REPUBLIQUE DU TCHAD
PRESIDENCE DE LA REPUBLIQUE

UNITE - TRAVAIL – PROGRES

جمهورية تشاد
رئاسة الجمهورية

وحدة – عمل – تقدم

LOI N°009/ PR/2015
PORTANT SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE.

قانون رقم _____/ رئاسة الجمهورية/ 2015
القاضي بالأمن الإلكتروني ومكافحة الجرائم الالكترونية

Vu la Constitution ;

L'Assemblée Nationale a délibéré et adopté en sa séance du 15 Décembre 2014,

Le Président de la République promulgue la Loi dont la teneur suit :

بناءا على الدستور؛
تداولت الجمعية الوطنية واعتمدت في جلستها المنعقدة في15 ديسمبر 2014
ويصدر رئيس الجمهورية القانون الآتي نصه

TITRE I : DES DISPOSITIONS GENERALES

الباب الأول: أحكام عامة

CHAPITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION

الفصل الأول: عن الهدف ونطاق التطبيق

Article 1er : La présente loi a pour objet de fixer le cadre juridique de la lutte contre la cybercriminalité dans le respect des droits et des libertés des individus. En particulier, elle vise à régir le cadre de sécurité des services d'information électroniques, des services et réseaux de communications électroniques, de même qu'elle définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication en République du Tchad.

المادة 1: يهدف هذا القانون إلى وضع إطار قانوني لمكافحة جرائم الإنترنت في ظل احترام حقوق وحريات الأفراد. وعلى وجه الخصوص، فإنه يهدف إلى ضبط الإطار الأمني لخدمات المعلومات الإلكترونية، وأقسام وشبكات الاتصالات الإلكترونية، كما إنه يحدد ويعاقب الجرائم المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات في تشاد.

Article 2 : Sont exclues du champ d'application de la présente loi, les applications spécifiques en matière de défense et de sécurité nationales.

المادة 2: يستثنى من نطاق تطبيق القانون الحالي، التطبيقات الخاصة بمجال الدفاع والأمن القومي.

Article 3 : Les réseaux de communications électroniques visés par la présente loi comprennent : les réseaux satellitaires, les réseaux terrestres, les réseaux électriques lorsqu'ils servent à l'acheminement des communications électroniques, les réseaux assurant la diffusion ou distribution de services de communication audiovisuelle.

المادة 3: شبكات الاتصالات الإلكترونية التي يشملها هذا القانون الحالي هي الآتية:
شبكات الأقمار الصناعية والشبكات الأرضية، وشبكات الطاقة المستخدمة في توصيل اتصالات إلكترونية وشبكات النشر أو توزيع خدمات الاتصالات السمعية والبصرية.

CHAPITREI II : DES DEFINITIONS

Article 4 : Au sens de la présente loi et de ses textes d'application, les termes et expressions suivants, s'entendent comme il est précisé ci-après :

ANSICE : Agence Nationale de Sécurité Informatique et de Certification Electronique. Autorité nationale administrative indépendante chargée de veiller au respect, sur le territoire national, des dispositions de la présente loi.

Chiffrement : procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations inintelligibles par des tiers n'ayant pas la connaissance de la clé.

Clé : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase, qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.

Communication électronique : toute transmission au public ou à une catégorie du public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de message de toute nature.

Confidentialité : état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication électroniques, systèmes d'information ou des équipements terminaux, afin de prévenir la divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert.

Cryptographie : ensemble des techniques qui, au moyen d'un code secret appelé clé, visent à rendre un message indéchiffrable pour toute autre personne que son émetteur ou son destinataire.

Cryptologie : science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation.

Cybercriminalité : ensemble des activités criminelles pénalement répréhensibles qui se commettent au moyen ou sur un réseau de communications électroniques ou sur

الفصل الثاني: التعريفات

المادة 4: لأغراض هذا القانون ونصوصه التطبيقية، يفهم معني الكلمات والعبارات المستخدمة كما تم توضيحها فيما يلي:

ANSICE: الوكالة الوطنية للأمن المعلوماتي والاعتماد الإلكتروني. إنها سلطة إدارية وطنية مستقلة مكلفة بضمان الامتثال لأحكام هذا القانون الحالي في الأراضي الوطنية.

التشفير: عملية يتم بموجبها استخدام مفتاح سري يسمى الاتفاقية السرية، معلومات واضحة إلى معلومات مشفرة غير مفهومة لدى الاطراف الثالثة التي ليس لها إلمام بالمفتاح.

مفتاح: في نظام التشفير، فإنه يعادل قيمة رياضية، كلمة، جملة، والتي، بحكم خوارزمية التشفير تستخدم لفك رسالة.

اتصال إلكتروني: أي نقل إلى الجمهور أو إلى فئة من الجمهور، بوسيلة إلكترونية أو مغناطيسية، إشارات، أو رموز، أو كتابة أو صور أو أصوات أو رسالة من أي نوع كان.

سرية: وضع أمني لضمان سرية المعلومات والموارد المخزنة في شبكات أنظمة الاتصالات الإلكترونية، ونظم الإعلام أو الأجهزة الطرفية لمنع الكشف غير المصرح به من المعلومات إلى أطراف ثالثة، من خلال القراءة ، الاستماع، والنسخ غير القانوني عن قصد أو من غير مقصد أثناء التخزين والمعالجة أو النقل.

كتابة التشفير: مجموعة من التقنيات التي تستخدم كلمات سرية تسمى مفتاح، وتهدف إلى تحويل رسالة إلى رموز غير مفهومة لأي شخص آخر غير المصدر أو المتلقي.

علم التشفير: علوم يتعلق بحماية وأمن المعلومات في إطار السرية، والتوثيق، والنزاهة وعدم التخلي عن الواجب.

un système d'information par d'autres moyens que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique.

Cyberespace : ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

Cybersécurité : désigne un ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurisation des réseaux de communications électroniques, des systèmes d'information et pour la protection de la vie privée des personnes.

Déchiffrement : Opération faisant écho au chiffrement, ayant pour but l'obtention de la version originale d'un message précédemment chiffré.

Disponibilité : désigne l'état de sécurité permettant de garantir que les informations et ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins.

Données : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction.

Données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

Données relatives au trafic : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Fournisseur de services : toute personne physique ou morale fournissant pour son propre compte ou pour le compte d'autrui des services de communications

جرائم إلكترونية: جميع الأنشطة الإجرامية التي تعاقب كجرائم جنائية والتي ترتكب عبر شبكة الاتصالات الإلكترونية أو عبر نظام المعلومات من خلال وسائل أخرى غير تلك التي تسخر عادة كمكمل في تنفذ الجرائم التقليدية.

الفضاء الإلكتروني: مجموعة من البيانات الرقمية التي تشكل كيانا للمعلومات ومجالا للاتصال المرتبط بشبكة عالمية من أجهزة الكمبيوتر.

الأمن الإلكتروني: يعني مجموعة من الإجراءات الوقائية والحماية والردع التقني والتنظيمي والقانوني والمالي والبشري والإجرائي وغيرها من الإجراءات التي تمكن من تحقيق أهداف أمن شبكات الاتصالات الإلكترونية، وأنظمة المعلومات من أجل حماية حياة الأفراد الشخصية.

فك التشفير: عملية تعود إلى التشفير، تهدف إلى الحصول على النسخة الأصلية من رسالة مشفرة سابقا.

توفر: يعني الوضع الأمني الذي يجعل المعلومات وموارد شبكات الاتصالات الإلكترونية، ونظم المعلومات أو المعدات الطرفية، متاحة ويمكن استخدامها حسب الحاجة.

بيانات: هي حقائق أو معلومات أو مفاهيم في شكل قابل للمعالجة من قبل الأجهزة الطرفية، بما في ذلك برنامج يساعد هذا الأخير على أداء وظيفة.

بيانات معلوماتية: يعني أي حدث أو معلومات بيانات الكمبيوتر أو مفاهيم في شكل قابل للمعالجة بالكمبيوتر، بما في ذلك برنامج من شأنه أن يعالج وظيفة في نظام الكمبيوتر.

بيانات متعلقة بالحركة: أي بيانات ذات صبغة اتصال يمر بنظام معلوماتي تم إنتاجها من هذه الأخير كعنصر من سلسلة اتصالات مع بيان المصدر والهدف والطريق والزمن التاريخ وحجم ومدة الاتصال أو نوع الخدمة الكامنة من وراء ها.

électroniques ou de services d'information électroniques, y compris la fourniture de l'accès à l'utilisation de ces services.

Intégrité : désigne l'état de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal demeuré intact et que les ressources et informations qui y stockées n'ont pas été altérées, modifiées ou détruites, d'une façon intentionnelle ou accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité.

Matériel raciste et xénophobe : tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes.

Mineur : toute personne âgée de moins de dix-huit (18) ans au sens de la loi nationale.

Prestataire de service de sécurité : toute personne physique ou morale qui exerce des activités liées à la sécurité électronique notamment, la délivrance et la gestion des certificats électroniques ou la fourniture d'autres services liés aux signatures électroniques, la création des logiciels de sécurité, la surveillance des réseaux, la détection d'intrusions, l'audit des réseaux et systèmes de sécurité.

Preuve numérique : toute information probante stockée ou transmise sous forme numérique.

Pornographie enfantine : toute donnée quels qu'en soient la nature, la forme ou le support représentant :

- un mineur se livrant à un comportement sexuellement explicite ;
- une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;
- des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

Réseau de communications électroniques : systèmes de transmission, actif ou passif et, le cas échéant, les équipements de commutation et de routage et les autres

مزود خدمات: أي شخصية طبيعية أو اعتبارية توفر لحسابها الخاص أو لحساب الغير خدمات اتصالات إلكترونية أو خدمات معلومات إلكترونية، بما في ذلك توفير معدات الولوج إلى استخدام هذه الخدمات.

سلامة: تعني الوضع الأمني الذي يوفر لشبكة الاتصالات الإلكترونية نظام المعلومات أو المعدات الطرفية سلامتها بحيث أن تبقى الموارد والمعلومات المخزنة كماهي دون تلف أو تغيير أو تدمير مقصود أو غير مقصود وذلك لضمان دقتها، ومصداقيتها واستدامتها.

مواد عنصرية ومعادية للأجانب: تعني أي مادة مكتوبة، أي صورة أو أي تمثيل آخر من الأفكار أو النظريات التي تدعو وتشجع أو تحرض على الكراهية أو التمييز أو العنف ضد شخص أو مجموعة من الأشخاص بسبب العرق، اللون أو النسب أو الأصل القومي أو العرقي أو الدين، لدرجة أن تكون هذه الأخيرة ذريعة لأي من هذه العناصر، أو تشجع على مثل هذه الأعمال.

قاصر: أي شخص دون سن الثامنة عشرة (18) طبقا للقانون الوطني.

مزود خدمة السلامة: أي شخصية طبيعية أو اعتبارية تباشر الأنشطة المتعلقة بالأمن الإلكتروني وعلى وجه الخصوص إصدار وإدارة الشهادات الإلكترونية أو تقديم خدمات أخرى ذات صلة بتوقيع الشهادات الإلكترونية، إنشاء البرامج الأمنية، مراقبة الشبكات وكشف التسلل، ومراجعة الشبكات وأنظمة الأمن.

الأدلة الرقمية: أي معلومات ثبوتية مخزنة أو المنقولة رقميا.

المواد الإباحية عن الأطفال: أي بيانات مهما كان طبعها أو شكلها أو ما يرمز لها:

- قاصر يقوم بسلوك جنسي صريح.
- شخص يبدو كقاصر يقوم بتصرفات سلوك جنسي صريح.
- صور واقعية تمثل قاصرا في ممارسة جنسية صريحة.

ressources qui permettent l'acheminement des signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobile, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission des signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.

Sécurité : situation dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable ou à en limiter les effets.

Service de communications électroniques : prestation consistant entièrement ou principalement en la fourniture de communications électroniques à l'exclusion des contenus des services de communication audiovisuelle.

Système informatique : désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assurent ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

Système d'information : désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données.

Technologies de l'information et de la communication (TIC) : désigne les technologies employées pour recueillir, stocker, utiliser et envoyer des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

Article 5 : Pour les termes et expressions qui ne sont pas définis dans la présente loi, il convient en tant que de besoin, de se référer

aux définitions données par les conventions, décisions et documents de l'Union Internationale des Télécommunications (UIT) ou à ceux de l'Union Africaine

شبكة الاتصالات الالكترونية: أنظمة ارسال، نشطة أو مستقبلة، وعند الاقتضاء، معدات الوصل والتمرير والموارد الأخرى لنقل الإشارات بواسطة الأسلاك، أوعن الطريقة الهرتزية، أو الضوئية أو عبر طرائق أخرى ألكترو مغناطيسية التي تشمل شبكات الأقمار الصناعية والشبكات الأرضية الثابتة (مع إتصال دوائر الأحزمة، بما في ذلك الإنترنت) والأنظمة المتنقلة والأنظمة التي تستخدم الشبكة الكهربائية، لنقل الإشارات، والشبكات المستخدمة في البث الإذاعي والتلفزيوني، وشبكات التلفزيون وأي نوع كان من المعلومات المرسلة.

أمن: وضعية شخص ما أو شيئا ما بحيث لا يتعرض لأي خطر. آلية من أجل الوقاية من وقوع ضرر أو الحد من آثاره.

خدمة الاتصالات الإلكترونية: خدمة قائمة كليا أو أساسا في توفير الاتصالات الإلكترونية باستثناء محتوى الاتصال السمعي البصري.

نظام معلوماتي: يعني أي نظام معزول أو مجموعة من الأجهزة المرتبطة بعضها البعض أو المتماثلة، حيث تقوم بمجملها أو يقوم عدة من عناصرها بمعالجة البيانات آليا.

نظام المعلومات: يعني أي نظام معلومات معزول أو مجموعة من الأجهزة المرتبطة بعضها البعض، يقوم بنفسه أو بواسطة أحد أو أكثر من عناصره، بمعالجة البيانات آليا.

تكنولوجيا المعلومات والاتصالات: يعني التكنولوجيا المستخدمة لجمع وتخزين واستخدام وإرسال المعلومات، إضافة إلى تلك التي تتطلب استخدام أجهزة الكمبيوتر أو أي نظام اتصالات بما في ذلك الاتصال عن بعد.

المادة 5: بالنسبة للكلمات والعبارات التي لم يتم تعريفها في هذا القانون، فيستحسن، كلما دعت إليه الحاجة، أن يتم اللجوء

(UA), de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC), ou à ceux de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC).

TITRE II : DE LA POLITIQUE GENERALE EN MATIERE DE CYBERSECURITE

CHAPITRE I : DE LA MISSION DE L'ETAT

Article 6 : En collaboration avec les parties prenantes comprenant, l'industrie et les organisations professionnelles, la société civile et les citoyens, l'Etat, à travers le Ministère en charge des communications électroniques, élabore et met en œuvre une politique nationale de cybersécurité en tenant compte de l'évolution technologique et des priorités du Gouvernement dans ce domaine.

A ce titre, l'Etat :

a) assure la promotion de la sécurité des réseaux de communications électroniques et des systèmes d'information ainsi que le suivi de l'évolution des questions liées aux activités de sécurité informatique ;
b) coordonne sur le plan national les activités concourant à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information ;
c) veille à la mise en place d'un cadre légal et règlementaire adéquat pour la sécurité des communications électroniques ;
d) assure la représentation de l'Etat aux instances internationales chargées des activités liées à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information.

Article 7 : La politique nationale de cybersécurité devra intégrer dans ses grandes lignes, la protection de l'information dans les réseaux, la sécurité des transactions électroniques, la protection de la vie privée et des mineurs dans le cyberespace, ainsi que la lutte contre la fracture numérique.

CHAPITRE II : DE LA REGULATION ET DU SUIVI DES ACTIVITES DE SECURITE ELECTRONIQUE

إلى التعاريف التي وردت في اتفاقيات وقرارات ووثائق الاتحاد الدولي للاتصالات أو تلك التابعة للاتحاد الأفريقي، أو المجموعة الاقتصادية لدول وسط أفريقيا أو المجموعة الاقتصادية والنقدية لوسط أفريقيا (سيماك).

الباب الثاني عن السياسة العامة في مجال الأمن الإلكتروني

الفصل الأول: عن مهمة الدولة

المادة 6: بالتعاون مع الشركاء والمصانع والمنظمات المهنية والمجتمع المدني والمواطنين، تقوم الدولة، عبر الوزارة المكلفة بالاتصالات الإلكترونية، بسن وترسيخ سياسة وطنية للأمن الإلكتروني مع الأخذ في الاعتبار التطورات التكنولوجية وأولويات الحكومة في هذا المجال.

ولذا تقوم الدولة بـ:

أ) ضمان تطوير أمن شبكات الاتصالات الإلكترونية ونظم المعلومات وكذلك متابعة تطور القضايا المرتبطة بأنشطة أمن المعلومات؛

ب) بتنسيق، على المستوى الوطني، الأنشطة المساهمة في أمن وحماية شبكات الاتصالات الإلكترونية ونظم المعلومات.

ج) بالسهر على إنشاء إطار قانوني و تنظيمي مناسب لتأمين الاتصالات الإلكترونية؛

د) بتمثيل الدولة لدى الهيئات الدولية المسؤولة عن الأنشطة المتعلقة بأمن وحماية شبكات الاتصالات الإلكترونية ونظم المعلومات.

المادة 7: يجب أن تدمج السياسة الوطنية في مجال الأمن الألكتروني، حماية المعلومات في الشبكات، وسلامة المعاملات الإلكترونية، وحماية الحياة الشخصية والقصر في الفضاء الإلكتروني ومكافحة الفجوة الرقمية.

Article 8: La régulation des activités de sécurité électronique, la coordination des activités de lutte contre la cybercriminalité sur l'ensemble du territoire national et le suivi de la mise en œuvre des dispositions de la présente loi sont assurées par l'Agence Nationale de Sécurité Informatique et de Certification Electronique (ANSICE), créée par la loi s'y rapportant.

TITRE III : DE LA CYBERCRIMINALITE

CHAPITRE I : DES DISPOSITIONS PROCEDURALES

Article 9: En cas d'infraction relevant de la cybercriminalité, les officiers de police judiciaire et les agents habilités de l'ANSICE procèdent aux enquêtes conformément aux dispositions du Code de Procédure Pénale en vigueur.

Article 10: Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données sur le territoire national, sont utiles à la manifestation de la vérité, les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent perquisitionner, accéder ou ordonner de perquisitionner ou d'accéder au système informatique ou à une partie de celui-ci ou au support de stockage.

Article 11: Lorsque les officiers de police judiciaire et les agents habilités de l'ANSICE perquisitionnent, accèdent ou ordonnent la perquisition ou l'accès d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément à l'article précédent et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur le territoire national, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, ceux-ci peuvent étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

Article 12: Lorsque les officiers de police judiciaire et les agents habilités de l'ANSICE découvrent dans un système informatique des données qui sont utiles à la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ils peuvent saisir, ordonner la saisie ou

الفصل الثاني: تنظيم ومتابعة أنشطة الأمن الإلكتروني

المادة 8 يتم تنظيم أنشطة الأمن الإلكتروني، تنسيق أنشطة مكافحة الجرائم الإلكترونية في جميع أنحاء الأراضي الوطنية ومتابعة وترسيخ أحكام هذا القانون، من قبل الوكالة الوطنية للأمن المعلوماتي والاعتماد الإلكتروني (ANSICE)، التي يتم أنشاؤها طبقا للقانون المتعلق بها.

الباب الثالث: الجرائم الإلكترونية

الفصل الأول: أحكام إجرائية

المادة 9: في حالة وقوع جريمة إلكترونية، يقوم ضباط الشرطة القضائية وعملاء الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني(ANSICE) بالتحقيقات وفقا لأحكام قانون الإجراءات الجنائية المعمول به.

المادة 10: عندما تكون بيانات مخزنة في نظام الكمبيوتر أو في حامل للحفاظ على بيانات داخل الأراضي الوطنية، ويبدوا أنها صالحة للكشف عن حقيقة، بإمكان ضباط الشرطة القضائية وعملاء الوكالة الوطنية للأمن المعلوماتي والاعتماد الإلكتروني (ANSICE) أن يقوموا بالتفتيش، أو إصدار إذن بدخول النظام المعلوماتي أو جزء منه أو الوصول إلى نظام التخزين.

المادة 11: عندما يقوم ضباط الشرطة القضائية وعملاء الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني (ANSICE) بعمليات تفتيش، أو أمر بتفتيش أو ولوج نظام مماثل لنظام كمبيوتر معين أو جزء منه، وفقا للمادة السابقة و لديهم الأدلة بأن البيانات المطلوبة مخزنة في نظام كمبيوتر آخر أو جزء منه داخل الأراضي الوطنية، وأن هذه البيانات يمكن الوصول إليها بشكل قانوني عن طريق النظام الأولي أو متاحة على النظام الأولي، بإمكانهم توسيع البحث أو الوصول إليها عن طريق النظام المماثل الآخر.

obtenir d'une façon similaire des données informatiques pour lesquelles l'accès a été réalisé en application de l'article précédent. Cette mesure inclut les prérogatives suivantes :

a) saisie ou obtention d'une façon similaire d'un système informatique ou d'une partie de celui-ci, ou un support de stockage informatique ;

b) réalisation et conservation d'une copie de ces données ;

c) préservation de l'intégrité des données informatiques stockées jugées pertinentes ;

d) action en vue de rendre inaccessibles ou en vue d'enlever ces données informatiques du système informatique consulté.

Article 13 : Les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures prévues par le présent article et par l'article précédent.

Article 14 : En cas de condamnation, le tribunal peut prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou données ainsi que des sommes ou produits résultant de l'infraction et appartenant au condamné.

Article 15 : L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier pour établir les infractions à la loi pénale sous réserves des conditions suivantes :

a) d'une part, qu'elle soit apportée au cours des débats contradictoires et discutée devant le juge ;
b) d'autre part, que puisse être dûment identifiée la personne dont elle émane et qu'elle soit établie et conservée dans des conditions de nature à garantir son intégrité.

Article 16 : Les officiers de police judiciaire et les agents habilités de l'ANSICE ont accès, lors des investigations, aux

المادة 12: عندما يكتشف ضباط الشرطة القضائية وعملاء الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني (ANSICE)، في نظام معلوماتي بيانات يمكن تصلح لاكتشاف الحقيقة، ولكن يتعذر الإستيلاء على وسائط التسجيل، بإمكانهم مصادرتها أو الأمر بمصادرتها بنفس بطريقة الحصول على بيانات معلوماتية بتطبيق المادة السابقة. ويشمل هذا الإجراء الصلاحيات التالية:

أ) مصادرة أو الحصول على نظام معلوماتي بطريقة مماثلة أو جزء منه، أو وسائط تخزين البيانات؛

ب) الاحتفاظ بنسخة من هذه البيانات؛

ج) الإحتفاظ بكامل البيانات المعلوماتية المخزنة والتي تعتبر ذات أهمية.

د) العمل بهدف منع الوصول إليها أو إزالة تلك البيانات من النظام المعلوماتي الذي تم الوصول إليه.

المادة 13: بإمكان ضباط الشرطة القضائية المخولون وعملاء الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني (ANSICE) تفويض أي شخص ملم بتشغيل النظام المعلوماتي أو بالتدابير المطبقة لحماية البيانات المعلوماتية، ليقدم المعلومات اللازمة والمعقولة لتطبيق الإجراءات المنصوص عليها في هذه المادة.

المادة 14: في حالة الإدانة، يجوز للمحكمة أن تأمر بمصادرة المعدات والأدوات والبرامج المعلوماتية أو البيانات، فضلا عن المبالغ أو المنتجات الناجمة عن المخالفة والتي هي ملكية المدان؛

المادة 15: يتم قبول المكتوب الإلكتروني في مجال العقوبات الجزائية، كشكل من أشكال الأدلة، كالأدلة المكتوبة على الورق العادي لإثبات انتهاكات للقانون الجنائي وفقا للشروط التالية:

أ) من جهة، أن تقدم أثناء المرافعات أمام القاضي.

ب) ومن جهة أخرى، يجب أن تشخص شرعا الشخص الذي صدرت منه كما يجب إثباتها في ظل ظروف تضمن سلامتها.

moyens de transport, à tout local à usage professionnel, à l'exclusion des domiciles privés, en vue de rechercher, de constater les infractions, de demander la communication de tous les documents professionnels et d'en prendre copie, de recueillir, sur convocation ou sur place, les renseignements et justifications nécessaires à l'accomplissement de leur mission.

Article 17: Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur des données stockées sur des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

Lorsqu'une copie des données saisies a été faite, celle-ci peut être détruite sur instruction du Procureur de la République pour des raisons de sécurité.

Sur accord du Procureur de la République, seuls seront gardés sous scellé par l'Officier de Police Judiciaire, les objets, documents et données utilisées à la manifestation de la vérité.

Les personnes présentes lors de la perquisition peuvent être réquisitionnées pour fournir les renseignements sur les objets, documents et données saisis.

Article 18 : Les perquisitions et les saisies sont effectuées dans les conditions prévues par le Code de Procédure Pénale.

Article 19 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

Article 20 : La réquisition prévue à l'article 19 ci-dessus

المادة 16: ضباط الشرطة القضائية وعملاء وكالة (ANSICE) المخولون لهم أثناء التحقيقات، صلاحية دخول أي مقر ذات استخدام شخصي باستثناء المنزل الخاص بالفرد، بهدف البحث والعثور على الجرائم، والمطالبة بكل الوثائق الشخصية وأخذ نسخة منها، بدعوة أو في الحال للإطلاع على الوثائق والمبررات اللازمة لإنجاز مهمتهم.

المادة 17: إن التفتيش في مجال الجرائم الإلكترونية يمكن أن يتعلق ببيانات مخزنة على وسائط مادية أو نسخ تم أخذها بحضور أشخاص شهدوا التفتيش.

عندما يتم إنشاء نسخة من البيانات المصادرة، فإنه يمكن تدميرها بناء على تعليمات من المدعي العام لأسباب أمنية.

بناءا على موافقة المدعي العام، لا يبقى بحوزة ضابط الشرطة القضائية، سوى الوثائق والبيانات المستخدمة في إبراز الحقيقة.

يمكن استدعاء الحاضرين أثناء البحث لغرض توفير معلومات حول الأشياء أو الوثائق أو البيانات المضبوطة.

المادة 18: يتم إجراء التفتيش والضبط وفقا لقانون الإجراءات الجنائية.

المادة 19: عندما تبدو ت البيانات المحتجزة أو التي تم الحصول عليها أثناء التحقيق أو المحاكمة أصبحت محل عملية تغيير يحول دون معرفة الحقيقة أو من شأنها أن تؤدي إلى تزييف المعلومات التي تحتويها، بإمكان مدعيى الجمهورية وقاضي التحقيق أو المحكمة المختصة إستجواب أي شخصية طبيعية أو إعتبارية مؤهلة للقيام بالعمليات الفنية بهدف الحصول على نسخة واضحة من البيانات.

عندما تستخدم وسيلة تشفير، بإمكان السلطات القضائية أن تطلب الإتفاقية السرية لفك النص المشفر.

peut être faite à tout expert. Dans ce cas, son exécution est faite conformément aux dispositions du Code de Procédure Pénale relative à la commission d'expert.

Article 21 : Les autorités judiciaires tchadiennes peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne physique ou morale pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire de la République du Tchad ou dont l'un des auteurs ou complices se trouve dans ledit territoire.

Sous réserve des règles de réciprocité entre le Tchad et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de Procédure Pénale.

Article 22 : Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux officiers de police judiciaire ou aux agents habilités de l'ANSICE, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

Les Officiers de Police Judiciaire et les agents habilités de l'ANSICE peuvent demander aux fournisseurs des prestations visés à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Article 23 : Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne et/ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission. Il est dressé, dans chacun des lieux, un procès-verbal des opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel et/ou sonore.

Lorsque les circonstances l'exigent, l'interprétation peut être faite au cours d'une audition, d'un interrogatoire ou d'une

المادة 20: إن الاستدعاء القانوني الوارد في المادة 19 أعلاه، يمكن إجراؤه على أي خبير. في هذه الحالة، يتم تنفيذه وفقا لأحكام قانون الإجراءات الجنائية في لجنة الخبراء.

المادة 21: بإمكان السلطات القضائية التشادية أن تفوض لجنة إنابية وطنية أو دولية أو أي شخصية طبيعية أو اعتبارية للعثور على العناصر المكونة للجرائم الإلكترونية، والتي حيث وقع على الأقل أحد من عناصرها في أراضي جمهورية تشاد أو حيث يتواجد أحد المتواطئين بالجريمة في نفس البلد.
تحت طائلة قواعد المعاملة بالمثل بين تشاد و الدول الأجنبية المرتبطة بإتفاقية التعاون القضائي، فإن اللجان الإنابية تنفذ وفقا لأحكام قانون الإجراءات الجنائية.

المادة 22: إن الشخصيات الطبيعية أو الاعتبارية التي تقدم خدمات تشفير لضمان وظيفة الخصوصية، ملزمة بتسليم ضباط الشرطة القضائية و عملاء وكالة (ANSICE) المختصون، بناء على طلبهم، الاتفاقيات التي تسمح بفك تشفير البيانات المحولة عن طريق الخدمات التي يقدمونها.

بإمكان ضباط الشرطة القضائية وعملاء وكالة (ANSICE) المختصون، الطلب من موردي الخدمات المشار إليهم في الفقرة 1 أعلاه ترسيخ هذه الاتفاقيات، ما لم يثبت هؤلاء عدم قدرتهم على تلبية مثل هذه الطلبات.

المادة 23: عندما تقتضي ضرورة التحقيق، أو الاستجواب و/أو المواجهة بين عدة أشخاص، تجري في عدة نقاط من الأراضي الوطنية، يمكن أن تتم في عدة أماكن من الأراضي الوطنية مرتبطة عن طريق الاتصالات الإلكترونية لضمان سرية الإرسال. يتم تحرير محضر عن العمليات في كل من تلك المناطق، كما يمكن أن تكون هذه العمليات محل تسجيل سمعية بصرية و / أو سمعي.
متى ما دعت الضرورة، يمكن أن تتم القراءة أثناء جلسة قضائية أو استجواب أو مواجهة عن طريق الاتصالات الإلكترونية.

confrontation par des moyens de communications électroniques.

Les dispositions du présent article sont également applicables pour l'exécution simultanée, sur un point du territoire national et sur un point situé à l'extérieur, des demandes d'entraide émanant des autorités judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des autorités judiciaires tchadiennes.

Article 24 : Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatiques stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification, les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux (2) ans maximum, pour la bonne marche des investigations judiciaires.

Article 25 : La personne en charge de la garde des données est tenue de garder le secret sur la mise en œuvre desdites procédures.

Article 26 : Les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent ordonner :

a) à une personne présente sur le territoire national de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ;
b) à un fournisseur de services offrant des prestations sur le territoire national, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Article 27 : Pour la constatation des infractions définies par la présente loi, les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques sur le territoire national, transmises au moyen d'un système informatique. Ils

يمكن تطبيق أحكام هذه المادة في التنفيذ المتزامن في وقت واحد من نقطتين إحدى في الأراضي الوطنية ونقطة خارج الأراضي الوطنية، عند طلب المساعدة من قبل سلطات قضائية أجنبية أو المساعدة عند التبادل القضائي بناء على طلب من السلطات القضائية التشادية.

المادة 24: متى ما دعت ضرورة المعلومات المطلوبة، وخاصة عندما تكون هناك أسباب للاعتقاد بأن البيانات المعلوماتية المخزنة في نظام معلوماتي معرضة بشكل خاص للضياع أو للتعديل، بإمكان ضباط الشرطة القضائية المختصون وعملاء الوكالة الوطنية (ANSICE) أن تأمر أي شخص لصون وحماية سلامة البيانات التي بحوزته أو تحت سيطرته، لمدة سنتين على الأقل لحسن سير التحقيقات القضائية.

المادة 25: على الشخص المكلف بحفظ البيانات الإلتزام بسرية ترسيخ هذه الإجراءات.

المادة 26: بإمكان ضباط الشرطة القضائية وعملاء الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني (ANSICE) أن :

أ) تأمر شخصا موجودا في الأراضي الوطنية لتقديم البيانات الرقمية المحددة التي في حوزته أو تحت سيطرته، والتي تم تخزينها في نظام حاسوبي أو وسيلة تخزين حاسوبية.
ب) تأمر مزود خدمات داخل الأراضي الوطنية، لتوصيل البيانات التي بحوزته أو الخاضعة لسلطته والمتعلقة بالمشتركين و بهذه الخدمات.

المادة 27: للحصول على معرفة المخالفات المنصوص عليها في هذا القانون، بإمكان ضباط الشرطة القضائية وعملاء وكالة (ANSICE) المختصون، استخدام الوسائل التقنية المناسبة لجمع أو تسجيل، في الوقت الفعلي، البيانات المتعلقة بمحتوى إتصالات محدد داخل الأراضي الوطنية، تم نقلها عن طريق نظام معلوماتي. يجوز لهم، في نفس الظروف الطلب من مزود خدمة، بحكم قدرته التقنية، تقديم دعمه ومساعدته للسلطات المختصة لجمع وتسجيل تلك البيانات.

peuvent, dans les mêmes circonstances, obliger un fournisseur de services, en considération de ses capacités techniques, à prêter aux autorités compétentes, son concours et son assistance pour la collecte ou enregistrement de ces données.

Article 28 : Le fournisseur de services a l'obligation de garder le secret sur les informations reçues.

Article 29 : Les officiers de police judiciaire et les agents habilités de l'ANSICE peuvent collecter, enregistrer ou ordonner la collecte ou l'enregistrement par l'utilisation de moyens techniques existant sur le territoire national ou obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

a) à collecter ou à enregistrer les informations requises par l'utilisation de moyens techniques existant sur son territoire ;
b) à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Article 30 : Le fournisseur de services est tenu de garder le secret sur le fait que l'un quelconque des pouvoirs prévus dans le présent article ait été exécuté ainsi que toute information à ce sujet.

Article 31 : Si les officiers de police judiciaire et les agents habilités de l'ANSICE sont convaincus que dans le cadre d'une enquête concernant une infraction prévue par la présente loi, il y a des motifs raisonnables de croire que des preuves essentielles ne peuvent pas être collectées par l'application d'autres instruments énumérés au chapitre I, du titre III de la présente loi, ils peuvent utiliser un logiciel à distance et l'installer dans le système informatique de la personne mise en cause afin de recueillir les éléments de preuve pertinents recherchés.

Afin d'éviter tout abus, la démarche doit nécessairement mentionner par écrit les informations suivantes :

a) la personne mise en cause, si possible avec nom et adresse ;
b) la description du système informatique ciblée ;
c) la description de la mesure envisagée, l'étendue et

المادة 28: على مزود الخدمة الحفاظ على سرية المعلومات الواردة.

المادة 29: بإمكان ضباط الشرطة القضائية وعملاء وكالة (ANSICE)، جمع أو تخزين أو الأمر بالجمع أو التسجيل عن طريق استخدام الوسائل التقنية المتاحة في الأراضي الوطنية أو إجبار مزود خدمات، في إطار قدرته التقنية على:

أ) جمع أو تسجيل المعلومات المطلوبة عن طريق استخدام الوسائل التقنية المتاحة في بلده؛

ب) تقديم دعمه ومساعدته للسلطات المختصة لجمع أو تسجيل في الوقت الفعلي، البيانات متعلقة بالحركة المرتبطة باتصالات محددة في أراضيها من خلال نظام معلوماتي.

المادة 30: على مزود الخدمات الإحتفاظ بالسرية، إلى أن يتم تنفيذ أحد الأحكام المذكورة في هذه المادة بالإضافة إلى أية معلومة حول هذا الموضوع.

المادة 31: إذا اقتنع ضباط الشرطة القضائية وعملاء وكالة (ANSICE)، في إطار تحقيق في جريمة بموجب هذا القانون، هناك أسباب معقولة للاعتقاد بأن الأدلة الأساسية لا يمكن جمعها عن طريق تطبيق الإجراءات الواردة في الفصل الأول من الباب الثالث من هذا القانون، فإنه يمكن استخدام البرمجيات عن بعد وربطها بنظام كمبيوتر الشخص المتهم من أجل جمع الأدلة المطلوبة.

تفاديا للتجاوزات، يجب أن يتضمن الإجراء بالضرورة المعلومات التالية:

أ) الشخص المتهم مع ذكر الاسم والعنوان إن أمكن؛

ب) وصف النظام المعلوماتي المستهدف؛

ج) وصف الإجراءات ومدى ومدة الاستخدام؛

د) أسباب الحاجة إلى استخدام البرنامج.

la durée de l'utilisation ;

d) les raisons de la nécessité de l'utilisation du logiciel.

SECTION I : DE LA CONSERVATION DES DONNEES

Article 32 : Lorsqu'il y a des raisons de penser que des données archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle pendant une durée de dix (10) ans maximum, pour la bonne marche des investigations judiciaires.

La personne en charge de la garde des données ou toute autre personne chargée de conserver celles-ci est tenue d'en garder le secret.

Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

Article 33 : Si les nécessités de l'information l'exigent et lorsqu'il y a des raisons de craindre la disparition des données archivées valant preuve, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de dix (10) ans maximum, pour la bonne marche des investigations judiciaires.

SECTION II : DE LA PERQUISITION ET DE LA SAISIE INFORMATIQUES

Article 34 : lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données sur le territoire national, sont utiles à la manifestation de la vérité, le juge peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un système informatique situé en dehors du territoire national, elles sont recueillies par

القسم الأول: عن حفظ البيانات

المادة 32: عندما يكون هناك سبب للاعتقاد بأن البيانات المخزنة في نظام حاسوبي معرضة بشكل خاص للخسارة أو التعديل، بإمكان قاضي التحقيق أن يأمر أي شخص لصون وحماية سلامة البيانات التي بحوزته أو تحت سيطرته لمدة عشر (10) سنوات كحد أقصى لحسن سير التحقيقات القضائية.

على الشخص المكلف بحفظ البيانات أو أي شخص آخر مكلف بحفظها أن يلتزم بالسرية.
فإن أي انتهاك للسرية يؤدي إلى العقوبات المطبقة في انتهاك السرية المهنية.

المادة 33: إذا ما دعت ضرورة الإعلام أو عندما يكون هناك سبب للتخوف من فقدان بيانات مؤرشفة ذات قيمة برهانية، يجوز للقاضي أن يأمر أي شخص لصون وحماية سلامة البيانات التي بحوزته أو تحت سيطرته، لمدة عشر (10) سنوات كحد أقصى لحسن سير التحقيقات القضائية

القسم الثاني: عن التفتيش ومصادرة الأجهزة الحاسوبية

المادة 34: عندما تكون البيانات المخزنة في نظام معلوماتي أو في وسيط حفظ بيانات عبر الأراضي الوطنية، وهي مفيدة في إبراز الحقيقة، يمكن للقاضي أن يتنفذ عملية تفتيش أو الوصول إلى نظام معلوماتي أو جزء منه أو نظام معلوماتي آخر، عندما تكون البيانات ممكنة المنال أو متوفرة في النظام الأولي.

إذا مسبقا أن هذه البيانات يمكن الوصول إليها من المرحلة الأولى أو متاحة عبر النظام الأولي، وهي مخزنة في نظام معلوماتي خارج الأراضي الوطنية، يتم جمعها من قبل القاضي، مع مراعاة شروط الالتزامات الدولية.

le juge, sous réserve des conditions d'accès prévues par les engagements internationaux.

Article 35 : Lorsque le juge découvre dans un système informatique des données stockées qui sont utiles à la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

Le juge désigne toute personne qualifiée pour utiliser les moyens techniques appropriées afin d'empêcher l'accès aux données visées à l'alinéa ci-dessus dans le système informatique ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le juge ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Lorsque la mesure prévue à l'alinéa 2 du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge utilise les moyens techniques appropriées pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Le juge informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Article 36 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait

المادة 35: إذا تبين للقاضي أن بيانات مخزنة في نظام معلوماتي تفيد لاكتشاف الحقيقة، ولكن مصادرة الوسيلة لا تبدو مرغوبة، يمكن نسخ هذه البيانات، في وسائط تخزين وتظل محفوظة.

فيعين القاضي شخصا مؤهلا لاستخدام الوسائل التقنية المناسبة للحيلولة دون الوصول إلى البيانات المشار إليها في الفقرة أعلاه في النظام المعلوماتي أو نسخ من البيانات المتوفرة التي بحوزة شخصية مخولة باستخدام النظام الحاسوبي لضمان سلامتها.

إذا ما كانت البيانات المرتبطة بالمخالفة، هي الغاية، أو الهدف، تعتبر مخالفة للنظام العام أو الآداب العامة أو تشكل خطرا على سلامة الأنظمة المعلوماتية أو البيانات المخزنة، التي تمت معالجتها أو نقلها من خلال هذه الأنظمة؛ يأمر القاضي باتخاذ التدابير الوقائية اللازمة، بما في ذلك تعيين أشخاص مؤهلين في مهمة تهدف الى استخدام كل الوسائل التقنية المناسبة لجعل هذه البيانات غير ممكنة الوصول.

عندما تكون الإجراءات المنصوص عليها في الفقرة 2 من هذه المادة غير ممكن لأسباب فنية أو بسبب حجم البيانات، يستخدم القاضي الوسائل التقنية المناسبة لمنع الوصول إلى البيانات في النظام المعلوماتي، فضلا عن نسخ من البيانات المتوفرة للمستخدمين المرخص لهم في استخدام النظام المعلوماتي وكذلك لضمان سلامتها.

يقوم القاضي بإبلاغ مسؤول النظام المعلوماتي للأبحاث التي أجريت في النظام ويوصل نسخة من البيانات التي تم نسخها، والتي أصبحت غير متاحة.

المادة 36: عندما يبدو أن البيانات المحتجزة أو التي تم الحصول عليها أثناء التحقيق أو التي أصبحت محل عملية نقل جعلتها غير متاحة أو من شأنها أن تعرض المعلومات التي تحتويها للتلاف، على مدعى

l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

SECTION III : DE L'INTERCEPTION DES DONNEES INFORMATIQUES

Article 37 : Si les nécessités de l'information l'exigent, le juge d'instruction peut, sur réquisition du Procureur de la République, utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu des communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, avec les moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatiques.
Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation de secret professionnel.

Article 38 : En cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction saisie peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction, en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement.

Le juge peut faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction, à toute personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

الجمهورية، وقاضي التحقيق أو المحكمة، تفويض أي شخصية طبيعية أو اعتبارية مؤهلة، لأداء العمليات الفنية للحصول على نسخة واضحة من هذه البيانات.
عندما تستخدم وسيلة ترميز، بإمكان السلطات القضائية أن تطلب الاتفاقية السرية للتشفير وفك الرموز.

القسم الثالث: اعتراض البيانات الحاسوبية

المادة 37: إذا ما دعت ضرورة الاعلام المطلوبة، بناء على طلب مدعي الجمهورية ، بإمكان قاضي التحقيق استخدام الوسائل التقنية المناسبة لجمع أو تسجيل البيانات في الوقت الحقيقي على محتوى اتصالات محددة تم نقلها عن طريق نظام معلوماتي، أو إجبار مزود خدمات، وذلك بحكم قدرته التقنية التي يتمتع بها، في جمع أو تسجيل بيانات بالوسائل التقنية المتاحة، أو تقديم مساعدته للسلطات المختصة لجمع أو تسجيل البيانات المعلوماتية المطلوبة.
المزود بالخدمات ملزم بالحفاظ على السرية. فإن أي انتهاك للسرية يؤدي إلى عقوبات جريمة خرق السرية المهنية.

المادة 38: في حالة الإدانه بجريمة ارتكبت من خلال وسيلة اتصال رقمي، يجوز للمحكمة أن تفرض عقوبات إضافية، حظر إصدار رسائل الاتصال الرقمية، الحظر المؤقت أو الدائم من الوصول إلى الموقع المستخدم في ارتكاب الجريمة، أو قطع الوصول إلى جميع الوسائل التقنية المتاحة أو حتى منع الإقامة.
يجوز للقاضي أن يأمر أي شخص مسؤول قانونا عن الموقع المستخدم في ارتكاب الجريمة، أي شخص مؤهل لتنفيذ الوسائل الفنية اللازمة لضمان حظر الوصول، واستضافة أو القطع الوصول إلى موقع الاجرام.

Article 39 : En cas de condamnation pour une infraction commise par le biais d'un support numérique, le juge ordonne à titre complémentaire la diffusion au frais du condamné, par extrait, de la décision sur ce même support.

La publication prévue à l'alinéa précédent doit être exécutée dans les quinze (15) jours calendaires suivant le jour où la condamnation est devenue définitive.

La personne condamnée qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa précédent sera puni des peines prévues par le Code pénal.

Si dans le délai de quinze (15) jours après que la condamnation soit devenue définitive, la personne condamnée n'a pas diffusé ou fait diffuser cet extrait, les peines prévues au présent article sont portées au double.

CHAPITRE II : DES DROITS, OBLIGATIONS ET MESURES DE SECURITE ELECTRONIQUE

SECTION I : DES DROITS ET OBLIGATIONS RELATIVES A LA VIE PRIVEE

Article 40 : Toute personne a droit au respect de sa vie privée. Les juges peuvent prendre les mesures conservatoires, notamment le séquestre et la saisie pour empêcher ou faire cesser une atteinte à la vie privée.

Article 41 : Les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information sont tenus d'assurer la confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information, y compris les données relatives au trafic.

Article 42 : Le fournisseur de contenus est responsable des contenus véhiculés par son système d'information, notamment lorsque ces contenus portent atteinte à la dignité humaine, à l'honneur et à la vie privée.

Article 43 : Il est interdit à toute personne physique ou morale d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférent, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés, sauf lorsque cette personne y

المادة 39: في حالة الإدانة بجريمة ارتكبت من خلال وسيط رقمي، يأمر القاضي بصفة تكميلية أن ينشر على نفقة المدان استخراج نسخ من قرار الحكم بواسطة نفس الوسيلة.

النشر المنصوص عليه في الفقرة السابقة يجب أن يتم تنفيذها خلال خمسة عشر يوما (15) حسب التقييم الميلادي حيث يتم الحكم النهائي.

إن الشخص المدان الذي لا يتنشر أو لن ينشر قرار الحكم في الفقرة السابقة يعاقب بالعقوبات المنصوص عليها في قانون العقوبات الجزائية.

إذا لم يقوم المدان بنشر قرار الحكم، خلال خمسة عشر بعد (15) يوما وهو الحكم النهائي، تضاعف العقوبات المنصوص عليها في هذه المادة.

الفصل الثاني: الحقوق والواجبات وتدابير الأمن الالكتروني

القسم الأول: حقوق والتزامات متعلقة بالحياة الشخصية

المادة 40: لكل شخص الحق في احترام حياته الخاصة. بإمكان القضاة إتخاذ تدابير تحفظية، خصوصا العزل والمصادرة لمنع أو وقف انتهاك الخصوصية.

المادة 41: على مستخدمي شبكات الاتصالات الإلكترونية ونظم المعلومات الالتزام بضمان سرية الاتصالات الممررة عبر شبكات الاتصالات الإلكترونية ونظم المعلومات، بما في ذلك بيانات حركة المرور.

المادة 42: مزود المحتوى هو مسؤول عن المحتوى التي يحملها نظام المعلومات الخاصة به، وخصوصا عندما تنتهك هذه المحتويات الكرامة الإنسانية والشرف والخصوصية.

المادة 43: يحظر على أي شخصية طبيعية أو اعتبارية استماع، وتنصت، وتخزين حركة الاتصالات والبيانات المتعلقة بالمرور، أو أن يخضعها لأية أنواع أخرى من الإعتراض أو المراقبة دون موافقة

est légalement autorisée.

Toutefois, le stockage technique préalable à l'acheminement de toute communication est autorisé aux opérateurs et exploitants des réseaux de communications électroniques, sans préjudice du principe de confidentialité.

Article 44 : L'enregistrement des communications et des données de trafic y afférentes, effectué dans le cadre professionnel en vue de fournir la preuve numérique d'une communication électronique est autorisé.

Article 45 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, sont tenus de conserver les contenus ainsi que les données stockées dans leurs installations pendant une durée de dix (10) ans maximum.

Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, ont l'obligation de mettre en place des dispositifs nécessaires pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Article 46 : L'utilisation des réseaux de communications électroniques et des systèmes d'information aux fins de stocker les informations ou d'accéder à des informations stockées dans un équipement terminal d'une personne physique ou morale, ne peut se faire qu'avec son consentement préalable ou à la demande des autorités judiciaires.

Article 47 : L'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer une adresse valide à laquelle le destinataire peut transmettre une demande visant à obtenir l'arrêt de ces informations est interdite.

Article 48 : L'émission des messages électroniques en usurpant l'identité d'autrui est interdite.

Article 49 : Les personnes dont l'activité est d'offrir un accès à des services de communications électroniques, sont tenus d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à

المستخدمين المعنيين، إلا في حالة كون هذا الشخص مخول بذالك قانونا.
إلا أنه، يسمح بالتخزين التقني قبل تقديم أي اتصال مسموح به لمشغلي شبكات الاتصالات الإلكترونية، دون المساس بالسرية.

المادة 44: يسمح بتسجيل الاتصالات وبيانات حركة المرور ذات الصلة، المستخدمة في إطار شخصي بهدف توفير الأدلة الرقمية المسموح بها.

المادة 45: مزودي محتوى شبكات الاتصالات الإلكترونية ونظم المعلومات مطالبون بالحفاظ على محتويات البيانات المخزنة في مرافقها لمدة عشر (10) سنوات كحد أقصى.

مزودي محتويات الشبكات الالكترونية ونظم المعلومات ملزمون بوضع آليات لمواجهة الانتهاكات التي تضر بالبيانات الشخصية وخصوصية المستخدم.

المادة 46: استخدام شبكات الاتصالات الإلكترونية ونظم المعلومات لتخزين المعلومات أو الوصول إلى المعلومات المخزنة في المعدات الطرفية لشخصية طبيعية أو اعتبارية، لا يمكن أن تتم إلا بالموافقة المسبقة نفسها أو بناء على طلب من السلطات القضائية.

المادة 47: إصدار الرسائل الإلكترونية لأغراض التسويق بإخفاء هوية المرسل نيابة عنه، أو دون تحديد عنوان صالح يمكن المتلقي من إرسال طلب لإيقاف هذه المعلومات محظور.

المادة 48: إصدار الرسائل الإلكترونية بانتحال هوية الغير محظور.

المادة 49: إن الاشخاص الذين يرتكز نشاطهم في توفير الولوج إلى الاتصالات الإلكترونية، ملزمون بإشعار مشتركيهم بوجود وسائل تقنية لتقييد الوصول إلى خدمات معينة أو إنتقائها أو أن يقترح لهم احد هذه الخيارات على الأقل.

المادة 50: إنه من مسؤولية أولئك الذين يقومون حتى مجانا، بتخزين إشارات أو كتابات أو صور أو أصوات أو

certains services ou de les sélectionner et leur proposer au moins un de ces moyens.

Article 50 : La responsabilité des personnes qui assurent, même à titre gratuit, le stockage des signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis aux destinataires de ces services, peut être engagée.
Toutefois, la responsabilité prévue à l'alinéa 1 ci-dessus n'est point engagée dans les cas suivants :

a) si les personnes n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;

b) si, dès le moment où elles ont eu connaissance des faits, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

Article 51 : Les personnes mentionnées aux articles 49 et 50 ci-dessus, sont tenues de conserver, pendant une durée de dix (10) ans, les données permettant l'identification de toute personne ayant contribué à la création du contenu des services dont elles sont prestataires.
L'autorité judiciaire peut requérir communication des données prévues à l'alinéa 1 ci-dessus auprès des prestataires mentionnés aux articles 49 et 50.

Article 52 : La juridiction compétente saisie doit statuer dans un délai maximum de trois (3) mois sur toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Article 53 : Toute personne victime d'une diffamation au moyen d'un service de communications électroniques, dispose d'un droit de réponse et peut en exiger la rectification suivant les conditions prévues par les textes en vigueur.

En cas de refus ou de non publication de son droit de réponse, la personne victime d'une diffamation peut user des voies de droit prévues par les textes en vigueur pour obtenir réparation du préjudice subi.

Article 54 : Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir

رسائل من أي نوع كان، موجهة إلى المستفيدين.
ومع ذلك، لا يدخل في إطار المسؤولية الواردة في الفقرة 1 أعلاه، في الحالات التالية:
أ) إذا لم يكن لدى الأشخاص المعرفة الفعلية للطابع غير القانونية أو الأحداث أو الوقائع التي تظهر هذا الطابع.

ب) إذا كان هؤلاء منذ الحين بعلم عن الحقائق، فيتصرفون على الفور لإزالة البيانات أو جعلها مستحيلة الوصول.

المادة 51: إن الأشخاص المشار إليهم في المادتين 49 و50 أعلاه، ملزمون بالحفاظ على البيانات، لمدة عشر (10) سنوات، هذه البيانات تمكن من تشخيص أي شخص ساهم في إنشاء محتوى الخدمات التي قدموها.
بإمكان السلطة القضائية أن تطلب تقديم البيانات المنصوص عليها في الفقرة 1 أعلاه لدى مقدمي الخدمات المذكورين في المادتين 49 و 50.

المادة 52: إن المحاكم المختصة يجب أن تصدر الحكم خلال مدة أقصاها ثلاثة (3) أشهر على جميع التدابير اللازمة لمنع الإصابة أو وقف الأضرار المتسببة عن محتوى خدمة الاتصالات الإلكترونية.

المادة 53: أي ضحية بهتان من قبل خدمة الاتصالات الإلكترونية، لديها حق الرد والمطالبة بالتصحيح طبقا للشروط المنصوص عليها في التشريع المعمول به.

في حالة الرفض أو عدم نشر حقها في الرد، بإمكان ضحية بهتان أن تلجأ للسبل القانونية التي نصت عليها القوانين المعمول بها من أجل الحصول على تعويض عن الأضرار لحقت بها.

المادة 54: يعاقب كل من يقوم بنشاط نقل المحتوى في شبكة الاتصالات الإلكترونية أو توفير سبل الوصول إلى شبكة الاتصالات الإلكترونية، لا يمكن أن يكون مسؤولا عن ذالك إلا في الحالات التالية:
أ) إذا كان السبب في طلب النقل المتنازع فيه؛
ب) يختار أو يعدل موضوع المحتوى الذي تم توصيله.

sa responsabilité engagée que lorsqu'elle :

a) est à l'origine de la demande de transmission litigieuse ;
b) sélectionne ou modifie les contenus faisant l'objet de la transmission.

Article 55 : Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet, ne peut voir sa responsabilité civile ou pénale engagée en raison de ces contenus que dans le cas où elle :

a) a modifié ces contenus ;
b) ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour ; ou
c) a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir les données.

SECTION II : DE L'OBLIGATION DE PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES

Article 56 : Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques sont tenus de prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts. A cet effet, ils sont tenus d'informer les usagers :

a) du danger encouru en cas d'utilisation de leurs réseaux ;
b) des risques particuliers de violation de la sécurité notamment, les dénis de service distribués, le re-routage anormal, les pointes de trafic, le trafic et les ports inhabituels, les écoutes passives et actives, les intrusions et tout autre risque ;
c) de l'existence de moyens techniques permettant d'assurer la sécurité de leurs communications.

Article 57 : Les opérateurs de réseaux et les fournisseurs de services de communications électroniques ont l'obligation de conserver les données de connexion et de trafic pendant une période de dix (10) ans.

Les opérateurs de réseaux et les fournisseurs de services de communications électroniques sont tenus d'installer des mécanismes de surveillance de trafic des données de leurs

المادة 55: أي شخص قام بغرض جعل نقل المعلومات اللاحق أكثر فعالية، أو أنشطة تخزين آلي، لمرحلة إنتقالية ومؤقتة، لمحتوى قام بتحويله مزود خدمات، ليس له أية مسؤولية مدنية أو جزائية بسبب هذه المحتويات في حالة أنها:

أ) قامت بتعديل هذه المحتويات.

ب) لا تتوافق مع ظروفه الولوج والقواعد المعتادة بشأن التحديث؛ أو

ج) قد أدى إلى إعاقة الاستخدام القانوني والعرفي للتكنولوجيا المستخدمة للحصول على البيانات.

القسم الثاني: عن الالتزام بحماية شبكات الاتصالات الإلكترونية

المادة 56: على مشغلي شبكات الاتصالات الإلكترونية ومقدمي خدمات الاتصالات الالكترونية اتخاذ جميع التدابير الفنية والإدارية لضمان سلامة الخدمات المقدمة؛ ولهذه الغاية فإنهم ملزمون بإبلاغ المستخدمين بـ:

أ) الخطر المتوقع عند استخدام شبكاتهم.

ب) المخاطر الخاصة بخرق للأمن ولا سيما الحرمان من الخدمة الموزعة، إعادة المرور والموانئ العادية، والتنصت السلبي والاقتحام وغيرها من المخاطر.

ج) وجود وسائل تقنية لضمان أمن الاتصالات الخاصة بهم.

المادة 57: إن مشغلي الشبكات وخدمات الاتصالات الإلكترونية ملزمون بالحفاظ على بيانات حركة المرور لمدة عشر (10) سنوات.

وملزمون أيضا بإنشاء آليات مراقبة مرور البيانات في شبكاتهم. يمكن الوصول إلى هذه البيانات عند التحقيقات القضائية.

إن لمشغلي الشبكات و مقدمي خدمات الاتصالات الإلكترونية مسؤولية إذا ما استخدمت البيانات المنصوص عليها في الفقرة 2 أعلاه لإنتهاك الحريات الفردية للمستخدمين.

réseaux. Ces données peuvent être accessibles lors des investigations judiciaires.

La responsabilité des opérateurs de réseaux et celles des fournisseurs de services de communications électroniques est engagée si l'utilisation des données prévue à l'alinéa 2 ci-dessus porte atteinte aux libertés individuelles des usagers.

SECTION III : DE L'OBLIGATION DE PROTECTION DES SYSTEMES D'INFORMATION

Article 58 : Les exploitants des systèmes d'information sont tenus de prendre toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A cet effet, ils doivent se doter de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer de manière continue les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement.

Les exploitants des systèmes d'information doivent mettre en place des mécanismes techniques pour faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique.

Les mécanismes prévus à l'alinéa 2 ci-dessus, doivent faire l'objet d'approbation par l'ANSICE.

Les plates-formes des systèmes d'information doivent faire l'objet de protection contre d'éventuels rayonnements et des intrusions qui pourraient compromettre l'intégrité des données transmises et contre toute autre attaque externe notamment par un système de détection d'intrusions.

Article 59 : Les personnes morales dont l'activité est d'offrir un accès à des systèmes d'information sont tenues d'informer les usagers :

a) du danger encouru dans l'utilisation des systèmes d'information non sécurisés notamment pour les particuliers ;

b) de la nécessité d'installer des dispositifs de contrôle parental ;

القسم الثالث: عن مسؤولية حماية نظم المعلومات

المادة 58: مشغلي نظم المعلومات ملزمون باتخاذ جميع التدابير الفنية والإدارية لضمان سلامة الخدمات؛ تحقيقا لهذه الغاية، يجب تطوير نظم موحدة تسمح لهم بتشخيص وتقييم وعلاج بشكل مستمر إدارة مخاطر أمن نظم المعلومات في سياق الخدمات المقدمة بشكل مباشر أو غير مباشر.
يجب على مشغلي نظم المعلومات وضع آليات تقنية لمواجهة الاضرار التي تلحق بالنظم، وسلامتها، وسمعتها وعدم التنصل من قبل المستخدمين، وخصوصية البيانات والأمن المادي.

إن الآليات المنصوص عليها في الفقرة 2 أعلاه، يجب أن تخضع لموافقة وكالة (ANSICE).
يجب أن تكون منصات نظم المعلومات محل حماية من الإشعاع والاختراقات التي يمكن أن تهدد سلامة البيانات المرسلة، وضد أي هجوم خارجي من قبل نظام رصد التسلل الممكن.

المادة 59: إن الأشخاص الاعتبارية التي يكمن عملها في توفير ولوج نظم المعلومات ملزمون بإبلاغ المستخدمين بـ:
أ) الخطر في استخدام نظم معلومات غير آمنة بشكل خاص للأفراد.
ب) الحاجة إلى تثبيت عناصر تحكم الوالدين؛

ج) مخاطر االاختراقات الأمنية، بما في ذلك الفيروسات.

د) وجود وسائل تقنية لتقييد الوصول إلى خدمات معينة وتقديم خيارات على الأقل من هذه الوسائل، بما في ذلك استخدام أحدث أنظمة التشغيل وأدوات مكافحة الفيروسات ومكافحة برامج التجسس والغش،

c) des risques particuliers de violation de sécurité, notamment la famille générique des virus ;

d) de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents, les outils antivirus et contre les logiciels espions et trompeurs, l'activation des pare-feu personnels, de systèmes de détection d'intrusions et l'activation des mises à jour automatiques.

Article 60 : Les exploitants des systèmes d'information sont tenus d'informer les utilisateurs de l'interdiction faite d'utiliser le réseau de communications électroniques pour diffuser des contenus illicites ou tout autre acte qui peut entamer la sécurité des réseaux ou des systèmes d'information, ou attenter à la vie privée des individus.

L'interdiction porte également sur la conception de logiciel trompeur, de logiciel espion, de logiciel potentiellement indésirable ou de tout autre outil conduisant à un comportement frauduleux.

Article 61 : Les exploitants des systèmes d'information ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix (10) ans.

Les exploitants des systèmes d'information sont tenus d'installer des mécanismes de surveillance et de contrôle d'accès aux données de leurs systèmes d'information. Les données conservées doivent être accessibles lors des investigations judiciaires.

Les installations des exploitants des systèmes d'information peuvent faire l'objet de perquisition ou de saisie sur ordre d'une autorité judiciaire dans les conditions prévues par les lois et règlements en vigueur.

Article 62 : Les exploitants des systèmes d'information doivent évaluer et réviser périodiquement leurs systèmes de sécurité et introduire en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies.

وتفعيل جدران الحماية الشخصية، وأنظمة كشف التسلل وتمكين التحديثات التلقائية.

المادة 60: إن مشغلي نظم المعلومات ملزمون بإعلام المستخدمين عن الحظر المفروض على استخدام شبكة الاتصالات الإلكترونية لنشر محتوى غير قانوني أو أي عمل آخر قد يؤثر على أمن الشبكات وأنظمة المعلومات، أو تعريض خصوصية الأفراد.

ويشمل الحظر أيضا تصميم البرامج المضللة، والبرمجيات التجسسية، والبرامج الغير المرغوب فيها أو أي أداة أخرى تؤدي إلى سلوك احتيالي.

المادة 61: إن مشغلي نظم المعلومات ملزمون بالحفاظ على الاتصال ونقل البيانات من أنظمة المعلومات الخاصة بهم لمدة عشر (10) سنوات.

مشغلو نظم المعلومات ملزمون بإدخال آليات للرصد والتحكم في الوصول إلى البيانات في نظم المعلومات الخاصة بهم. يجب أن يكون الوصول إليها متاحا أثناء التحقيقات القانونية.

يمكن أن تكون منشآت مستثمري نظم المعلومات محل تفتيش أو مصادرة بناءا على أمر من سلطة قضائية في إطار الشروط التي تحددها القوانين والنظم السارية.

المادة 62: على مشغلي نظم المعلومات القيام بالتقييم والمراجعة الدورية لأنظمة سلامتهم وإدخال إذا لزم الأمر، التغييرات المناسبة في ممارساتها، وتدابير وتقنيات السلامة وفقا لتطور التكنولوجيا.

يمكن أن يتعاون مشغلوا ومستخدمو نظم المعلومات في تطوير وتنفيذ ممارسات وتدابير تقنيات سلامة أنظمتها.

المادة 63: مقدموا المحتويات الالكترونية وشبكات الاتصالات ونظم المعلومات ملزمون بضمان توفير

Les exploitants des systèmes d'information et leurs utilisateurs peuvent coopérer entre eux pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.

Article 63 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations.

Ils ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

SECTION IV : DE L'OBLIGATION D'AUDIT

Article 64 : Les réseaux de communications électroniques et les systèmes d'information des opérateurs, des Autorités de certification et des fournisseurs de services de communications électroniques sont soumis à l'audit de sécurité obligatoire et périodique par l'Agence Nationale de Sécurité Informatique et de Certification Electronique (ANSICE).

L'audit de sécurité et les mesures d'impact de gravité sont effectués chaque année ou lorsque les circonstances l'exigent.

Les rapports d'audit sont confidentiels et adressés au Ministre en charge des Technologies de l'Information et de la Communication.

Les conditions d'évaluation des niveaux d'impact de gravité, ainsi que les conditions et les modalités de l'audit de sécurité seront fixées par voie règlementaire.

Article 65 : Le personnel de l'ANSICE et les experts commis en vue d'accomplir des opérations d'audit sont astreints au secret professionnel.

CHAPITRE III : DES INFRACTIONS DE CYBERCIMINALITE

SECTION I : DES ATTEINTES AUX SYSTEMES INFORMATIQUES

Sous-Section 1 : Des atteintes à la confidentialité et à l'intégrité des systèmes informatiques

المحتوى، وكذلك البيانات المخزنة في منشآتهم. إن عليهم ضرورة إنشاء مصفاة لمواجهة الأضرار التي تلحق بالبيانات الشخصية وخصوصية المستخدم.

القسم الرابع: وجوب المراجعة

المادة 64 : شبكات الاتصالات الإلكترونية وأنظمة المعلومات وسلطات التصديق ومقدمي خدمات الاتصالات الإلكترونية يخضعون لمراجعة السلامة الإلزامية دوريا التي تقوم بها وكالة (ANSICE).

يتم تنفيذ التدقيق الأمني على مدى تأثير التضرر سنويا أو عندما تقتضيه الظروف.

تقارير المراجعة تبقى سرية وموجهة إلى الوزير المسؤول عن تكنولوجيا المعلومات والاتصالات.

يتم تحديد شروط تقييم حدة مستويات التأثير وشروط مراجعة السلامة الأمنية من خلال وسائل تنظيمية.

المادة 65: عمال الوكالة الوطنية للأمن المعلوماتي والإعتماد الإلكتروني (ANSICE) والموظفين والخبراء المكلفون بالمراجعة ملتزمون بالسرية المهنية.

الفصل الثالث: عن المخالفات الرقمية

القسم الأول: النيل من النظم المعلوماتية

القسم الفرعي 1: إنتهاك سرية وسلامة نظم المعلوماتية

المادة 66: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين أي شخص يدخل أو يحاول ولوج نظام معلوماتي عن طريق الغش، كل أو جزء من نظام معلوماتي.

يعاقب بنفس العقوبات، من حاول الحصول عن طريق الاحتيال لنفسه أو لغيره، أي ميزة ما من خلال ولوج نظام معلوماتي.

Article 66 : Est punie d'un emprisonnement d'un (1) an à cinq ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique.

Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 67 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique.

Article 68 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui entrave, fausse ou tente d'entraver ou de fausser le fonctionnement d'un système informatique.

Sous-Section 2 : De l'introduction frauduleuse de données dans un système

Article 69 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui introduit ou tente d'introduire frauduleusement des données dans un système informatique.

SECTION II : DES ATTEINTES AUX DONNEES INFORMATIQUES

Sous-Section 1 : De la falsification et de l'usage des données falsifiées

Article 70 : Est punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de cinq (5) millions à cinquante (50) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui introduit ou tente d'introduire, altère ou tente d'altérer, efface ou tente d'effacer, supprime ou tente de supprimer

المادة 67: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين، أي الشخص يحاول أن يلج عن طريق الخداع جزء أو كل من نظام معلوماتي.

المادة 68: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين أي شخص يعرقل، أو يحاول عرقلة أو تضليل تشغيل نظام معلوماتي.

القسم الفرعي 2: إدخال بيانات غير شرعية في النظام

المادة 69: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين ، أي شخص يدخل أو يحاول إدخال بيانات في نظام معلوماتي بطريقة غير شرعية.

القسم الثاني: إنتهاك البيانات المعلوماتية

القسم الفرعي 1: عن تزوير واستخدام البيانات المزورة

المادة 70: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة ق من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين فقط، أي شخص يدخل أو يحاول إدخال، يغير أو يحاول تغيير ، يحذف أو يحاول حذف بطريقة غير شرعية بيانات زائفة بقصد تحميلها في النظام أو استخدامها لأغراض قانونية كما لو كانت أصيلة، بحيث أن تكون مقروءة مباشرة أو بطريقة دقيقة.

المادة 71: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من ثلاثة ملايين إلى ثلاثين (30) مليون فرنك، أو بإحدى هاتين العقوبتين كل من قام عن قصد باستخدام البيانات التي تم الحصول عليها وفقا للشروط المنصوص عليها في المادة 66 أعلاه.

frauduleusement 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.

Article 71 : Est punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de trois (3) millions à trente (30) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, en connaissance de cause, fait usage des données obtenues dans les conditions énoncées par l'article 66 ci-dessus.

Article 72 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Article 73 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, modifie ou tente de modifier frauduleusement des données informatiques.

Article 74 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit ou fabrique un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Article 75 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui obtient frauduleusement,

المادة 72: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين ، أي شخص يعترض أو يحاول اعتراض، بوسائل تقنية بيانات معلوماتية غير مخصصة للعامة أثناء نقلها من المرسل إلى المتلقي داخل النظام المعلوماتي.

المادة 73: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص يضر أو يحاول إضرار، يحذف أو محاول حذف، يتدهور أو يحاول تدهور، يغير أو يحاول تغيير بيانات معلوماتية بطريقة غير شرعية.

المادة 74: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين ، أي الشخص ينتج أو يصنع مجموعة من البيانات الرقمية عن طريق الدس، أو طمس أو إزالة، عن طريق الإحتيال بيانات إلكترونية مخزنة، تمت معالجتها أو إرسالها عن طريق نظام معلوماتي، مما ينتج بيانات مزيفة، بقصد أن تؤخذ في الاعتبار أو استخدامها لأغراض قانونية كما لو كانت الأصلي.

المادة 75: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين أي شخص يحصل عن طريق الاحتيال لنفسه أو الآخرين، أي ميزة، لإدخال، تعديل، حذف أو قمع بيانات الكمبيوتر أو أي شكل لعرقلة سير عمل نظام الكمبيوتر.

المادة 76: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين أي شخص، يقوم بمعالجة بيانات الشخصية ولو بإهمال دون مراعاة الشكليات قبل تنفيذها المنصوص عليها في قانون البيانات الشخصية المقدمة لهذا الغرض.

pour lui-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique.

Article 76 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, même par négligence, procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données personnelles prévue à cet effet.

Sous-Section 2 : Des abus de dispositifs

Article 77 : Est punie d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit, vend, importe, détient, diffuse, offre, cède ou met à disposition :

a) un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées par les articles 70, 71, 72, 73 et 74 ci-dessus ;

b) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 70, 71, 72, 73 et 74 ci-dessus.

Les auteurs de l'une des infractions prévues à l'article 81 ci-dessus encourent également les peines complémentaires suivantes :

a) la confiscation, selon les modalités prévues par les textes en vigueur, de tout objet destiné ou ayant servi à commettre l'infraction considéré, à l'exception des objets susceptibles de restitution ;

b) l'interdiction dans les conditions prévues par les textes en vigueur pour une durée de cinq (5) ans au moins, d'exercer une fonction publique ou une activité socioprofessionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions de la personne incriminée ;

القسم الفرعي 2: إساءة استخدام الأجهزة

المادة 77: يعاقب بالحبس من سنة واحد إلى ثلاث (3) سنوات وبغرامة من واحد مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص ينتج، يبيع، واردات، يمتلك، ويوزع، ويعرض للعامة:

أ) جهاز، بما في ذلك برنامج معلوماتي، مصمم أو مكيف في المقام الأول لغرض ارتكاب أي من الجرائم المشار إليها في المواد 70 و 71 و 72 و 73 و 74 أعلاه؛

ب) استخدام كلمة سر، رمز مرور، أو بيانات مماثلة من خلال توفير إمكانية الوصول إلى جميع أو جزء من نظام معلوماتي، مع نية أن يتم استخدامها لارتكاب أحد الجرائم بموجب المواد 70 و 71 و 72 و 73 و 74 أعلاه.

مرتكبي أحد الجرائم الواردة في المادة 81 أعلاه يتعرضون للعقوبات الإضافية التالية:

أ)مصادرة على النحو المنصوص عليه في القوانين النافذة، لأية أداة مستخدمة في ارتكاب الجريمة المذكورة، باستثناء المواد القابلة للاسترداد.

ب) الحظر على النحو المنصوص عليه في القوانين سارية المفعول لمدة خمس (5) سنوات على الأقل، لشغل الوظائف العامة أو المهنية الاجتماعية، عند ارتكاب الأفعال في سياق أو في فرصة لممارسة مهام الشخص المتهم؛

ج) الإغلاق، على النحو المنصوص عليه في القوانين السارية المفعول لمدة خمس (5) سنوات على الأقل، لمؤسسات واحد ة منها أو عدة من مؤسسات الشركة المستخدمة في ارتكاب الجريمة؛

د) إبعاد لمدة خمس (5) سنوات على الأقل، من السوق العامة.

القسم الفرعي 3: عن اختلاس الهوية الرقمية وتكوين جمعيات الإجرام الرقمي

المادة 78: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة

c) la fermeture, dans les conditions prévues par les textes en vigueur, pour une durée de cinq (5) ans au moins, des établissements ou de l'un ou plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
d) l'exclusion, pour une durée de cinq (5) ans au moins, des marchés publics.

Sous-Section 3 : De l'usurpation d'identité numérique, de l'association de malfaiteurs informatiques et de la complicité

Article 78 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui usurpe l'identité numérique d'un tiers ou une ou plusieurs données permettant d'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa considération ou à ses intérêts.

Article 79 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi.

Article 80 : Une personne qui intentionnellement commet un acte de complicité en vue de la perpétration d'une des infractions prévues par la présente loi, dans l'intention qu'une telle infraction soit perpétrée, commet une infraction punissable des mêmes peines que celles prévues pour l'infraction principale.

SECTION III : DES INFRACTIONS RELATIVES AU CONTENU

Sous-Section 1 : De la pornographie infantile

Article 81 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit en vue de sa diffusion, tente de produire en vue de la vente, offre, met à disposition, diffuse ou tente de diffuser de la pornographie

(10) ملايين فرنك، أي شخص يختلس الهوية الرقمية من طرف ثالث أو واحد أو بيانات عدة لزعزعة السلام، أو أمن الآخرين أو المساس بالشرف أو المصالح الشخصية.

المادة 79: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك، أو بإحدى هاتين العقوبتين ، أي شخص يشارك في جمعية تشكلت أو قائمة على ارتكاب أحد أو أكثر الجرائم المنصوص عليها في هذا القانون.

المادة 80: من يرتكب عمدا عملا من أعمال التواطؤ لارتكاب جريمة بموجب هذا القانون بقصد ارتكاب نفس الجريمة، أو يرتكب جريمة يعاقب عليها بنفس تلك العقوبات الواردة للجريمة الرئيسية.

القسم الثالث: الجرائم المتعلقة بالمحتوى

القسم الفرعي 1: من الصور الإباحية للأطفال

المادة 81: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك، الشخص الذي ينتج أو يحاول أن ينتج أو ينشر، في محاولة بيع أو عرض، أو توزيع أو يحاول توزيع المواد الإباحية عن الأطفال من خلال النظام المعلوماتي.

المادة 82: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك، إي شخص يحصل أو يقدم للآخرين، أو يجعل أي استيراد أو تصدير المواد الإباحية عن الأطفال من خلال نظام المعلوماتي.

المادة 83: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أي شخص يمتلك عن قصد مواد إباحية عن الأطفال في نظام معلوماتي أو أي وسيلة تخزين بيانات معلوماتية.

enfantine par le biais d'un système informatique.

Article 82 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui se procure ou procure à autrui, importe ou fait importer, exporter ou fait exporter de la pornographie enfantine par le biais d'un système informatique.

Article 83 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui possède intentionnellement de la pornographie enfantine dans un système informatique ou dans un moyen quelconque de stockage de données informatiques.

Article 84 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui facilite l'accès des mineurs à des images, des documents, du son ou une représentation présentant un caractère de pornographie.

Article 85 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui propose intentionnellement, par le biais des technologies de l'information et de la communication, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions prévues par les articles 81, 82, 83 et 84 ci-dessus.

Lorsque la proposition sexuelle a été suivie d'actes matériels conduisant à ladite rencontre, l'auteur commet une infraction aggravé punissable d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de deux (2) millions à vingt (20) millions de francs, ou de l'une de ces deux peines seulement.

Sous-Section 2 : Des actes racistes et xénophobes par le biais d'un système informatique

Article 86 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui crée, télécharge, diffuse ou

المادة 84: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أي شخص يسهل الوصول إلى القصر دون العمر القانوني، صورا، ووثائق، وأصوات ذات طابع إباحي.

المادة 85: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك ،أي شخص يقدم عمدا، من خلال تكنولوجيا المعلومات والاتصالات، لقاء مع قاصر، لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد 81، 82، 83 و 84 أعلاه. عندما يتبع الاقتراح الجنسي الأفعال المادية التي تؤدي إلى الاجتماع، يرتكب المؤلف جريمة يعاقب عليها بالسجن المشدد خمس (5) سنوات إلى عشر (10) سنوات وبغرامة مليونين اثنين إلى عشرين (20) مليون فرنك، أو بإحدى هاتين العقوبتين.

القسم الفرعي 2: عن الأعمال العنصرية وكراهية الأجانب عن طريق النظم الرقمية

المادة 86: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك ، أي شخص يخلق، أو يشحن، ويوزع أو يوفر بأي شكل من الأشكال سواء كانت مكاتيب، رسائل أو صور أو رسومات أو أي تمثيل آخر من الأفكار أو النظريات، أو الطبيعة العنصرية أو كراهية الأجانب، بواسطة نظام معلوماتي

المادة 87: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص ارتكب تهديدات من خلال نظام معلوماتي لشخص بسبب عضويته في مجموعة، تميزه على أساس العرق أو اللون أو النسب أو الأصل القومي التابعة له أو العضوية العرقية أو الدين، بمثابة ذريعة لأي من هذه العناصر، أو مجموعة من الأشخاص تمتاز بهذه الخصائص.

met à disposition sous quelle que forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

Article 87 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) à dix (10) millions de francs, ou de l'une de ces deux peines seulement,

toute personne auteur de menace commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'affiliation ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 88 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne auteur d'une insulte commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, la religion, l'affiliation ou l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 89 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, intentionnellement, nie, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

SECTION IV : DE LA NON EXECUTION DES INJONCTIONS ET DE LA DIVULGATION DES INFORMATIONS D'ENQUETE

Article 90 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne, autre que le mis en cause, qui omet intentionnellement sans excuse légitime ou

المادة 88: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة مالية من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص أخرج ونشر شتيمة من خلال نظام معلوماتي لشخص بسبب عضويته في مجموعة تمتاز على أساس العرق أو اللون أو النسب أو الأصل القومي، أو العرق أو الدين أو الرأي السياسي أو الانتماء إلى أحد هذه العضوية، بمثابة ذريعة لأي من هذه العناصر، أو مجموعة من الأشخاص تميزهم بهذه الخصائص.

المادة 89: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي الشخص ينفي عن قصد أو يوافق أو يبرر الأفعال التي تشكل جريمة الإبادة الجماعية أو جرائم ضد الإنسانية من خلال نظام معلوماتي.

القسم الرابع: عدم تنفيذ الأوامر والكشف عن معلومات التحقيق

المادة 90: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص آخر ماعدا المتهم يرفض عمدا دون عذر قانوني أو مبرر للامتثال لأمر من أوامر ضباط الشرطة وعملاء وكالة (ANSICE) المخولون.

المادة 91: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين،

أي مزود خدمة يتلقى أمر، كجزء من التحقيق الجنائي، الذي ينص صراحة على أن السرية يجب المحافظة عليها أو تصدر من القانون، ويقوم بكشفها دون عذر قانوني أو مبرر متعلق بالتحري؛

justification de se conformer à une injonction des officiers de police judiciaire et des agents habilités de l'ANSICE.

Article 91 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, tout fournisseur de service qui reçoit une injonction, dans le cadre d'une enquête criminelle, qui stipule explicitement que la confidentialité doit être maintenue ou qu'elle résulte de la loi et qui, intentionnellement et sans excuse ou justification légitime divulgue les informations relatives à l'enquête.

Article 92 : Est puni(e) d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, le responsable légal du site ayant servi à commettre l'infraction ou toute personne qualifiée pour mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé et qui ne respecte pas les injonctions émises par le juge à cet effet.

SECTION V : DES INFRACTIONS EN MATIERE DE CRYPTOLOGIE

Article 93 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui n'aura pas satisfait à l'obligation de communiquer à l'Autorité publique en charge de la cryptologie une description des caractéristiques techniques des moyens de cryptologie conformément aux textes s'y rapportant.

Article 94 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura importé un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable auprès de l'Autorité publique en charge de la cryptologie.

Article 95 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura fourni des prestations

المادة (92): يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، المسؤول القانوني للموقع المستخدم في ارتكاب الجريمة أو أي شخص مؤهل لتنفيذ الوسائل الفنية اللازمة لضمان حظر الوصول، واستضافة أو قطع الوصول إلى موقع و لا يمتثل للأوامر التي يصدرها القاضي لهذا الغرض.

القسم الخامس: عن البنيات التحتية في مجال التشفير

المادة 93: يعاقب بالسجن من سنة واحدة إلى خمس سنوات وبغرامة مالية من واحد مليون إلى عشرة ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص لا يستوفي الالتزام بإبلاغ السلطة العامة المسؤولة عن التشفير وصف الخصائص الفنية لطرق التشفير وفقا للنصوص ذات الصلة.

المادة 94: يعاقب بالسجن من سنة واحدة إلى خمس سنوات وبغرامة مالية من واحد مليون إلى عشرة ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص يقدم وسيلة للتشفير دون أية مصادقة مسبقة من السلطات المختصة بذالك؛

المادة 95: يعاقب بالسجن من سنة واحدة إلى خمس سنوات وبغرامة مالية من واحد مليون إلى عشرة ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص خدمات التشفير دون الحصول على موافقة مسبقة من السلطة العامة المسؤول عن التشفير.

المادة 96: يعاقب بالسجن من سنة واحدة إلى خمس سنوات وبغرامة مالية من واحد مليون إلى عشرة ملايين فرنك، أو بإحدى هاتين العقوبتين، أي شخص إستورد وسيلة للتشفير وليس له وظيفة تخوله بتلك المهام دون إذن مسبق من الهيئة العامة المسؤول عن التشفير.

de cryptologie sans en avoir obtenu préalablement l'agrément de l'Autorité publique en charge de la cryptologie.

Article 96 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura exporté un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans en avoir obtenu préalablement l'autorisation de l'Autorité publique en charge de la cryptologie.

Article 97 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura mis à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation.

Article 98 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui utilise un moyen de cryptologie pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission.

SECTION VI : DU SPAMMING

Article 99 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, de manière intentionnelle et sans excuse ou justification légitime :

a) déclenche intentionnellement la transmission de courriers électroniques multiples à partir ou par l'intermédiaire d'un système informatique ;
b) utilise un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages les destinataires ou tout prestataire de services de courriers électroniques ou de services internet ;
c) falsifie matériellement les informations se trouvant dans les en-têtes de messages électroniques multiples et déclenche intentionnellement la

المادة 97: يعاقب يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص وضع تحت تصرف شخص آخر وسيلة تشفير محظورة الاستخدام.

المادة 98: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص يستخدم وسيلة للتشفير لإعداد أو ارتكاب جريمة أو جنح أو تسهيل إعداد أو تلقي عمولات.

القسم السادس: الرسائل الدعائية

المادة 99: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة قدرها من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص، قام عن قصد ودون عذر قانوني أو مبرر:

أ) إطلاق رسائل إلكترونية متعددة من أو عن طريق نظام معلوماتي.
ب) استخدام نظام معلوماتي محمي لنقل أو إعادة إرسال رسائل الكترونية متعددة بقصد خداع أو تضليل متلقي الرسائل أو مقدمي خدمات البريد الإلكتروني أو خدمات الإنترنت؛
ج) يزيف ماديا المعلومات الموجودة في رؤوس رسائل البريد الإلكتروني المتعددة وينشر عن قصد مثل هذه الرسائل.

الباب الرابع: تكييف المخالفات التقليدية على تكنولوجيا المعلومات والاتصالات

الفصل الأول: الجرائم ضد الممتلكات

المادة 100: يعاقب بالسجن من سنة واحدة إلى خمس سنوات ودفع غرامة من واحد (1) مليون إلى عشرة (10) ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص نسخ أو يحاول تزييف بيانات معلوماتية

transmission desdits messages.

TITRE IV : DE L'ADAPTATION DES INFRACTIONS CLASSIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

CHAPITRE I : DES INFRACTIONS CONTRE LES BIENS

Article 100 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui copie ou tente de copier frauduleusement des données informatiques au préjudice d'un tiers.

Article 101 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, aura obtenu la remise ou aura tenté d'obtenir la remise de données informatiques et aura, par un de ces moyens, escroqué ou aura tenté d'escroquer en partie ou en totalité la fortune d'autrui.

Article 102 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, ayant reçu des propriétaires, possesseurs, ou détenteurs des données informatiques à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage ou pour un travail salarié ou non salarié, n'aura pas, après simple mise en demeure, exécuté son engagement de les rendre ou de les représenter, ou d'en faire un usage ou un emploi déterminé.

Article 103 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, sciemment, aura recelé, en tout ou en partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit.

Article 104 : Est considérée comme infraction aggravée et punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de (10) millions à cinquante (50) millions de francs, ou de l'une de ces deux peines seulement, le fait

على حساب الآخر.

المادة 101: يعاقب بالسجن من سنة إلى خمس سنوات ويدفع غرامة مالية من واحد مليون إلى عشر ملايين فرنك، أي شخص، من خلال استخدام أسماء وهمية أو صفات كاذبة، أو باستخدام أية وسيلة احتيالية، تحصل على بيانات أو حاول الحصول على تسلم بيانات معلوماتية وحاول من خلال هذه الوسائل، الإحتيال على جزء من ثروة أو بأكملها من ثروات الآخرين.

المادة 102: يعاقب بالسجن من سنة إلى خمس سنوات ويدفع غرامة مالية من واحد مليون إلى عشر ملايين فرنك، أي شخص، بعد أن تلقى من أصحاب ومالكي أو حاملي بيانات معلوماتية، بصفة إيجار، إيداع، ولاية ، توكيل، لخدمة مأجورة أو غير مأجورة، دون أي إنذار مسبق جعل منها وثائق عقود لخدمة، أو وظيفة محددة.

المادة 103: يعاقب بالسجن من سنة إلى خمس سنوات ويدفع غرامة مالية من واحد مليون إلى عشر ملايين فرنك أو بإحدى هاتين العقوبتين، أي شخص أخفى عن قصد، كليا أو جزئيا، بيانات معلوماتية، مختلسة أو التي تم الحصول عليها بارتكاب جريمة.

المادة 104: يعتبر جريمة خطرة ويعاقب عليها بالسجن لمدة خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من عشر ملايين إلى خمسين مليون فرنك، أو بإحدى هاتين العقوبتين، في حالة قيام أي شخص، أو من خلال أسماء وهمية أو صفات كاذبة أو باستخدام أي وسيلة مزورة، إستلم، أو يحاول أن يستلم أو أن يحصل إلى ممتلكات أو السندات، عملات، وعود، وإيصالات أو التصريف من خلال نظام الكمبيوتر أو شبكة الاتصالات الإلكترونية، من خلال أي من هذه الوسائل، والاحتيال أو محاولة للاحتيال جزئيا أو كليا على ثروة الآخرين.

pour toute personne qui, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, billets, promesses, quittances ou décharges par le biais d'un système informatique ou d'un réseau de communication électronique et aura, par un de ces moyens, escroqué ou tenté d'escroquer en partie ou en totalité la fortune d'autrui.

CHAPITRE II : DES ATTEINTES A LA DEFENSE NATIONALE

Article 105 : Est puni d'un emprisonnement de cinq (5) ans à dix (10) ans, tout citoyen tchadien qui :

a) livre à une puissance étrangère ou à ses agents, sous quelle que forme ou par quelque moyen que ce soit, un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;

b) s'assure, par quelque moyen que ce soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisée ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;

c) détruit ou laisse détruire un renseignement, objet, document, procédé, une donnée informatisée ou un fichier informatisé en vue de le (la) livrer à une puissance étrangère.

CHAPITRE III : DES INFRACTIONS DE PRESSE

Article 106 : Une personne qui commet une infraction de presse, notamment une diffamation, une injure publique, une apologie de crime, par le biais d'un moyen de communication électronique public, commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour les infractions de presse commises par d'autres moyens.

CHAPITRE IV : DE LA RESPONSABILITE DES PERSONNES MORALES

Article 107 : Les personnes morales autres que l'Etat, les collectivités territoriales décentralisées et les établissements publics sont responsables des infractions

الفصل الثاني: الانتهاكات الدفاع الوطني

المادة 105: يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات، أي مواطن تشادي:

أ) يقدم لقوة أجنبية أو وكلائها، في أي شكل أو بأي وسيلة سرا على الإطلاق، معلومات رقمية، وثيقة، وثائق ممسوحة ضوئيا، بيانات أو ملف إلكتروني خاص بمصلحة الدفاع الوطني.

ب) تأكد، بأي وسيلة حيازة مثل هذه المعلومات، وثيقة، عملية، وبيانات معلوماتية أو ملف معلوماتي تم تسليمه لدولة أجنبية أو وكلائها.

ج) يدمر أو يتيح تدمير معلومات، وثيقة، عملية، بيانات رقمية أو ملف معلوماتي بهدف تقديمها لقوة أجنبية.

الفصل الثالث: عن المخالفات الصحفية

المادة 106: عندما يقع الشخص في جريمة الصحافة، بما في ذلك التشهير والسب، تمجيد الجريمة، من خلال وسيلة الاتصالات الالكترونية، جريمة يعاقب عند إدانته لنفس العقوبات المنصوص عليها في جنح الصحافة بوسائل أخرى.

الفصل الرابع: مسؤولية الأشخاص الاعتبارية

المادة 107: إن الأشخاص الاعتبارية الأخرى غير الدولة والسلطات الإقليمية والمحلية والمؤسسات العامة هي المسؤولة عن الجرائم المرتكبة بموجب هذا القانون لصالحهم من قبل أي شخص، يتصرف إما بشكل فردي أو عضوا في هيئة الشخصية الاعتبارية، التي تمارس سلطة إدارية بداخلية قائمة على:

أ) سلطة تمثيل الشخصية الاعتبارية.

ب) سلطة تتخذ القرارات نيابة عن الشركة.

ج) سلطة لممارسة رقابة داخل الشخصية الاعتبارية.

prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein et qui est fondé sur :

a) un pouvoir de représentation de la personne morale ;
b) une autorité pour prendre des décisions au nom de la personne morale ;
c) une autorité pour exercer un contrôle au sein de la personne morale.

Article 108 : Outre les cas déjà prévus à l'article 106 ci-dessus, une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée audit article a rendu possible la commission des infractions prévues par la présente loi pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

Article 109 : La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 110 : Les peines encourues par les personnes morales sont :

a) l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;

b) la dissolution, lorsque la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq (5) ans, détournée de son objet pour commettre les faits incriminés ;

c) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

d) la fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à

المادة 108: بالإضافة إلى الحالات المنصوص عليها في المادة 106 أعلاه، يمكن تحميل شخصية إعتبارية مسؤولية فراغ الإشراف من قبل الشخصية الطبيعية المشار إليها في تلك المادة والتي تسببت في إمكانية وقوع الجرائم المنصوص عليها في هذا القانون نيابة عن شخصية إعتبارية تعمل تحت سلطتها.

المادة 109: إن مسؤولية الأشخاص الاعتبارية لا تستبعد مسؤولية الأشخاص الطبيعية أو المتواطئين في نفس الوقائع.

المادة 110: العقوبات التي تتكبدها الأشخاص الاعتبارية هي:

أ) الغرامة، حيث يبلغ الحد الأقصى منها معدل يساوي خمسة أضعاف ما تدفعه لأشخاص الطبيعية بموجب قانون معاقبة الجريمة؛

ب) الحل، عندما تم إنشاء الشخصية الاعتبارية، أو في حالة وجود جريمة أو مخالفة، تعاقب بخصوص الأشخاص الذين يعانون من حكم بالسجن لأكثر من خمسة (5) سنوات، فتم تحويلها عن الغرض المستخدمة من أجله لارتكاب الجريمة؛

ج) الحظر النهائي أو لمدة خمس (5) سنوات بممارسة مباشر أو غير مباشر أكثر من الأنشطة المهنية أو الاجتماعية؛

د) إغلاق بصورة دائمة أو لمدة خمس (5) سنوات لأكثر من مؤسسة تم استخدامها في ارتكاب وقائع الجريمة؛

ه) الابعاد من الصفقات العامة، إما بشكل دائم أو لفترة خمس (5) سنوات؛

و) فرض حظر دائم أو لمدة خمس (5) سنوات لجعل دعوى الاكتتاب مفتوحة للعمة.

ز) حظر لمدة خمس (5) سنوات لإصدار شيكات أخرى غير تلك التي تسمح لسحب الأموال من

commettre les faits incriminés ;

e) l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ;

f) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ;

g) l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;

h) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

i) l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique aux frais de la personne morale incriminée.

CHAPITRE V : DES DISPOSITIONS PARTICULIERES

Article 111 : Constitue une circonstance aggravante au sens de la présente loi l'utilisation des technologies de l'information et de la communication (TIC) en vue de commettre des infractions de droit commun, comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux ou la commission d'infractions en bande organisée.

Article 112 : Commet une infraction au sens de la présente loi toute personne qui porte atteinte aux biens d'autrui par l'utilisation des TIC, notamment aux données informatiques, par vol, escroquerie, recel, abus de confiance, extorsion de fonds, terrorisme, blanchiment d'argent, chantage.

Article 113 : Ne constitue pas une infraction au sens de la présente loi, l'utilisation des nouveaux supports immatériels à savoir les « données numérisées » ou les « fichiers informatisés » qui sont tenus secrets par les Etats dans l'intérêt de la sécurité et/ou de la défense nationale.

المسحوب عليه ببطاقات الدفع المعتمدة أو استخدام الدفع المباشر.

ح) مصادرة الشيء الذي كان يستخدم أو كان يهدف إلى ارتكاب الجريمة أو النتيجة؛

ط) عرض القرار الوارد أو نشر ذلك إما عن طريق الصحافة أو عن طريق أي وسيلة اتصال الى الجمهور عن طريق الوسائل الإلكترونية على حساب الشركة المخالفة.

الفصل الخامس: أحكام خاصة

المادة (111): يشكل ظرفا مشددا لأغراض هذا القانون، استخدام تكنولوجيا المعلومات والاتصالات لارتكاب جرائم عادية، مثل السرقة والغش والإخفاء، والاختلاس والابتزاز والإرهاب وغسل الأموال أو ارتكاب الجرائم من قبل عصابة منظمة.

المادة 112: يعتبر جريمة مرتكبة بموجب هذا القانون أي شخص ينتهك ممتلكات الآخرين من خلال استخدام تكنولوجيا المعلومات والاتصالات، بما في ذلك بيانات معلوماتية والسرقة والاحتيال والإخفاء والاختلاس والابتزاز والإرهاب وغسل الأموال والابتزاز.

المادة (113): لا يعتبر جريمة بموجب هذا القانون، استخدام وسائل الإعلام الحديثة مثل "البيانات الرقمية" أو "الملفات المعلوماتية" التي يتم الاحتفاظ بها سرا من قبل الدولة في مصلحة الأمن و / أو الدفاع الوطني.

TITRE V: DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRES INTERNATIONALES

CHAPITRE I : DE LA COOPERATION JUDICIAIRE INTERNATIONALE

Article 114 : Les autorités judiciaires nationales peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire tchadien ou dont l'un des auteurs ou complices se trouve sur ledit territoire. Sous réserve des règles de réciprocité entre le Tchad et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de Procédure Pénale.

Article 115 : A la demande d'un autre Etat membre de la CEMAC ou de la CEEAC, les autorités nationales compétentes pourront instruire les instances en charge de lutte contre la cybercriminalité afin de coopérer à la recherche et à la constatation de toutes les infractions pénales relatives aux systèmes informatiques, ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale.

Cette coopération est mise en œuvre dans le respect des instruments internationaux pertinents sur la coopération internationale en matière pénale.

CHAPITRE II: DE L'ENTRAIDE JUDICIAIRE INTERNATIONAE

Article 116 : A moins qu'une convention internationale à laquelle le Tchad est partie n'en dispose autrement, les demandes d'entraide émanant des autorités judiciaires tchadiennes et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère en charge des Affaires Etrangères. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

Les demandes d'entraide judiciaire émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires tchadiennes doivent être présentées par la voie diplomatique par le Gouvernement étranger intéressé.

الباب الخامس: التعاون والمساعدة القضائية الدولية

الفصل الأول: التعاون القضائي

المادة 114: يمكن للسلطان القضائية الوطنية أن تعطي تفويضا على المستوى الوطني والدولي على حد سواء، إلى أي شخص أو شركة للعثور على عناصر الجرائم الإلكتروني، حيث يتواجد أحد عناصرها على الأقل في الأراضي التشادية وحيث يتواجد أحد المتواطئين؛

تحت طائلة المعاملة بالمثل بين تشاد وغيرها من الدول الملزمة بموجب اتفاق التعاون القانوني، يتم تنفيذ التفويضات القضائية وفقا لأحكام قانون الإجراءات الجنائية.

المادة 115: بناء على طلب من دولة أخرى عضو في الجموعة النقدية لدول وسط إفريقيا، بإمكان السلطات الوطنية المختصة إيعاز الهيئات المسؤولة عن مكافحة الجرائم الإلكترونية في التعاون في مجال البحوث والاعتراف والإلمام بكل الجرائم الجنائية المتعلقة بالأنظمة المعلوماتية وجمع الأدلة في شكل الكتروني ذات علاقة بالمخالفة الجنائية.

ويتم تنفيذ هذا التعاون وفقا للإتفاقيات الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية.

الفصل الثاني: عن المساعدة القانونية

المادة 116: حينما لا تنص إتفاقية دولية للتعاون تشاد طرف فيها إجراءا مخالفا، ترسل طلبات المساعدة القضائية من السلطات القضائية التشادية إلى السلطات القضائية الأجنبية عبر وزارة العلاقات الخارجية الأجنبية؛ يتم إرجاع وثائق التنفيذ إلى الدولة الطالبة بنفس الطريقة.

يجب تقديم طلبات المساعدة القانونية الموجهة من السلطات القضائية الأجنبية إلى السلطات القضائية التشادية عبر القنوات الدبلوماسية من قبل الحكومة الأجنبية المهتمة.

Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

En cas d'urgence, les demandes d'entraide judiciaires émises par les autorités tchadiennes ou étrangères peuvent être transmises directement aux autorités de l'Etat requis pour leur exécution. Le renvoi des pièces d'exécution aux autorités compétentes de l'Etat requérant est effectué selon les mêmes modalités.

Sous réserve des conventions internationales, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires tchadiennes doivent faire l'objet d'un avis de la part du gouvernement étranger intéressé. Cet avis est transmis aux autorités judiciaires tchadiennes compétentes par voie diplomatique.

En cas d'urgence, les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises au Procureur de la République ou au Juge d'Instruction territorialement compétent.

Si le Procureur de la République reçoit directement d'une autorité étrangère, une demande d'entraide qui ne peut être exécutée que par le Juge d'Instruction, il la transmet pour exécution à ce dernier ou saisit le Procureur Général dans le cas prévu à l'article 117 ci-dessus.

Avant de procéder à l'exécution d'une demande d'entraide judiciaire dont il a été directement saisi, le Juge d'Instruction la communique immédiatement pour avis au Procureur de la République.

Article 117: Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées par le Procureur de la République ou par les officiers ou agents de Police Judiciaire requis à cette fin par ce magistrat.
Elles sont exécutées par le Juge d'Instruction ou par des officiers de Police Judiciaire agissant sur commission rogatoire de ce magistrat lorsqu'elles nécessitent certains actes de procédure qui ne peuvent être ordonnés ou exécutés qu'au cours d'une instruction préparatoire.

Article 118: Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées selon les règles de procédure prévues par le Code de Procédure Pénale.

يتم إرجاع الوثائق التنفيذية إلى سلطات الدولة الطالبة بنفس الطريقة.

في حالة الطوارئ، ترسل طلبات المساعدة القضائية التي تصدرها السلطات التشادية أو الأجنبية مباشرة إلى سلطات الدولة المعنية بتنفيذها. ترسل الوثائق التنفيذية إلى السلطات المختصة في الدولة الطالبة بنفس الشروط.

مع مراعاة الاتفاقيات الدولية، ينبغي أن تخضع طلبات المساعدة القضائية الصادرة من الدولة الأجنبية والموجهة إلى السلطات القضائية التشادية، لإذن من الحكومة الأجنبية المهتمة. ينتقل هذا الرأي إلى السلطات القضائية التشادية المختصة من خلال القنوات الدبلوماسية.

في حالات الطوارئ، ترسل طلبات المساعدة من السلطات القضائية الأجنبية إلى مدعي الجمهورية أو القاضي المختص إقليميا.

إذا تلقى مدعي الجمهورية مباشرة من سلطة أجنبية طلبا بالمساعدة لا يمكن أن يتم تنفيذه إلا من قبل قاضي التحقيق، ثم يحيله إلى النائب العام على النحو المنصوص عليه في المادة 117 أدناه.

قبل تنفيذ طلب المساعدة التي يتم إدخاله مباشرة، يقوم قاضي التحقيق بإبلاغ مدعي الجمهورية.

المادة 117: يتم تنفيذ طلبات المساعدة من السلطات القضائية الأجنبية من قبل مدعي الجمهورية أو من قبل ضباط أو الشرطة القضائية للقيام بذلك.
يتم تنفيذها من قبل قاضي التحقيق أو من قبل ضباط الشرطة القضائية متصرفا بموجب الصلاحيات المفوضة للقاضي عندما يتطلب بعض الإجراءات التي لا يمكن الأمر بها أو تطبيقها إلا في إجراء التحقيق الأولي.

المادة 118: يتم تنفيذ طلبات المساعدة من السلطات القضائية الأجنبية وفقا للقواعد الإجرائية المنصوص عليها في قانون الإجراءات الجنائية.
ومع ذلك، إذا أوضح طلب المساعدة، سيتم تنفيذه وفقا للقواعد الإجرائية المشار إليها صراحة من قبل

السلطات المختصة في الدولة الطالبة، دون أن يحد هذه القواعد من حقوق الأطراف أو الضمانات الإجرائية المنصوص عليها في مدونة الإجراءات الجنائية.

عندما لا يمكن تنفيذ طلب المساعدة وفقا لمتطلبات الدولة الطالبة، يجب على السلطات التشادية على الفور إخطار الدولة الطالبة مع بيان ظروف تنفيذ الطلب.

سوف يتفق السلطات التشادية المختصة وسلطات الدولة الطالبة في وقت لاحق على اتخاذ مزيد من الإجراءات للمطالبة، إن وجدت، مع مراعاة تحقيق تلك الشروط.

مخالفة نظام نقل طلب المساعدة لن يكون سببا لإبطال الأعمال المنجزة وفقا لهذا الطلب.

المادة 119: إذا كان تنفيذا طلب المساعدة من سلطة قضائية أجنبية من شأنه أن يقوض النظام العام أو المصالح الأساسية للأمة، يقوم مدعي الجمهورية بإخطار هذا الطلب، أو بإحالته إلى النائب العام، الذي يحيله إلى وزير العدل ويشعر مدعي الجمهورية. بعد إشعاره، يقوم وزير العدل بإبلاغ السلطة الطالبة، وعند الاقتضاء بناء على طلبها. يتم إبلاغ هذه المعلومات إلى الجهة القضائية المختصة ويعوق تنفيذ طلب المساعدة إلى حين عودة أجزاء مستندات التنفيذ.

الباب السادس: أحكام انتقالية وختامية

المادة 120: إن التصاريح وإشهار إستيراد تقنيات التشفير الصادرة عن السلطات المختصة تظل سارية المفعول حتى انتهاء الوقت المحدد المذكورة أعلاه.

Toutefois, si la demande d'entraide le précise, elle est exécutée selon les règles de procédure expressément indiquées par les autorités compétentes de l'Etat requérant, sans que ces règles ne réduisent les droits des parties ou les garanties procédurales prévues par le Code de Procédure Pénale.

Lorsque la demande d'entraide ne peut être exécutée conformément aux exigences de l'Etat requérant, les autorités compétentes tchadiennes en informent sans délai les autorités de l'Etat requérant et indiquent dans quelles conditions la demande pourrait être exécutée.

Les autorités tchadiennes compétentes et celles de l'Etat requérant peuvent ultérieurement s'accorder sur la suite à réserver à la demande, le cas échéant, en la subordonnant au respect desdites conditions.

L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Article 119: Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Procureur de la République saisi ou avisé de cette demande, la transmet au Procureur Général qui en saisit le Ministre chargé de la Justice et donne, le cas échéant, avis de cette transmission au Procureur de la République.

S'il est saisi, le Ministre chargé de la Justice informe l'autorité requérante, le cas échéant, de ce qu'il ne peut être donné suite, totalement ou partiellement, à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.

TITRE VI : DES DISPOSITIONS TRANSITOIRES ET FINALES

Article 120: Les autorisations et les déclarations d'importation, de fourniture et d'exportation de moyens de cryptographie délivrées par les autorités compétentes demeurent valables jusqu'à l'expiration du délai prévu par celles-ci.

Article 121 : En tant que de besoin, les autres conditions d'application de la présente loi seront précisées par voie réglementaire.

المادة 121: متى ما لزم الأمر، يتم تحديد الشروط الأخرى بالسبل التنظيمية.

Article 122 : La présente loi, sera enregistrée, publiée au Journal Officiel de la République et exécutée comme loi de l'Etat.

المادة 122: يسجل وينشر القانون الحالي في الجريدة الرسمية للجمهورية وينفذ باعتباره قانونا للدولة.

N'Djamena, le 10 Février 2015
أنجمينا بتاريخ

IDRISS DEBY ITNO
إدريس ديبي إتنو