. la demande concerne une infraction que l'État membre requis considère comme une infraction politique ou une infraction liée à une infraction politique ;
 - b. l'État membre requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels ; ou
 - c. si, au moment de la communication, il apparaît par la suite clair à l'État membre requis que la demande se rapporte au paragraphe 5 alinéa a. ou b. du présent article.
6. Lorsqu'un État membre requis estime que la conservation ne garantit pas la disponibilité future des données ou menace la confidentialité de l'enquête de l'État membre requérant ou y porte autrement préjudice, il en informe sans délai l'État membre requérant, qui détermine alors si la demande doit néanmoins être exécutée.
7. Chaque État membre veille à ce que toute conservation effectuée en réponse à une telle demande soit d'une durée minimale de soixante (60) jours, afin de permettre à l'autorité requérante de présenter une demande d'entraide judiciaire. Après réception d'une telle demande, les données informatiques continuent d'être conservées jusqu'à ce qu'une décision définitive soit rendue.

Article 40 – Divulgence accélérée des données de trafic conservées

1. Lorsque, dans le cadre de l'exécution d'une demande formulée au titre de l'article 39 de la présente Directive ou autrement en relation avec une communication spécifique, un État membre découvre qu'un prestataire de services situé dans un pays tiers a participé à la transmission de la communication, l'État membre communique sans délai au gouvernement étranger requérant ou à l'organisation multilatérale compétente concernée une quantité suffisante de données de trafic pour identifier ce prestataire de services et le chemin par lequel la communication a été transmise.
2. La divulgation des données de trafic visées au paragraphe 1 du présent article ne peut être refusée que lorsque :
 - a. la demande concerne une infraction que l'État membre requis considère comme une infraction politique ou une infraction liée à une infraction politique ;
 - b. l'État membre requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels ; ou

- c. lorsque, au moment de la divulgation, il apparaît par la suite clairement à l'État membre requis que la demande se rapporte au paragraphe 2 alinéas a. ou b. du présent article.
- d. lorsque les autorités de l'État membre sont empêchées par son droit national d'entreprendre l'action demandée relativement à toute infraction similaire, si celle-ci avait fait l'objet d'une enquête, de poursuites ou d'une procédure judiciaire relevant de leur propre juridiction ; ou
- e. lorsque l'État membre a des motifs sérieux de croire que la demande a été faite dans le but de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politiques, ou que le fait de donner suite à la demande porte préjudice à la situation de cette personne pour l'une de ces raisons.

Article 41 – Entraide judiciaire en matière de recherche, de saisie et de communication de données informatiques stockées

1. Chaque Etat membre adopte les mesures nécessaires pour habiliter leurs autorités compétentes, à la demande du gouvernement d'un pays tiers ou d'une organisation multilatérale compétente, à ordonner ou à effectuer de toute autre manière la recherche ou l'accès similaire, la saisie ou la sécurisation similaire, et la divulgation de programmes informatiques ou de données informatiques stockés au moyen d'un système informatique sur leur territoire, y compris les données conservées conformément à l'article 39 de la présente Directive.
2. Les demandes d'entraide judiciaire au titre du présent article doivent, dans la mesure du possible et selon les possibilités, préciser :
 - a. l'autorité menant l'enquête ou la procédure à laquelle la demande se rapporte ;
 - b. la nature de l'affaire pénale, avec un résumé des faits pertinents et du droit applicable ;
 - c. l'objet de la demande et le type d'assistance recherchée ;
 - d. en cas de gel ou de confiscation d'avoirs présumés se trouver dans l'État membre demandé, les détails de l'infraction, de toute enquête ou procédure engagée à l'égard de l'infraction, et une copie de toute ordonnance de gel ou de confiscation pertinente ;
 - e. détails de toute procédure à suivre pour donner suite à la demande, notamment en ce qui concerne le recueil de preuves ;
 - f. toutes les exigences de confidentialité et leurs raisons ;
 - g. la période dans laquelle l'État membre requérant cherche à obtenir le respect des obligations ;
 - h. le cas échéant, les détails relatifs au bien, au système informatique ou à l'appareil à localiser, à retenir, à saisir ou à confisquer, ainsi que les motifs permettant de croire que le bien se trouve dans l'État membre demandé ;
 - i. détails des données informatiques stockées ou du programme informatique à saisir et leur lien avec l'infraction ;

- j. toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou du programme informatique, ou l'emplacement du système ou du dispositif informatique ;
 - k. dispositions relatives à la répartition des coûts ou des dommages découlant de l'exécution de la demande; et
 - l. toute autre information pertinente pour une exécution efficace.
3. Dès réception d'une demande formulée en application du présent article, l'autorité compétente de l'État membre requis prend toutes les mesures appropriées, y compris la recherche des autorisations judiciaires ou administratives nécessaires, pour exécuter la demande conformément aux procédures et pouvoirs nationaux prévus par la présente Directive.
 4. Lorsque cela est nécessaire et compatible avec le droit national, l'autorité compétente peut solliciter la coopération ou la participation de l'État membre requérant ou de l'organisation multilatérale compétente applicable pour l'exécution de la perquisition et de la saisie.
 5. L'État membre requis peut transmettre les résultats de la perquisition et de la saisie, ainsi que toute preuve électronique obtenue, à l'État membre requérant ou à l'organisation multilatérale compétente applicable.
 6. L'entraide judiciaire prévue au présent article peut être refusée pour les motifs mentionnés au paragraphe 9 de l'article 37 de la présente Directive.

Article 42 – Assistance mutuelle pour la collecte en temps réel des données de trafic

1. Chaque Etat membre prend les mesures nécessaires pour habilitier leurs autorités compétentes, à la demande d'un gouvernement étranger ou d'une organisation multilatérale compétente, à fournir une assistance pour la collecte ou l'enregistrement en temps réel des données de trafic associées à des communications spécifiques transmises au moyen d'un système informatique sur le territoire de l'État membre.
2. Une demande d'assistance au titre du présent article doit, dans la mesure du possible et selon les possibilités, préciser :
 - a. le nom de l'autorité requérante ;
 - b. l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un résumé des faits connexes ;
 - c. l'autorité ou le fournisseur de services ayant accès aux données de trafic pertinentes ;
 - d. toutes les données disponibles permettant d'identifier le propriétaire ou l'utilisateur des données ou l'emplacement du système informatique ;
 - e. l'objectif visé pour lequel les données de trafic sont recherchées ;
 - f. les informations suffisantes pour identifier les données de trafic ;

- g. tout autre détail pertinent concernant les données de trafic ;
 - h. la justification de la nécessité de collecter les données de trafic ;
 - i. la période pendant laquelle les données de trafic doivent être collectées et une justification correspondante de sa durée ; et
 - j. les conditions ou limitations régissant l'utilisation ou la divulgation ultérieure des données de trafic à des tiers.
3. Dès réception d'une demande formulée en application du présent article, un État membre prend toutes les mesures appropriées pour obtenir les autorisations nécessaires , y compris les mandats, afin d'exécuter la demande conformément aux procédures et pouvoirs prévus par la présente Directive.
 4. Lorsque cela est conforme au droit national, l'Etat membre peut solliciter la coopération du Gouvernement d'un pays tiers requérant ou l'organisation multilatérale compétente pour l'exécution des mesures prévues au présent article.
 5. Lors de la mise en œuvre des mesures prévues au présent article, l'État membre peut transmettre les résultats de la collecte en temps réel des données de trafic associées à des communications spécifiques au gouvernement d'un pays tiers requérant ou à l'organisation multilatérale compétente concernée.
 6. L'entraide judiciaire prévue au présent article peut être refusée pour les motifs mentionnés au paragraphe 9 de l'article 37 de la présente Directive.

Article 43 – Entraide en matière d'interception de données de contenu

1. Chaque Etat membre prend les mesures nécessaires pour habilitier leurs autorités compétentes, à la demande d'un gouvernement étranger ou d'une organisation multilatérale compétente , à apporter une assistance en matière d'interception, de collecte ou d'enregistrement de données de contenu associées à des communications spécifiques transmises au moyen d'un système informatique sur le territoire d'un État membre.
2. Une demande d'assistance au titre du présent article doit, dans la mesure du possible, préciser :
 - a. l'autorité qui sollicite l'usage des pouvoirs conférés par le présent article ;
 - b. l'infraction qui fait l'objet d'une enquête ou de poursuites pénales et un bref résumé des faits connexes ;
 - c. le nom de l'autorité ayant accès à la communication concernée ;
 - d. le lieu ou la nature de la communication ;
 - e. l'objectif visé par la communication requise ;
 - f. les informations suffisantes pour identifier les communications ;
 - g. les détails des données de l'interception concernée ;

- h. le destinataire de la communication ;
 - i. la durée prévue d'utilisation de la communication ;
 - j. la nécessité d'utiliser les pouvoirs conférés par le présent article; et
 - k. les conditions d'utilisation et de divulgation de la communication à des tiers.
3. Dès réception de la demande visée au présent article, l'État membre prend, si celle-ci concerne une infraction punissable d'une peine au moins égale à celle prévue par sa loi nationale, toutes les mesures appropriées pour obtenir l'autorisation nécessaire , y compris les mandats d'exécution, conformément aux procédures et pouvoirs prévus par la présente Directive.
 4. Sur obtention des autorisations nécessaires, y compris les mandats d'exécution requis, l'État membre peut solliciter le soutien et la coopération du gouvernement étranger ou de l'organisation multilatérale compétente lors de la perquisition et de la saisie.
 5. Lors de la mise en œuvre des mesures prévues au présent article, l'État membre peut transmettre les résultats de ces mesures ainsi que les données relatives à l'interception, à la collecte ou à l'enregistrement du contenu des communications concernées au gouvernement étranger ou à l'organisation multilatérale compétente .
 6. L'entraide judiciaire prévue au présent article peut être refusée pour les motifs mentionnés au paragraphe 9 de l'article 37 de la présente Directive.

Article 44 – Accès transfrontalier aux données informatiques stockées lorsqu'elles sont accessibles au public ou avec consentement

1. Chaque Etat membre veille à ce que ses autorités compétentes soient habilitées, sans autorisation préalable d'un autre État membre, à :
 - a. accéder aux données informatiques stockées et accessibles au public, quel que soit l'emplacement géographique de ces données ;
 - b. accéder ou recevoir, par le biais d'un système informatique situé sur leur territoire, des données informatiques stockées dans un autre État membre, lorsque le consentement licite et volontaire de la personne habilitée à divulguer ces données a été obtenu ; ou
 - c. accéder ou recevoir, par l'intermédiaire d'un système informatique situé dans l'État membre, des données informatiques stockées situées hors de l'État membre, lorsqu'il existe une situation dans laquelle :
 - i. il existe un risque important et imminent pour la vie ou la sécurité des personnes, ou
 - ii. il y a eu un préjudice économique important, que ce soit en termes de montant ou de nombre de victimes dans l'État membre et le recours à d'autres procédures d'entraide judiciaire porterait atteinte de manière irréparable à la capacité de l'État membre d'enquêter sur une infraction et de la poursuivre, à condition que l'autorité compétente notifie le pays

où se trouvaient les données dès que possible après avoir accédé aux données informatiques ou les avoir reçues.

2. Chaque Etat membre veille à ce que ces mesures soient mises en œuvre conformément à son droit national et dans le respect des obligations internationales applicables.

Article 45 – Coopération policière

1. Les Etats membres coopèrent étroitement entre eux, dans le respect de leurs systèmes juridiques et administratifs nationaux respectifs, afin de renforcer l'efficacité des mesures répressives visant à lutter contre les infractions prévues par la présente Directive. Ils prennent notamment des mesures efficaces, afin de :
 - a. renforcer et, le cas échéant, d'établir des canaux de communication entre leurs autorités, agences et services compétents, en tenant compte des canaux existants, notamment ceux de l'Organisation internationale de police criminelle (INTERPOL) ou du Système d'information de la police ouest-africaine (SIPAO), afin de faciliter l'échange sécurisé et rapide d'informations concernant tous les aspects des infractions établies conformément à la présente Directive, y compris, si les Etats membres concernés le jugent approprié, les liens avec d'autres activités criminelles ;
 - b. coopérer avec les autres États membres dans le cadre d'enquêtes relatives aux infractions constatées conformément à la présente Directive concernant :
 - i. l'identité, le lieu de séjour et les activités des personnes soupçonnées d'être impliquées dans de telles infractions ou la localisation d'autres personnes concernées ;
 - ii. le mouvement des produits du crime ou des biens provenant de la commission de telles infractions ;
 - iii. le déplacement de biens, d'équipements ou d'autres instruments utilisés ou destinés à être utilisés dans la commission de telles infractions ;
 - c. fournir, le cas échéant, les éléments ou données nécessaires à des fins d'analyse ou d'enquête ;
 - d. échanger, le cas échéant, des informations avec d'autres États membres concernant les moyens et méthodes spécifiques utilisés pour commettre les infractions établies conformément à la présente Directive, notamment l'utilisation de fausses identités, de documents falsifiés, modifiés ou contrefaits et d'autres moyens de dissimulation d'activités, ainsi que les tactiques, techniques et procédures de cybercriminalité ;
 - e. afin de faciliter une coordination efficace entre leurs autorités, agences et services compétents et de promouvoir l'échange de personnel et d'autres

experts, y compris, sous réserve d'accords ou d'arrangements bilatéraux entre les Etats membres concernés, le détachement d'agents de liaison ;

- f. échanger des informations et coordonner les mesures administratives et autres prises, le cas échéant, aux fins de l'identification rapide des infractions établies conformément à la présente Directive.
2. Les Etats membres, afin de donner effet à la présente Directive, doivent :
- a. envisager de conclure des accords ou des arrangements bilatéraux ou multilatéraux de coopération directe entre leurs services répressifs et, lorsque de tels accords ou arrangements existent déjà, de les modifier.
 - b. considérer la présente Directive comme le fondement de leur coopération répressive mutuelle en matière d'infractions définies en l'absence de tels accords ou arrangements.
 - c. Le cas échéant, tirer pleinement parti des accords ou arrangements existants, y compris ceux conclus avec des organisations internationales ou régionales, afin de renforcer la coopération entre leurs services répressifs.

Article 46 – Enquêtes conjointes

- 1. Les Etats membres doivent envisager de conclure des accords ou arrangements bilatéraux ou multilatéraux en vertu desquels, pour les infractions établies conformément à la présente Directive et faisant l'objet d'enquêtes pénales, de poursuites ou de procédures judiciaires dans un ou plusieurs Etats membres, les autorités compétentes concernées peuvent constituer des organes d'enquête conjoints.
- 2. À défaut de tels accords ou arrangements, des enquêtes conjointes peuvent être menées d'un commun accord, au cas par cas.
- 3. Les Etats membres concernés veillent à ce que la souveraineté de l'Etat membre sur le territoire duquel les enquêtes doivent avoir lieu soit pleinement respectée.

Article 47 – Mécanismes de recouvrement des biens par la coopération internationale en matière de confiscation

- 1. Chaque Etat membre, afin de fournir une entraide juridique conformément à l'article 48 de la présente Directive en ce qui concerne les biens acquis par le biais d'une infraction établie conformément à la présente Directive ou impliqués dans sa commission, doit, conformément à sa législation nationale :
 - a. prendre les mesures qui peuvent être nécessaires pour permettre à ses autorités compétentes de donner effet à une ordonnance de confiscation rendue par un tribunal d'un autre Etat membre ;
 - b. prendre les mesures nécessaires pour permettre à ses autorités compétentes, lorsqu'elles ont juridiction, d'ordonner la confiscation de ces biens d'origine étrangère par la constatation d'une infraction de blanchiment d'argent ou de

- toute autre infraction relevant de sa compétence ou par d'autres procédures autorisées par son droit national ; et
- c. envisager de prendre les mesures nécessaires pour permettre la confiscation de ces biens sans condamnation pénale dans les cas où le contrevenant ne peut être poursuivi en raison de son décès, de sa fuite ou de son absence, ou dans d'autres cas appropriés.
2. Chaque État membre, afin de fournir une entraide juridique mutuelle sur demande formulée en application du paragraphe 2 de l'article 48 de la présente Directive, doit, conformément à sa loi nationale :
- a. prendre les mesures qui peuvent être nécessaires pour permettre à ses autorités compétentes de geler ou de saisir des biens sur la base d'une ordonnance de gel ou de saisie émise par un tribunal ou une autorité compétente d'un État membre requérant qui fournit une base raisonnable permettant à l'État membre requis de croire qu'il existe des motifs suffisants pour prendre de telles mesures et que les biens seraient éventuellement soumis à une ordonnance de confiscation aux fins du paragraphe 1 alinéa a. du présent article ;
 - b. prendre les mesures nécessaires pour permettre à ses autorités compétentes de geler ou de saisir des biens sur une demande qui fournit à l'État membre requis des motifs raisonnables de croire qu'il existe des motifs suffisants pour prendre de telles mesures et que les biens seraient finalement soumis à une ordonnance de confiscation aux fins du paragraphe 1 alinéa a. du présent article ; et
 - c. envisager de prendre des mesures supplémentaires pour permettre à ses autorités compétentes de conserver des biens en vue de leur confiscation, par exemple sur la base d'une arrestation étrangère ou d'une accusation criminelle liée à l'acquisition de ces biens.

Article 48 – Coopération internationale aux fins de confiscation

1. Un État membre qui a reçu d'un autre État membre compétent pour juger une infraction établie conformément à la présente Directive une demande de confiscation du produit du crime, de biens, de matériels ou d'autres instruments visés à l'article 34, paragraphe 1, de la présente Directive situés sur son territoire peut, dans toute la mesure permise par son système juridique national :
- a. Soumettre la demande aux autorités compétentes afin d'obtenir une ordonnance de confiscation et, si une telle ordonnance est accordée, la mettre en œuvre ; ou
 - b. Transmettre à ses autorités compétentes, en vue de leur donner effet dans la mesure demandée, une ordonnance de confiscation rendue par un tribunal du territoire de l'État membre requérant conformément à l'article 34, paragraphe 1, de la présente Directive, pour autant qu'elle concerne le produit du crime, des biens, du matériel ou d'autres instruments situés sur le territoire de l'État membre requis.

2. Suite à une demande formulée par un autre État membre compétent pour une infraction établie conformément à la présente Directive, l'État membre requis prend des mesures pour identifier, retracer et geler ou saisir le produit du crime, les biens, les équipements ou autres instruments visés à l'article 34, paragraphe 1, de la présente Directive en vue d'une éventuelle confiscation ordonnée soit par l'État membre requérant, soit, en application d'une demande formulée au titre du paragraphe 1 du présent article, par l'État membre requis.
3. Les décisions ou actions prévues aux paragraphes 1 et 2 du présent article sont prises par l'État membre requis conformément aux dispositions de son droit national et de ses règles de procédure, ou à tout traité, accord ou arrangement bilatéral ou multilatéral auquel il peut être lié à l'égard de l'État membre requérant.
4. Chaque État membre transmet à la Commission de la CEDEAO une copie de sa législation et de sa réglementation donnant effet au présent article, ainsi que de toute modification ultérieure de ces lois et réglementations, ou une description de celles-ci. lorsqu' un État membre choisit de subordonner l'application des mesures visées aux paragraphes 1 et 2 du présent article à l'existence d'un traité pertinent, cet État membre considère la présente Directive comme la base conventionnelle nécessaire et suffisante.
5. La coopération au titre du présent article peut également être refusée ou les mesures provisoires peuvent être levées si l'État membre requis ne reçoit pas de preuves suffisantes et en temps opportun ou si le bien est d'une valeur minime.
6. Avant de lever toute mesure provisoire prise en application du présent article, l'État membre requis donne, dans la mesure du possible, à l'État membre requérant la possibilité de présenter les motifs qui justifient le maintien de la mesure.
7. Les dispositions du présent article ne sauraient être interprétées comme portant atteinte aux droits des tiers de bonne foi. Chaque Etat membre envisage de conclure des traités, accords ou arrangements bilatéraux ou multilatéraux afin de renforcer l'efficacité de la coopération internationale menée en application du présent article.

Article 49 – Réseau 24h/24 et 7j/7

1. Chaque Etat membre désigne un point de contact national disponible 24 heures sur 24 et 7 jours sur 7 afin de fournir une assistance immédiate aux fins d'enquêtes ou de poursuites concernant des infractions pénales relevant du champ d'application de la présente Directive.
2. Chaque point de contact désigné a le pouvoir de :
 - a. fournir des conseils techniques aux autres interlocuteurs ;
 - b. faciliter la conservation des données et la divulgation partielle des données de trafic conformément aux articles 28 et 29 de la présente Directive ;

- c. appuyer la collecte de preuves, la fourniture d'informations juridiques et la localisation des suspects ;
 - d. faciliter et accélérer la communication avec l'autorité nationale compétente en matière d'entraide judiciaire ;
 - e. fournir des données informatiques pour prévenir une situation d'urgence ;
 - f. fournir des coordonnées accessibles et des informations sur les procédures aux autres points de contact ;
 - g. transmettre sans délai les demandes officielles reçues à l'autorité nationale compétente ;
 - h. maintenir une communication directe avec les points de contact étrangers, les forces de l'ordre et les réseaux internationaux, et encourager le partage d'informations avant toute demande d'entraide judiciaire ;
 - i. échanger, le cas échéant, des informations de manière informelle avec ses homologues étrangers ;
 - j. participer à des enquêtes conjointes ou à des groupes de travail avec des autorités étrangères ou régionales en vue de détecter, de prévenir, d'enquêter et de poursuivre les infractions relevant du champ d'application de la présente Directive ; et
 - k. Utiliser des plateformes et des réseaux sécurisés pour l'échange d'informations et de données.
3. Chaque Etat membre veille à ce que le point de contact désigné dispose des ressources et des capacités techniques nécessaires pour communiquer de manière sécurisée et efficace avec les autres points de contact dans les meilleurs délais. Si le point de contact désigné par un Etat membre ne relève pas de l'autorité ou des autorités, de cet Etat membre, compétentes en matière d'entraide judiciaire, il veille à pouvoir se coordonner avec cette ou ces autorités dans les meilleurs délais.
 4. Chaque Etat membre veille à ce que du personnel formé et équipé soit disponible pour assurer le fonctionnement du réseau 24 heures sur 24 et 7 jours sur 7.
 5. Chaque Etat membre peut également utiliser et renforcer les réseaux autorisés existants de points de contact, le cas échéant et dans les limites de leur législation nationale, y compris les réseaux fonctionnant 24 heures sur 24 et 7 jours sur 7 établis en vertu d'autres instruments internationaux ou régionaux ou les réseaux fonctionnant 24 heures sur 24 et 7 jours sur 7 pour la criminalité informatique de INTERPOL ou le SIPAO pour une coopération policière rapide et d'autres méthodes de coopération en matière d'échange d'informations.

CHAPITRE VI – MISE EN ŒUVRE

Article 50 – Mise en œuvre

1. Chaque Etat membre adopte les mesures législatives, réglementaires et administratives nécessaires pour se conformer à la présente Directive au plus tard trois (3) ans à compter de sa signature.
2. Les mesures visées au paragraphe 1 du présent article font référence à la présente Directive ou être accompagnées d'une telle référence lors de leur publication officielle.
3. Chaque Etat membre informe la Commission de la CEDEAO des mesures qu'il adopte pour se conformer à la présente Directive.
4. Chaque Etat membre notifie au président de la Commission les difficultés qu'il rencontre pour mettre en œuvre la présente Directive. Le président de la Commission fait rapport de ces difficultés à la prochaine session du Conseil des ministres, lequel prend alors les mesures appropriées pour assurer la mise en œuvre effective de la présente Directive.

CHAPITRE VII – DISPOSITIONS FINALES

Article 51 Publication

1. La présente **Directive C/DIR.2/7/26** est publiée au Journal officiel de la Communauté par la Commission dans un délai de trente (30) jours à compter de la date de sa signature par le Président du Conseil des ministres.
2. Elle est également publiée dans le même délai par chaque État dans son Journal Officiel après notification par la Commission.

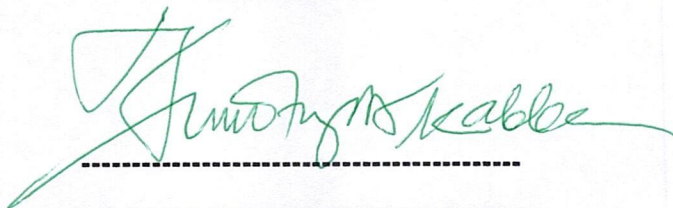
Article 52 Entrée en vigueur

La présente Directive C/DIR.2/7/26 entre en vigueur dès sa publication.

FAIT À FREETOWN, LE 17 JUILLET 2026.

POUR LE CONSEIL,

LE PRESIDENT



S.E. ALHAJI MUSA TIMOTHY KABBA