



Projet de Loi n°042/2026 du 07 juillet 2026 relative à lutte contre la cybercriminalité

EXPOSE DES MOTIFS

Depuis l'adoption de la loi n°2014-006 du 17 juillet 2014 sur la lutte contre la cybercriminalité, les technologies de l'information et de la communication ont connu une évolution particulièrement rapide, favorisant le développement de nouveaux services numériques, de nouvelles formes d'échanges économiques ainsi que de nouveaux usages reposant notamment sur les réseaux sociaux, les services financiers numériques, les cryptoactifs et les systèmes d'intelligence artificielle.

Parallèlement à ces progrès, les modes opératoires de la criminalité ont profondément évolué. Les infractions commises au moyen des technologies numériques sont devenues plus sophistiquées, plus transnationales et plus difficiles à détecter. Les escroqueries en ligne organisées, les usurpations d'identité numérique, les atteintes aux systèmes d'information, les fraudes utilisant les services de monnaie électronique et les cryptoactifs, la diffusion de contenus présentant des abus sexuels sur enfants, les campagnes de désinformation automatisées ainsi que l'utilisation malveillante de systèmes d'intelligence artificielle constituent désormais des menaces majeures pour la sécurité publique, l'économie nationale et les droits fondamentaux des citoyens.

Dans le même temps, la communauté internationale a considérablement renforcé la coopération destinée à prévenir et à réprimer ces nouvelles formes de criminalité. L'adoption de la Convention des Nations Unies contre la cybercriminalité marque une étape importante dans l'harmonisation des législations nationales et dans le développement des mécanismes de coopération internationale en matière de collecte des preuves électroniques, d'entraide judiciaire, d'investigations numériques et de confiscation des produits des infractions.

Si la loi n°2014-006 a permis à Madagascar de se doter d'un premier cadre juridique moderne de lutte contre la cybercriminalité, plusieurs de ses dispositions ne répondent plus pleinement aux réalités technologiques actuelles. Certaines infractions émergentes ne sont pas suffisamment appréhendées, plusieurs mécanismes procéduraux doivent être adaptés aux exigences des enquêtes numériques et les moyens institutionnels de prévention, d'investigation et de coopération doivent être renforcés.

Le présent projet de loi a ainsi pour objet de moderniser le cadre juridique actuel afin de doter les autorités nationales d'un dispositif juridique plus efficace, conforme aux standards internationaux et respectueux des principes de l'État de droit ainsi que des droits et libertés fondamentaux.

Le présent Projet de Loi contient 96 articles, répartis en 12 chapitres, dont :

CHAPITRE PREMIER — DISPOSITIONS GENERALES ET DEFINITIONS

CHAPITRE II — DES DELITS RELATIFS AUX SYSTEMES D'INFORMATION

CHAPITRE III — DES INFRACTIONS LIEES AUX CRYPTOACTIFS ET AUX SYSTEMES D'INTELLIGENCE ARTIFICIELLE

CHAPITRE IV — DE LA COMPETENCE TERRITORIALE

CHAPITRE V — DES ATTEINTES AUX PERSONNES PHYSIQUES PAR LE BIAIS D'UN SYSTEME D'INFORMATION

CHAPITRE VI — DES OBLIGATIONS DES OPERATEURS ET FOURNISSEURS DE SERVICES NUMERIQUES

CHAPITRE VII — DE LA RESPONSABILITE DES PERSONNES MORALES, DE LA TENTATIVE ET DE LA RECIDIVE

CHAPITRE VIII — DES MESURES D'INVESTIGATION ET DE CONFISCATION

CHAPITRE IX — DE L'UNITE DE PROTECTION ET D'INVESTIGATION NUMERIQUE (UPIN)

CHAPITRE X — DE LA COOPERATION INTERNATIONALE EN MATIERE DE CYBERCRIMINALITE

CHAPITRE XI — DE LA PROTECTION DES VICTIMES ET DES TEMOINS

CHAPITRE XII — DISPOSITIONS TRANSITOIRES ET FINALES

Tel est l'objet de la présente Loi.



PRESIDENCE DE LA REFONDATION DE LA REPUBLIQUE

Projet de Loi n°042/2026 du 07 juillet 2026 relative à la lutte contre la cybercriminalité

L'Assemblée nationale a adopté lors de sa séance plénière en date du _____.

LE PRESIDENT DE LA REPUBLIQUE

Vu la Constitution ;

Vu la décision n° _____ du _____ de la Haute Cour Constitutionnelle ;

Vu la décision n° 10-HCC/D3 du 14 octobre 2025 accordant à l'autorité militaire compétente, représentée par le Colonel RANDRIANIRINA Michaël, l'exercice des fonctions de Chef de l'Etat ;

PROMULGUE LA LOI DONT LA TENEUR SUIT :

CHAPITRE PREMIER — DISPOSITIONS GENERALES ET DEFINITIONS

Article premier.- La présente loi a pour objet de prévenir, poursuivre et réprimer les infractions commises au moyen ou à l'encontre des systèmes d'informations, des infrastructures numériques ou des télécommunications. Elle fixe des mesures procédurales et de coopération internationale en matière de lutte contre la cybercriminalité, conformément aux engagements internationaux de la République de Madagascar.

Article 2.- Aux fins de la présente loi, on entend par :

- *Bande organisée* : le fait de constituer, d'organiser, de financer, de diriger ou de participer à un groupement ou à une entente ayant pour objet la préparation ou la commission d'infractions commises au moyen d'un système d'information ;
- *Cryptoactif* : toute représentation numérique d'une valeur ou d'un droit pouvant être transférée ou conservée électroniquement au moyen d'un registre distribué ou d'une technologie équivalente ;
- *Cryptomonnaie* : une monnaie virtuelle stockée sur un système informatique ou un portefeuille numérique, pouvant être utilisée comme moyen d'échange ou de placement ;

- *Cybercriminalité* : tout fait illégal commis au moyen d'un système d'information, des infrastructures numériques ou des télécommunications ou de tout autre réseau physique connexe ou en relation avec un système d'information ;
- *Données de contenu* : toutes données électroniques autres que les données d'abonnement ou les données relatives au trafic, correspondant au contenu même d'une communication électronique ;
- *Données informatiques* : toute représentation de faits, d'informations ou de concepts sous une forme se prêtant à un traitement informatique, y compris un programme permettant à un système d'information d'exécuter une fonction ;
- *Données relatives au trafic* : toutes les données ayant trait à une communication transitant par un système d'information, indiquant notamment son origine, sa destination, son itinéraire, sa date, son heure, sa durée, son volume ou le service utilisé ;
- *Données relatives aux personnes abonnées* : toutes informations détenues par un fournisseur de services qui concernent les personnes abonnées à ses services, autres que les données de trafic ou de contenu, et qui permettent d'établir : (i) le type de service de communication utilisé, les dispositions techniques y relatives et la période de service ; (ii) l'identité, l'adresse postale ou géographique et le numéro de téléphone de la personne abonnée, ou tout autre numéro d'accès, les informations concernant la facturation ou le paiement, disponibles sur la base d'un contrat ou d'un accord de services ; (iii) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un accord de services ;
- *Fausse information numérique* : toute allégation ou imputation d'un fait inexact ou trompeur, propagé intentionnellement par voie électronique ;
- *Infrastructure numérique* : ensemble d'équipements, de réseaux, de systèmes ou de services nécessaires au fonctionnement, à l'accès ou à l'exploitation des systèmes d'information ;
- *Intelligence artificielle* : tout système capable, pour un ensemble donné d'objectifs définis par l'homme, de générer des résultats tels que des contenus, prédictions, recommandations ou décisions influençant les environnements avec lesquels il interagit ;
- *Portefeuille numérique* : tout dispositif, logiciel ou service permettant de stocker, gérer, transférer ou sécuriser des actifs numériques, notamment des cryptoactifs ou des instruments de monnaie électronique ;
- *Procédé automatisé* : tout procédé numérique dont les actions sont exécutées, en tout ou partie, par un programme informatique sans intervention humaine directe ;
- *Réseau coordonné de manipulation* : tout ensemble de comptes, automatisés ou non, agissant de manière concertée en vue de diffuser ou d'amplifier artificiellement un contenu ou une information ;
- *Situation d'urgence* : toute situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique ou pour l'intégrité d'une infrastructure critique ;
- *Système d'information* : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, en ligne ou hors ligne, qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

Article 3.- Aucune disposition de la présente loi ne doit être interprétée comme autorisant la répression des droits de l'homme ou des libertés fondamentales, notamment des droits liés à la liberté d'expression, de conscience, d'opinion, de religion ou de conviction, de réunion pacifique et d'association.

CHAPITRE II — DES DELITS RELATIFS AUX SYSTEMES D'INFORMATION

Article 4.- Constitue un accès frauduleux le fait, pour toute personne, sans droit ni autorisation légale, d'accéder intentionnellement à tout ou partie d'un système d'information.

Article 5.- Constitue un maintien frauduleux le fait, pour toute personne, sans droit ni autorisation légale, de rester connectée intentionnellement dans un système d'information ou dans une partie d'un système d'information, ou de continuer d'utiliser un système d'information.

Article 6.- Quiconque aura accédé ou se sera maintenu dans tout ou partie d'un système d'information selon les cas prévus aux articles 4 et 5 ci-dessus, sera puni de 100 000 Ariary à 10 000 000 d'Ariary d'amende.

Lorsque l'accès ou le maintien frauduleux, dans tout ou partie du système d'information, auront, soit endommagé, effacé, détérioré, modifié, altéré ou supprimé des données informatiques contenues dans le système, soit entravé ou altéré le fonctionnement de tout ou partie de ce système, la peine sera celle de six mois à cinq ans d'emprisonnement et de 100 000 Ariary à 10 000 000 Ariary ou l'une de ces peines seulement.

Article 7.- Quiconque aura, frauduleusement, introduit, endommagé, effacé, détérioré, modifié, altéré ou supprimé des données informatiques ou agi frauduleusement de manière à modifier ou à supprimer leur mode de traitement ou de transmission sera puni d'un emprisonnement de deux ans à dix ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

Article 8.- Quiconque aura, frauduleusement, fait usage de données informatiques volontairement endommagées, effacées, détériorées, modifiées, ou altérées sera puni d'un emprisonnement de deux ans à cinq ans d'emprisonnement et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary, ou l'une de ces peines seulement.

Article 9.- Quiconque aura introduit, altéré, effacé ou supprimé des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles, sera puni d'un emprisonnement de deux ans à dix ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary, ou l'une de ces peines seulement.

Article 10.- Quiconque participe à un groupement formé ou à une entente établie en vue de préparer, commettre, faciliter la commission ou le recel, caractérisés par un ou plusieurs faits matériels, d'une ou plusieurs des infractions prévues par les articles 4, 5, 7, 8 et 11 est puni des peines prévues pour l'infraction elle-même.

Article 11.- Est qualifiée d'atteinte à l'intégrité, toute altération ou entrave au fonctionnement du système d'information.

Est qualifiée d'altération au fonctionnement d'un système d'information, toute action consistant à fausser le fonctionnement dudit système pour lui faire produire un résultat autre que celui pour lequel il est normalement conçu et utilisé.

Est qualifiée d'entrave au fonctionnement d'un système d'information, toute action ayant pour effet, objet ou finalité de paralyser un système d'information par l'introduction, la transmission, l'endommagement, l'effacement, la modification, l'altération ou la suppression de données informatiques.

Article 12.- Quiconque aura entravé ou altéré le fonctionnement de tout ou partie d'un système d'information, sera puni d'un emprisonnement de deux ans à dix ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

Article 13.- Quiconque aura intercepté par des moyens techniques, des données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

Article 14.- Le fait, frauduleusement, de produire, importer, détenir, offrir, céder, diffuser ou mettre à disposition :

1°) un équipement, un dispositif, y compris un programme informatique, un mot de passe, un code d'accès, une signature électronique, des justificatifs d'accès ou des données informatiques similaires, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs des infractions prévues aux articles 4, 5, 7, 8, 11, 12 de la présente loi ;

2°) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information pour commettre l'une des infractions prévues aux articles précités,

est puni des peines prévues respectivement pour l'infraction elle-même.

Le présent article est sans application lorsque la production, l'importation, la détention, l'offre, la cession, la diffusion ou la mise à disposition n'a pas pour but de commettre l'une des infractions visées aux articles précités, comme dans le cas d'essai autorisé, de la recherche ou de protection d'un système d'information.

Article 15.- Quiconque aura causé un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système d'information, dans l'intention d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui, sera puni d'un emprisonnement de deux ans à dix ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

Article 16.- Constitue une infraction de fraude ou escroquerie numérique le fait, pour toute personne :

1° D'utiliser intentionnellement et sans droit un système d'information afin de tromper autrui sur des circonstances factuelles ou au moyen d'un contenu, d'un profil ou d'une identité numérique falsifiés ;

2° D'inciter une personne, par manœuvres frauduleuses, sollicitations affectives ou propositions fictives d'investissement, à accomplir ou à omettre un acte qu'elle n'aurait pas fait autrement ;

3° Dans l'intention d'obtenir illicitement un avantage financier, des données à caractère personnel, des cryptoactifs ou tout autre bien, à son profit ou au profit d'autrui.

L'auteur est puni de deux à dix ans d'emprisonnement et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary, ou de l'une de ces peines seulement.

Les peines sont portées au double lorsque les faits :

- sont commis en bande organisée,
- présentent un caractère transnational,

- ou sont facilités, automatisés ou amplifiés au moyen d'un système d'intelligence artificielle.

Article 17.- Est puni d'un emprisonnement de deux ans à cinq ans et d'une amende de 5 000 000 Ariary à 50 000 000 Ariary, le fait, au moyen d'un système d'information :

1° de tromper une personne, par la création d'un faux compte, d'un faux profil ou par l'usage d'une fausse identité numérique, afin de l'inciter à remettre des fonds, des valeurs ou tout bien quelconque ;

2° de créer, d'administrer ou d'utiliser un compte, une page ou un groupe numérique destiné à faciliter la commission d'une infraction pénale ;

3° d'utiliser frauduleusement un compte, un profil ou une identité numérique appartenant à autrui.

Les peines sont portées au double lorsque les faits sont commis en bande organisée ou au moyen d'un réseau coordonné de manipulation au sens de l'article 2 de la présente loi.

Article 18.- Est puni des mêmes peines que celles prévues à l'article 17 le fait de créer, d'organiser, d'animer ou de participer sciemment à un réseau coordonné de manipulation de l'information, au moyen de faux comptes, de comptes automatisés ou de tout autre procédé, en vue de commettre ou de faciliter la commission d'une infraction prévue par la présente loi.

CHAPITRE III — DES INFRACTIONS LIEES AUX CRYPTOACTIFS ET AUX SYSTEMES D'INTELLIGENCE ARTIFICIELLE

Article 19.- Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10 000 000 Ariary à 200 000 000 Ariary quiconque utilise, transfère, reçoit, convertit ou dissimule des cryptoactifs, des actifs numériques ou des services financiers numériques dans le but de préparer, faciliter ou dissimuler la commission d'une infraction prévue par la présente loi ou par toute autre législation pénale.

Lorsque les faits sont commis dans le cadre d'une organisation criminelle ou ont pour objet le blanchiment du produit d'une infraction, les peines prévues par la législation relative à la lutte contre le blanchiment de capitaux demeurent applicables lorsqu'elles sont plus sévères.

Article 20.- Est qualifiée d'utilisation illégale de cryptomonnaies et de services de mobile banking, le fait, dans le cadre d'activités criminelles telles que la traite des êtres humains, l'escroquerie en bande organisée, ou le blanchiment d'argent, d'utiliser, de transférer, de recevoir ou de convertir des cryptomonnaies ou d'utiliser des services de mobile banking pour dissimuler l'origine ou la destination de fonds issus d'infractions.

Article 21.- Quiconque aura, frauduleusement, utilisé, transféré, reçu ou converti des cryptomonnaies, ou utilisé des services de mobile banking, afin de dissimuler, de faciliter ou de favoriser la circulation, le transfert ou la conversion de fonds provenant d'une infraction, sera puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10 000 000 Ariary à 200 000 000 Ariary.

Article 22.- Est puni des peines prévues à l'article 33 de la présente loi le fait de produire, générer, modifier, diffuser, détenir, mettre à disposition, vendre ou acquérir, au moyen d'un système d'intelligence artificielle, tout contenu représentant ou simulant de manière réaliste un mineur se livrant à un acte sexuellement explicite ou se trouvant dans une situation d'exploitation ou d'abus sexuel.

Article 23.- Les personnes physiques ou morales qui développent, exploitent ou mettent à disposition des systèmes d'intelligence artificielle doivent mettre en œuvre les mesures

raisonnables destinées à prévenir l'utilisation de leurs services à des fins criminelles, dans le respect des lois relatives à la protection des données à caractère personnel et des libertés fondamentales.

Elles sont tenues de coopérer avec les autorités judiciaires dans les conditions prévues par la loi. À défaut de législation spécifique encadrant cette coopération, les personnes mentionnées au premier alinéa répondent, dans un délai raisonnable, à toute réquisition judiciaire relative à la prévention, la détection ou la répression des infractions commises au moyen de leurs systèmes, selon des modalités précisées par voie réglementaire.

CHAPITRE IV — DE LA COMPETENCE TERRITORIALE

Article 24.- Par dérogation aux dispositions du Code de procédure pénale relatives à la compétence territoriale, les infractions prévues par la présente loi peuvent être poursuivies, devant :

- 1° la juridiction du lieu de la résidence de la victime au moment des faits ;
- 2° la juridiction du lieu de constatation du préjudice ou de découverte des effets de l'infraction.

Les dispositions du présent article s'appliquent sans préjudice des règles de compétence résultant de l'organisation judiciaire et des conventions internationales auxquelles Madagascar est partie.

Par dérogation aux dispositions du Code de procédure pénale et du premier alinéa du présent article, le tribunal de première instance d'Antananarivo est seul compétent pour la poursuite, l'instruction et le jugement des infractions prévues par la présente loi lorsqu'elles présentent un caractère complexe, notamment en raison de leur ampleur, du nombre de victimes ou de leur incidence sur une infrastructure critique. Un décret pris sur proposition du Ministre de la Justice précise les critères de qualification des affaires complexes au sens du présent alinéa.

Article 25.- La présente loi est également applicable aux infractions qu'elle réprime lorsque :

- 1° L'infraction est commise à bord d'un navire battant pavillon malgache ou d'un aéronef immatriculé conformément au droit malgache ;
- 2° L'infraction est commise par un ressortissant malgache ou par une personne apatride résidant habituellement à Madagascar ;
- 3° L'infraction est commise à l'encontre d'un ressortissant malgache ;
- 4° L'infraction est commise à l'encontre de l'État malgache ou d'une de ses administrations publiques.

CHAPITRE V — DES ATTEINTES AUX PERSONNES PHYSIQUES PAR LE BIAIS D'UN SYSTEME D'INFORMATION

Article 26.- Quiconque, par écrit anonyme ou signé, image, symbole ou emblème, par le biais d'un support informatique ou électronique, aura menacé autrui d'assassinat, d'empoisonnement ou de tout autre attentat contre les personnes, punissable de travaux forcés à perpétuité ou de la déportation, sera, dans le cas où la menace aura été faite avec ordre de déposer une somme d'argent dans un lieu indiqué, ou de remplir toute autre condition, puni d'un emprisonnement de deux à cinq ans et d'une amende de 100 000 Ariary à 1 350 000 Ariary.

Le coupable pourra, en outre, être privé des droits mentionnés en l'article 42 du Code pénal pendant cinq ans au moins et dix ans au plus à compter du jour où il aura subi sa peine.

Le coupable pourra être interdit de séjour pendant deux ans au moins et cinq ans au plus, à dater du jour où il aura subi sa peine.

Si cette menace n'a été accompagnée d'aucun ordre ou condition, la peine sera d'un emprisonnement d'une année au moins et de trois ans au plus, et d'une amende de 100 000 Ariary à 1 350 000 Ariary. Dans ce cas, la peine de l'interdiction de séjour pourra être prononcée contre le coupable.

Article 27.- Si la menace faite avec ordre ou sous condition a été verbale, par le biais d'un support informatique ou électronique, le coupable sera puni d'un emprisonnement de six mois à deux ans, et d'une amende de 100 000 Ariary à 540 000 Ariary. Dans ce cas, la peine de l'interdiction de séjour pourra être prononcée contre le coupable.

Article 28.- Lorsque les menaces prévues à l'article 26 sont commises envers une personne ou un groupe de personnes à raison de leur origine, de leur sexe, de leur appartenance ou de leur non appartenance à une ethnie, une nation, une race ou une religion déterminée, réelle ou supposée, elles sont punies d'un emprisonnement de cinq ans à dix ans et d'une amende de 1 000 000 Ariary à 10 000 000 Ariary.

Le coupable pourra, en outre, être privé des droits mentionnés en l'article 42 du Code pénal pendant cinq ans au moins et dix ans au plus à compter du jour où il aura subi sa peine.

Le coupable pourra être interdit de séjour pendant deux ans au moins et cinq ans au plus, à dater du jour où il aura subi sa peine.

Article 29.- Constitue un cyberharcèlement le fait de tenir de manière répétée, par voie électronique, à l'égard d'une même personne, des propos ou d'adopter des comportements ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale.

Le cyberharcèlement est puni d'un emprisonnement d'un an à trois ans et d'une amende de 2 000 000 Ariary à 20 000 000 Ariary.

Les peines sont portées à un emprisonnement de deux ans à cinq ans et à une amende de 4 000 000 Ariary à 40 000 000 Ariary lorsque les faits sont commis :

1° par plusieurs personnes agissant en qualité d'auteur ou de complice, sans qu'elles constituent nécessairement une bande organisée ;

2° à l'égard d'un mineur ou d'une personne particulièrement vulnérable en raison de son âge, d'une maladie, d'une infirmité ou d'une déficience physique ou psychique ;

3° à raison du sexe, de l'orientation, de l'origine, de l'appartenance ou de la non-appartenance, réelle ou supposée, de la victime à une ethnie, une nation, une race ou une religion déterminée.

Article 30.- Quiconque aura sciemment, sur un support informatique ou électronique, usurpé l'identité de toute personne physique ou morale, ou une ou plusieurs données de toute nature permettant de l'identifier, en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à la considération de ces derniers, sera puni d'un emprisonnement de six mois à dix ans et d'une amende de 600 000 Ariary à 18 000 000 Ariary.

Lorsque l'usurpation d'identité est commise en bande organisée, au moyen de procédés automatisés ou dans le but de faciliter la commission d'une infraction, son auteur est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10 000 000 Ariary à 50 000 000 Ariary.

Les mêmes peines sont applicables lorsque l'infraction est commise au moyen d'un système d'intelligence artificielle ou de tout procédé technologique destiné à tromper sur l'identité d'une personne physique ou morale.

Article 31.- La diffusion ou toute autre forme de mise à disposition du public, par le biais d'un support informatique ou électronique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international, sera punie de six mois à cinq ans d'emprisonnement et d'une amende de 100 000 Ariary à 10 000 000 Ariary.

Article 32.- Quiconque aura, intentionnellement et sans droit, diffusé, vendu, distribué, transmis, publié, partagé ou mis autrement à disposition une image intime d'une personne au moyen d'un système d'information et de communication, sans le consentement de la personne représentée sur l'image, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 5 000 000 Ariary à 20 000 000 Ariary, ou l'une de ces deux peines seulement.

Par « image intime », on entend un enregistrement visuel d'une personne de plus de 18 ans réalisé par quelque moyen que ce soit, y compris une photographie ou un enregistrement vidéo, de nature sexuelle, où les organes sexuels de la personne sont exposés ou où cette personne se livre à un acte sexuel qui était à caractère privé au moment de l'enregistrement.

Article 33.- Infractions relatives aux contenus d'abus sexuels sur enfants et à l'exploitation sexuelle d'enfants en ligne.

1° Par « contenu présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants », on entend tout contenu visuel, écrit ou sonore, qui dépeint, décrit ou représente une personne de moins de 18 ans :

- a) Se livrant à un acte sexuel réel ou simulé, y compris le fait d'accomplir des gestes à caractère sexuel sur sa personne ou sur la personne d'autrui ;
- b) En présence d'une personne qui se livre à un acte sexuel ;
- c) Dont les organes sexuels sont exhibés à des fins principalement sexuelles ; ou
- d) Qui est soumise à des actes de torture ou à des peines ou traitements cruels, inhumains ou dégradants, lorsque ce contenu est à caractère sexuel.

2° Est puni des travaux forcés à temps, le fait de fixer, de produire ou de faire produire, de financer la production, par le biais d'un système d'information et de communication, des contenus visuels, écrits ou sonores présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants ;

2° bis Est puni de cinq à dix ans d'emprisonnement et d'une amende de 20 000 000 à 100 000 000 Ariary le fait de diffuser, de transmettre, d'offrir, de mettre à disposition, de distribuer, d'importer, d'exporter ou de rendre accessible, par tout moyen de communication électronique, des contenus visuels, écrits ou sonores présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants ;

2° ter Est puni de deux à cinq ans d'emprisonnement et d'une amende de 2 000 000 à 10 000 000 Ariary le fait de se procurer, de détenir, d'enregistrer ou de conserver, en connaissance de son caractère illicite, des contenus présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants stockés dans un système d'information et de communication ou sur tout autre support de stockage, ou de consulter habituellement des services de communication en ligne mettant à disposition de tels contenus ;

3° Le financement, direct ou indirect, de l'une des infractions mentionnées aux points 2°, 2° bis et 2° ter du présent article est passible des mêmes peines que celles prévues pour l'infraction financée.

4° La tentative est punie des mêmes peines.

5° Les dispositions du présent article sont également applicables aux contenus visuels, écrits ou sonores d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. Sont assimilés à des contenus présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants :

- l'image ou la représentation d'un mineur se livrant à un comportement sexuellement explicite ;
- l'image ou la représentation d'une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;
- l'image réaliste représentant un mineur se livrant à un comportement sexuellement explicite. L'expression « image réaliste » désigne notamment l'image altérée d'une personne physique, en tout ou partie créée par des méthodes numériques.

6° Les peines prévues au présent article sont prononcées sans possibilité de sursis. La décision de condamnation est assortie de l'interdiction définitive d'exercer une activité en lien avec les enfants.

Article 34.- Les plateformes de signalement, qu'elles soient gouvernementales ou non gouvernementales, opérant dans le domaine de la surveillance et de la protection des enfants en ligne, sont habilitées à recevoir et à transmettre à l'UPIN toute information relative à des faits susceptibles de constituer les infractions prévues par l'article 33 de la présente loi. Ces plateformes collaborent avec les autorités compétentes pour la détection, le signalement et le retrait des contenus illicites, dans le respect des dispositions de la loi sur la protection des données à caractère personnel et des droits des enfants.

Article 35.- Quiconque aura attenté aux mœurs, par l'utilisation d'un support informatique ou électronique, en excitant, favorisant ou facilitant, pour satisfaire les passions d'autrui, la débauche, la corruption ou la prostitution enfantine de l'un ou de l'autre sexe, est puni des travaux forcés à temps, dans chacun des deux cas suivants :

1° Lorsque les faits sont commis dans des établissements d'enseignement ou d'éducation ou dans des locaux de l'administration, ainsi que lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux ;

2° Lorsque les faits ont été commis en bande organisée, les coupables seront punis des travaux forcés à perpétuité.

Article 36.- Le fait pour un majeur de faire des propositions sexuelles à un mineur ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans à cinq ans d'emprisonnement et de 2 000 000 Ariary à 10 000 000 Ariary d'amende. Ces peines sont portées de cinq ans à dix ans d'emprisonnement lorsque les propositions ont été suivies d'une rencontre.

Article 37.- Constitue un harcèlement sexuel en ligne le fait, par le biais d'un système d'information ou de communication, de soumettre une personne, de manière répétée ou non, à des messages, propos, images ou sollicitations à connotation sexuelle, notamment sous forme de messages, images ou enregistrements à contenu sexuel explicite, dans le but d'obtenir d'elle

un acte ou un comportement à caractère sexuel, ou de la contraindre, l'intimider ou la manipuler à des fins sexuelles.

Le harcèlement sexuel en ligne est puni d'un emprisonnement d'un an à trois ans et d'une amende de 2 000 000 Ariary à 10 000 000 Ariary.

Les peines sont portées à un emprisonnement de deux ans à cinq ans et à une amende de 4 000 000 Ariary à 20 000 000 Ariary lorsque les faits sont commis sur un mineur.

Article 38.- Constitue une sextorsion le fait de menacer une personne de diffuser ou de rendre accessible à des tiers un contenu à caractère sexuel la représentant, dans le but de la contraindre à remettre une somme d'argent ou un avantage matériel, à produire ou transmettre un contenu sexuel supplémentaire, à poser, se filmer ou se photographier dans une attitude sexuelle, ou de lui imposer toute autre forme de pression à des fins sexuelles.

La sextorsion est punie d'un emprisonnement de deux ans à cinq ans et d'une amende de 5 000 000 Ariary à 25 000 000 Ariary.

Les peines sont portées de cinq ans à dix ans d'emprisonnement et à une amende de 10 000 000 Ariary à 50 000 000 Ariary lorsque les faits sont commis sur un mineur.

Dans tous les cas, les peines sont portées aux travaux forcés à temps lorsque les faits ont conduit la victime à s'infliger des blessures ou à attenter à sa vie.

Article 39.- Est puni d'un emprisonnement de six mois à deux ans et d'une amende de 1 000 000 Ariary à 5 000 000 Ariary le fait de créer, produire, générer, modifier ou altérer, au moyen d'un système d'intelligence artificielle ou de tout autre procédé de truchement numérique, une image, un enregistrement sonore ou une vidéo représentant de manière suffisamment réaliste une personne majeure, de nature à faire croire qu'il s'agit d'un contenu authentique, en lui attribuant des propos, des actes, une attitude ou une situation qu'elle n'a pas tenus ou vécus, dans l'intention de porter atteinte à son honneur, à sa réputation, à sa dignité ou à son intégrité morale.

Sont punis des mêmes peines le fait, en connaissance du caractère falsifié du contenu, de le diffuser, transmettre, publier, partager, rendre accessible ou mettre à la disposition d'un tiers ou du public, ainsi que le fait, après avoir été informé de ce caractère falsifié, d'en poursuivre volontairement la diffusion.

La juridiction ordonne le retrait du contenu litigieux, ainsi que toute mesure propre à faire cesser sa diffusion, dans les conditions prévues au Chapitre VI de la présente loi.

Article 40.- Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique, à caractère raciste ou xénophobe, ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de deux ans à cinq ans d'emprisonnement et de 10 000 000 Ariary à 20 000 000 Ariary d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues à l'article 346 du Code pénal et au présent article sont commises par la voie de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

CHAPITRE VI — DES OBLIGATIONS DES OPERATEURS ET FOURNISSEURS DE SERVICES NUMERIQUES

Article 41.- Les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications ou de communications électroniques sont tenus d'effacer ou de rendre anonyme toutes les données relatives au trafic, sous réserve des dispositions suivantes.

Article 42.- Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition du pouvoir judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines données techniques. Un décret détermine, dans les limites fixées par l'article 41, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et des prestataires de services et la nature des communications.

Article 43.- Pour les besoins de la facturation et du paiement des prestations de communications électroniques ou de services de télécommunications, les opérateurs et les prestataires de services peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement, les données techniques déterminées par décret.

Article 44.- Les opérateurs et les prestataires de services peuvent, en outre, réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'utilisateur et l'opérateur ou le prestataire de services.

Les opérateurs ou prestataires de service peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

Article 45.- Sans préjudice des dispositions des articles 41 et suivants et sous réserve des nécessités des enquêtes judiciaires, le consentement de l'abonné est requis pour toute éventuelle utilisation ou conservation des données permettant de localiser son équipement terminal.

Sa rétractation ou sa suspension est possible dès que l'abonné en fait connaître, par tout moyen, à l'opérateur ou au prestataire de services.

Article 46.- Les données conservées et traitées dans les conditions définies aux articles 41 et suivants portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et les prestataires de services, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

Les opérateurs et les prestataires de services prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi relative à la protection des données à caractère personnel.

Article 47.- Les opérateurs de communications électroniques, les fournisseurs d'accès à Internet, les fournisseurs de services numériques ainsi que les opérateurs de services financiers

numériques sont tenus de conserver, pendant la durée fixée par la réglementation en vigueur, les données dont la conservation est nécessaire aux enquêtes relatives aux infractions prévues par la présente loi.

Ils sont tenus de communiquer ces données aux autorités judiciaires compétentes dans les conditions prévues par la loi.

Article 48.- Les opérateurs mettant à disposition des services de monnaie électronique ou de portefeuilles numériques sont tenus de mettre en œuvre des procédures appropriées d'identification de leurs clients et de signaler aux autorités compétentes toute opération susceptible de présenter un caractère frauduleux ou criminel, conformément à la législation relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Article 49.- Les opérateurs de services de mobile banking et de transfert d'argent électronique sont tenus de rapporter à l'UPIN, sans délai, l'identité complète de toute personne physique ou morale ayant effectué, en l'espace de deux (2) jours consécutifs, une ou plusieurs transactions dont le montant total est supérieur ou égal à 40 000 000 Ariary. Cette déclaration doit inclure les détails de la transaction, l'identité de l'émetteur et du bénéficiaire, les coordonnées des comptes et portefeuilles numériques utilisés, ainsi que tout élément permettant d'identifier l'origine des fonds.

Le défaut de déclaration par l'opérateur est puni d'une amende de 50 000 000 Ariary à 200 000 000 Ariary.

Article 50.- Le fait pour un opérateur ou prestataire de services de ne pas se conformer aux obligations de conservation des données, de déclaration des transactions suspectes ou de ne pas faciliter l'accès de l'UPIN à ses bases de données est puni d'une amende de 100 000 000 Ariary à 500 000 000 Ariary.

Article 51.- Le refus injustifié de satisfaire aux obligations prévues par le présent chapitre ou l'entrave aux investigations légalement conduites par les autorités compétentes est puni d'une amende de 100 000 000 Ariary à 500 000 000 Ariary, sans préjudice des autres sanctions pénales ou administratives prévues par les lois en vigueur.

Article 52.- La responsabilité pénale du créateur de contenu, de l'administrateur d'un groupe ou du gestionnaire d'une page numérique peut être engagée à raison d'un contenu manifestement illicite publié par un tiers sur cet espace numérique lorsqu'il est établi qu'il en avait connaissance et qu'il s'est volontairement abstenu de le retirer après notification ou décision judiciaire.

Les peines encourues sont celles prévues pour l'infraction constituée par le contenu en cause.

Article 53.- En cas de contenu manifestement illicite au regard des infractions prévues par la présente loi, la victime ou toute personne ayant intérêt à agir dépose plainte auprès des officiers de police judiciaire territorialement compétents ou de l'UPIN.

Après constatation des faits, l'officier de police judiciaire saisit l'UPIN par voie de réquisition, visée par le Procureur de la République, aux fins d'ordonner en urgence le retrait ou le blocage provisoire du contenu litigieux.

Le ministère public peut également saisir directement l'UPIN aux mêmes fins.

La mesure de retrait ou de blocage est exécutée sous le contrôle de l'autorité judiciaire et notifiée, le cas échéant, aux fournisseurs de services numériques concernés, qui sont tenus de s'y conformer sans délai sous peine des sanctions prévues à l'article 51 de la présente loi.

Article 54.- Est puni des peines prévues pour l'infraction constituée par le contenu en cause, quiconque, en connaissance de son caractère manifestement illicite ou malgré une mesure de retrait ou de blocage prononcée en application de l'article 53, maintient, republie ou partage sciemment ce contenu.

Article 55.- Tout fournisseur de services numériques exerçant une activité significative à Madagascar, au sens des critères fixés par décret, désigne un représentant ou un point de contact local chargé de faciliter les échanges avec les autorités nationales, notamment l'UPIN, aux fins d'exécution des obligations prévues par la présente loi.

Le défaut de désignation est puni de l'amende prévue à l'article 49.

Article 56.- Le fait, pour les opérateurs ou les prestataires de services chargés de l'exploitation de réseaux et de services de télécommunications ou de communications électroniques, de ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives au trafic, dans les cas où ces opérations sont prescrites par la présente loi, est puni d'une amende de 1 000 000 Ariary à 150 000 000 Ariary.

Si le fait a été commis frauduleusement, avec l'intention de nuire, par un de leurs agents, il sera puni d'une peine d'emprisonnement de six mois à cinq ans et d'une amende de 100 000 Ariary à 10 000 000 Ariary, ou de l'une de ces deux peines seulement.

Article 57.- Le fait, pour les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications ou de communications électroniques, de ne pas conserver les données techniques dans les conditions où cette conservation est exigée par la présente loi, est puni d'une amende de 1 000 000 Ariary à 150 000 000 Ariary.

Si le fait a été commis frauduleusement par un de leurs agents, il sera puni d'une peine d'emprisonnement de six mois à cinq ans et d'une amende de 100 000 Ariary à 10 000 000 Ariary, ou de l'une de ces deux peines seulement.

Article 58.- Les opérateurs exploitant un réseau de télécommunications ouvert au public ou fournissant des services de télécommunications au public sont tenus de mettre en œuvre les dispositifs techniques destinés à interdire, à l'exception des numéros d'urgence, l'accès à leurs réseaux ou à leurs services des communications émises au moyen de terminaux mobiles, identifiés et qui leur ont été déclarés volés. Ces terminaux doivent être bloqués à compter de la réception par l'opérateur concerné de la déclaration officielle de vol, transmise par l'abonné.

Toutefois, l'officier de police judiciaire peut requérir des opérateurs, après accord donné par le Procureur de la République ou le juge d'instruction, de ne pas appliquer les dispositions du premier alinéa.

CHAPITRE VII — DE LA RESPONSABILITE DES PERSONNES MORALES, DE LA TENTATIVE ET DE LA RECIDIVE

Article 59.- Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par les articles 60 et 61, des infractions prévues par la présente loi.

Article 60.- Les peines encourues par les personnes morales sont :

- l'amende ;
- l'affichage ou la diffusion de la décision prononcée, le Tribunal décidant de l'insertion de cette publication ;

- l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- la fermeture définitive ou pour une durée de cinq ans au plus des établissements, ou de l'un ou de plusieurs d'entre eux, ayant servi à commettre les faits incriminés ;
- l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus.

Article 61.- Quiconque tente de commettre une des infractions prévues par la présente loi est puni des peines prévues pour l'infraction elle-même.

Article 62.- Il en sera également ainsi pour les délits réprimés par les articles 4 à 18 de la présente loi.

Article 63.- Quiconque, ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse de remettre ladite convention au pouvoir judiciaire ou de la mettre en œuvre, sur ses réquisitions délivrées en application des titres I et VI du livre II du Code de procédure pénale, est puni d'un emprisonnement de un an à cinq ans et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée de deux ans à dix ans d'emprisonnement et d'une amende de 2 000 000 Ariary à 100 000 000 Ariary ou l'une de ces peines seulement.

CHAPITRE VIII — DES MESURES D'INVESTIGATION ET DE CONFISCATION

Article 64.- Les autorités judiciaires peuvent ordonner le gel, la saisie et la confiscation des matériels informatiques, des actifs numériques, des cryptoactifs, des comptes électroniques et de tout bien ayant servi ou destiné à servir à la commission des infractions prévues par la présente loi, ainsi que des produits qui en sont issus, conformément au Code de procédure pénale et aux conventions internationales ratifiées par Madagascar.

La confiscation porte sur l'intégralité des biens saisis, sans restitution possible des matériels informatiques ayant servi à commettre l'infraction, ces derniers étant considérés comme des instruments du crime.

L'État peut saisir à titre conservatoire tout actif numérique dont la valeur est présumée correspondre au produit de l'infraction.

Article 65.- Les officiers de police judiciaire peuvent intervenir d'office, sans attendre une plainte ou une réquisition préalable, en cas d'identification d'un message, d'une image ou de tout autre contenu à caractère pornographique adressé à un enfant ou le représentant, et procéder aux premières constatations et mesures conservatoires utiles, à charge d'en aviser sans délai le Procureur de la République.

Article 66.- Les preuves électroniques régulièrement recueillies conformément aux dispositions de la présente loi ont la même force probante que les autres moyens de preuve admis en matière pénale. Leur intégrité, leur authenticité et leur traçabilité doivent être garanties durant toute la procédure.

Article 67.- De la préservation accélérée des données stockées.

1° Les autorités judiciaires peuvent, dans le cadre d'une enquête relative aux infractions prévues par la présente loi, ordonner à toute personne détenant des données électroniques stockées de

les préserver rapidement, lorsqu'il existe des raisons de penser que ces données sont particulièrement susceptibles d'être perdues ou modifiées.

2° L'ordonnance de préservation est délivrée par le Procureur de la République ou le juge d'instruction. Elle précise les données à préserver, l'identité du détenteur, et la durée de la préservation, qui ne peut excéder 90 jours, renouvelable une fois.

3° La personne tenue de préserver les données est tenue au secret sur la mesure dont elle fait l'objet.

Article 68.- De l'injonction de produire.

1° Les autorités judiciaires peuvent, par ordonnance motivée, enjoindre à toute personne présente sur le territoire national de communiquer des données électroniques spécifiées qui sont en sa possession ou sous son contrôle et qui sont stockées dans un système d'information ou sur un support de stockage.

2° Elles peuvent également enjoindre à un fournisseur de services offrant des prestations sur le territoire national de communiquer les données relatives aux personnes abonnées qui sont en sa possession ou sous son contrôle concernant ces prestations.

Article 69.- De la collecte en temps réel des données de trafic.

1° Pour les besoins des enquêtes portant sur des infractions graves, les autorités judiciaires peuvent, par ordonnance motivée du juge d'instruction ou, en l'absence d'information judiciaire ouverte, sur autorisation du Procureur de la République, autoriser :

- a) La collecte ou l'enregistrement, par l'application de moyens techniques, des données de trafic associées à des communications spécifiées transmises au moyen d'un système d'information ;
- b) L'obligation faite à un fournisseur de services, dans le cadre de ses capacités techniques, de prêter son concours pour cette collecte.

2° Le fournisseur de services est tenu au secret sur l'existence et l'exécution de cette mesure.

Article 70.- De l'interception des données de contenu.

1° Pour les besoins des enquêtes portant sur des infractions graves listées par décret, le juge d'instruction peut, par ordonnance motivée, autoriser la collecte ou l'enregistrement en temps réel des données de contenu de communications spécifiées, dans les conditions prévues à l'article 69.

2° La durée de la mesure d'interception ne peut excéder quatre mois, renouvelable dans les mêmes formes et conditions.

3° Le fournisseur de services est tenu au secret sur l'existence et l'exécution de cette mesure.

CHAPITRE IX — DE L'UNITE DE PROTECTION ET D'INVESTIGATION NUMERIQUE (UPIN)

Article 71.- Il est créé une Unité de Protection et d'Investigation Numérique, en abrégé UPIN, dotée de la personnalité morale et de l'autonomie financière. L'UPIN est un établissement public chargé de la prévention, de la détection, de l'investigation technique, de la coordination opérationnelle et de l'appui aux autorités judiciaires en matière de cybercriminalité.

Elle constitue également le point focal national pour la coopération internationale en matière de cybercriminalité, conformément aux engagements internationaux de la République de Madagascar. Elle assure, à ce titre, un service de point de contact joignable 24 heures sur 24, 7 jours sur 7 (réseau 24/7).

Article 72.- L'UPIN exerce notamment les missions suivantes :

- assurer la veille numérique et la détection des menaces cyber ;
- effectuer les investigations techniques nécessaires aux procédures judiciaires ;
- assister les officiers de police judiciaire et les magistrats dans la collecte, la conservation et l'exploitation des preuves numériques ;
- centraliser les signalements relatifs aux infractions prévues par la présente loi ;
- assurer la coopération technique avec les autorités nationales et étrangères compétentes ;
- contribuer au renforcement des capacités nationales en matière d'investigation numérique, notamment par la formation et la sensibilisation ;
- assurer la promotion des mesures préventives en coopération avec la société civile, les établissements scolaires et universitaires et le secteur privé ;
- procéder à la collecte et à l'analyse d'informations accessibles publiquement (OSINT), aux fins de détection des menaces cybernétiques, des réseaux coordonnés de faux comptes et des campagnes de manipulation numérique.

Article 73.- Dans l'exercice de ses missions, l'UPIN peut, sous le contrôle de l'autorité judiciaire compétente et dans les conditions prévues par la loi :

- procéder aux constatations techniques nécessaires ;
- effectuer les analyses numériques des supports saisis ;
- solliciter des opérateurs de communications électroniques et des fournisseurs de services numériques la communication des données dont la conservation est prévue par les textes en vigueur ;
- procéder, dans le respect des règles de procédure pénale et sous le contrôle du Procureur de la République ou du juge d'instruction lorsque ces opérations s'inscrivent dans une enquête, à la collecte et à l'analyse d'informations accessibles publiquement ;
- ordonner en urgence, dans les conditions prévues à l'article 53, le retrait ou le blocage provisoire d'un contenu manifestement illicite ;
- participer à l'exécution des commissions rogatoires, réquisitions judiciaires et demandes d'entraide internationale relatives aux preuves électroniques.

Seuls les agents de l'UPIN spécialement désignés à cet effet, assermentés et habilités dans les conditions fixées par décret, ont la qualité d'officier de police judiciaire pour l'exercice des pouvoirs mentionnés au présent article.

Article 74.- L'action de l'UPIN s'articule avec celle de la Police nationale, de la Gendarmerie nationale, du Bureau Indépendant Anti-Corruption (BIANCO), du Service de Renseignements Financiers (SAMIFIN), de l'Autorité de Régulation des Technologies de Communication (ARTEC), de la Commission Malgache de l'Informatique et des Libertés (CMIL) et du Centre de Veille, de Détection et de Réponse aux Incidents Informatiques (CIRT.mg) au sein d'un comité de coordination interinstitutionnel unique, dont la composition, les modalités de saisine et de fonctionnement sont fixées par décret.

Article 75.- Interconnexion légale et accès direct aux données.

L'UPIN dispose d'un accès technique direct et permanent, disponible en continu (24 heures sur 24, 7 jours sur 7), aux systèmes d'information des opérateurs de communications électroniques, des fournisseurs d'accès à Internet, des centres d'immatriculation et de tout autre organisme détenant des données nécessaires aux investigations relevant de sa compétence, selon des modalités techniques et de sécurité fixées par décret.

Cet accès porte sur les données d'identification, d'abonnement, de trafic et, le cas échéant, de contenu, dans les conditions et limites prévues par la présente loi.

Chaque consultation est enregistrée dans un journal sécurisé et inaltérable, précisant l'identité de l'agent, l'heure, la donnée consultée et le dossier concerné. Ce journal est tenu à la disposition du Procureur de la République et du juge d'instruction.

Toute consultation de données de trafic ou de contenu est notifiée, dans un délai de vingt-quatre (24) heures, au Procureur de la République ou au juge d'instruction compétent, qui peut en ordonner l'interruption ou la destruction si les conditions légales n'étaient pas réunies.

Les opérateurs, fournisseurs et organismes mentionnés au premier alinéa sont tenus de garantir la disponibilité technique permanente de cet accès, sous peine des sanctions prévues à l'article 51 de la présente loi.

Tout usage de cet accès à des fins étrangères aux missions de l'UPIN est puni des peines prévues par le Code pénal en matière d'abus de fonction, sans préjudice de sanctions disciplinaires.

Article 76.- Les modalités d'organisation, de fonctionnement, de recrutement des personnels ainsi que les règles de gouvernance de l'UPIN sont fixées par décret pris en Conseil des Ministres.

Article 77.- Les dispositions de la présente partie s'appliquent sans préjudice des compétences reconnues aux officiers de police judiciaire, aux autorités judiciaires, aux organismes chargés du renseignement ainsi qu'aux autres autorités administratives compétentes en vertu des lois et règlements en vigueur.

CHAPITRE X — DE LA COOPERATION INTERNATIONALE EN MATIERE DE CYBERCRIMINALITE

Article 78.- Les autorités compétentes de la République de Madagascar coopèrent avec les autorités compétentes des États étrangers, les organisations internationales et les mécanismes internationaux compétents dans la prévention, la recherche, la constatation, l'enquête, la poursuite et la répression des infractions prévues par la présente loi, conformément aux conventions internationales ratifiées par Madagascar, au principe de réciprocité, aux accords de coopération judiciaire ainsi qu'aux dispositions du Code de procédure pénale.

Cette coopération s'exerce dans le respect de la souveraineté nationale, des droits fondamentaux, des libertés individuelles et des garanties procédurales reconnues par le droit interne.

Article 79.- Les autorités compétentes peuvent, lorsqu'elles estiment que la communication d'informations est susceptible de prévenir une infraction, de faciliter une enquête ou de protéger des personnes ou des infrastructures critiques, transmettre spontanément à une autorité étrangère compétente des renseignements ou des preuves numériques, sans demande préalable, sous réserve des engagements internationaux de Madagascar et de la protection des données à caractère personnel.

Article 80.- Les demandes de coopération internationale, d'entraide judiciaire, de préservation de données, de transmission de preuves numériques ou de toute autre information peuvent être échangées par voie électronique sécurisée. Les moyens utilisés doivent garantir l'authenticité des communications, l'intégrité des documents transmis, leur confidentialité, leur traçabilité, ainsi que la vérification de l'identité des autorités requérantes et requises.

Article 81.- Les auditions de témoins, victimes, experts, personnes mises en cause ou toute autre mesure d'enquête ou d'instruction peuvent être réalisées par visioconférence ou par tout autre moyen technologique sécurisé permettant l'identification certaine des participants, le respect des droits de la défense ainsi que la confidentialité des échanges. Les procès-verbaux établis à cette occasion ont la même valeur probante que ceux dressés en présence physique, sous réserve des dispositions du Code de procédure pénale.

Article 82.- Lorsqu'une enquête concerne des données informatiques stockées, traitées ou réparties sur plusieurs territoires, les autorités compétentes peuvent solliciter la coopération des autorités étrangères compétentes afin d'assurer la conservation, la collecte, la transmission ou la saisie de ces données conformément aux conventions internationales applicables.

Article 83.- L'UPIN assure, en coordination avec le Ministère en charge de la Justice et les autres autorités compétentes, le fonctionnement permanent du point de contact national (réseau 24/7) destiné à faciliter les demandes urgentes relatives à la conservation, à la collecte et à la transmission des preuves électroniques dans le cadre de la coopération internationale.

Article 84.- En cas d'urgence, lorsque des données informatiques risquent d'être supprimées, altérées, chiffrées ou rendues inaccessibles, les autorités compétentes peuvent solliciter ou accorder une assistance immédiate auprès des autorités étrangères compétentes afin d'assurer leur préservation dans les meilleurs délais. Cette assistance est ensuite régularisée selon les procédures d'entraide judiciaire prévues par les conventions internationales ou les lois en vigueur.

Article 85.- Les autorités judiciaires peuvent constituer, conformément aux conventions internationales applicables, des équipes communes d'enquête avec les autorités compétentes d'États partenaires lorsque les infractions présentent un caractère transnational ou nécessitent une coopération opérationnelle renforcée.

Article 86.- De la restitution et du partage des biens confisqués.

1° Lorsque l'État malgache confisque des biens à la demande d'un autre État, il peut, si la demande lui en est faite, restituer ces biens à l'État requérant afin d'indemniser les victimes ou de les restituer à leurs propriétaires légitimes.

2° Il peut également, après avoir dûment pris en considération l'indemnisation des victimes, conclure des accords pour partager le produit de la confiscation avec d'autres États parties ayant contribué à l'enquête.

Article 87.- De la protection des données personnelles dans le cadre de la coopération.

1° Le transfert de données personnelles à un État étranger en application de la présente loi est effectué conformément à la législation malgache sur la protection des données à caractère personnel et aux obligations internationales applicables.

2° Lorsque le transfert de données personnelles est susceptible de ne pas respecter les garanties de protection, l'autorité malgache peut exiger des conditions spécifiques pour assurer la conformité.

3° Le transfert de données personnelles à un pays tiers ne peut se faire sans l'autorisation préalable de l'État qui a procédé au transfert initial.

CHAPITRE XI — DE LA PROTECTION DES VICTIMES ET DES TEMOINS

Article 88.- Les victimes des infractions prévues par la présente loi bénéficient, au cours de la procédure pénale, des mesures de protection prévues par les lois en vigueur.

Lorsque la victime est mineure ou particulièrement vulnérable, les autorités judiciaires prennent toute mesure propre à préserver sa dignité, son intégrité physique et psychologique ainsi que la confidentialité de son identité.

Des procédures adaptées sont mises en place pour assurer leur rétablissement physique et psychologique et leur permettre d'obtenir réparation, conformément aux engagements internationaux de Madagascar.

Article 89.- Toute personne ayant collaboré de bonne foi avec les autorités compétentes dans la recherche des infractions prévues par la présente loi peut bénéficier des mesures de protection prévues par la législation en vigueur lorsque sa sécurité ou celle de ses proches est menacée.

Des mesures appropriées sont prises pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux personnes qui déposent ou qui, de bonne foi et pour des motifs raisonnables, fournissent des informations concernant des infractions prévues par la présente loi ou coopèrent d'une autre manière avec les services d'enquête ou les autorités judiciaires, et, le cas échéant, à leurs parents et à d'autres personnes qui leur sont proches.

Ces mesures peuvent consister notamment :

- à établir, pour la protection physique de ces personnes, des procédures visant à leur fournir un nouveau domicile et à permettre que les renseignements concernant leur identité et le lieu où elles se trouvent ne soient pas divulgués ;
- à prévoir des règles de preuve qui permettent aux témoins de déposer d'une manière qui garantit leur sécurité, notamment en recourant à des techniques de communication telles que les liaisons vidéo.

CHAPITRE XII — DISPOSITIONS TRANSITOIRES ET FINALES

Article 90.- Les dispositions de la présente loi sont applicables sans préjudice :

- du Code pénal ;
- du Code de procédure pénale ;
- de la législation relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- de la législation relative à la protection des données à caractère personnel ;
- ainsi que des conventions internationales ratifiées par la République de Madagascar.

Sans préjudice des dispositions particulières prévues par la présente loi, quiconque, ayant été condamné pour une infraction prévue par la présente loi à une peine d'emprisonnement, sera reconnu coupable de la même infraction, ou d'une infraction de même nature, commise dans le délai de cinq ans à compter du jour où la condamnation est devenue définitive, sera condamné au double du maximum de la peine encourue.

Article 91.- Les procédures engagées avant l'entrée en vigueur de la présente loi demeurent régies par les dispositions législatives applicables à la date des faits, sauf lorsque les dispositions nouvelles sont plus douces au sens du principe de l'application de la loi pénale plus favorable.

Article 92.- Des textes réglementaires adoptés en Conseil des Ministres seront pris en tant que de besoin pour l'application de la présente loi, notamment en ce qui concerne :

- l'organisation et le fonctionnement de l'UPIN ;
- les modalités de coopération avec les opérateurs de communications électroniques et les fournisseurs de services numériques ;
- les procédures de conservation, de collecte et de transmission des preuves électroniques ;
- les conditions techniques de sécurisation des investigations numériques ;
- la liste des infractions ouvrant droit à la collecte en temps réel (articles 69 et 70).

Article 93.- Toutes dispositions antérieures contraires à celles de la présente loi sont et demeurent abrogées, notamment la loi n°2014-006 du 17 juillet 2014 modifiée et complétée par la loi n°2016-031 du 23 août 2016 sur la lutte contre la cybercriminalité.

Article 94.- Les dispositions de l'article 355.12, alinéa premier, du Code de procédure pénale sont modifiées comme suit :

« Art. 355.12, alinéa premier (nouveau).- Nonobstant les dispositions de la loi sur la lutte contre la cybercriminalité, en matière criminelle et en matière correctionnelle, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. (Le reste sans changement). »

Article 95.- Le décret portant création, organisation et fonctionnement de l'Unité de Protection et d'Investigation Numérique (UPIN), pris en application de l'article 76 de la présente loi, est adopté concomitamment à l'entrée en vigueur de la présente loi et mis en conformité avec les missions et pouvoirs de l'UPIN tels que définis au Chapitre IX ci-dessus.

Article 96.- La présente loi sera publiée au *Journal officiel* de la République de Madagascar et exécutée comme loi de l'État.

Promulguée à Antananarivo, le _____ 2026

Le Président de la Refondation de la République

Michaël RANDRIANIRINA