Décrets-lois

Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication.

Le Président de la République,

Vu la Constitution,

Vu le décret Présidentiel n° 2021-117 du 22 septembre 2021, relatif aux mesures exceptionnelles,

Après délibération du Conseil des ministres.

Prend le décret-loi dont la teneur suit :

Chapitre premier

Dispositions générales

Article premier - Le présent décret-loi vise à fixer les dispositions ayant pour objectif la prévention des infractions se rapportant aux systèmes d'information et de communication et leur répression, ainsi que celles relatives à la collecte des preuves électroniques y afférentes et à soutenir l'effort international dans le domaine, et ce, dans le cadre des accords internationaux, régionaux et bilatéraux ratifiés par la République tunisienne.

Art. 2 - Les autorités publiques doivent, lors de l'application des dispositions du présent décret-loi, respecter les garanties constitutionnelles, les traités internationaux, régionaux et bilatéraux y afférents ratifiés par la République tunisienne, et la législation nationale en matière des droits de l'Homme, des libertés et de la protection des données à caractère personnel.

Art. 3 - Sont applicables aux infractions mentionnées au présent décret-loi, selon le cas, les dispositions du code pénal, du code de procédure pénale, du code de justice militaire ainsi que les textes pénaux spéciaux, sans préjudice de l'application des peines plus graves.

Les enfants sont soumis au code de la protection de l'enfant.

Art. 4 - Les services compétents des ministères de la défense nationale et de l'intérieur exécutent les ordonnances judiciaires relatives à l'accès aux systèmes d'information, données et informations stockées, chacun en ce qui le concerne.

Art. 5 - Aux sens du présent décret-loi, on entend par:

- **Système d'information** : un ensemble de logiciels, outils et équipements, isolés, interconnectés ou apparentés assurant les opérations de traitement automatisé des données.

- **Données informatiques** : toute présentation des faits, d'informations ou de concepts sous une forme qui se prête à un traitement automatisé, y compris les logiciels permettant à un système d'information d'exécuter une fonction précise.

- **Système de communication** : un ensemble de supports métalliques, optiques, radio ou tout autre technologie qui puisse assurer les opérations de transmission, d'émission ou de réception de signaux ou de données.

- **Fournisseur de services de communications** : toute personne physique ou morale fournissant un service de télécommunications au public y compris les services d'internet.

- **Flux de trafic ou données d'accès** : des données produites par un système d'information indiquant la source de la communication, sa destination, son itinéraire, son heure, sa date, son volume et sa durée ainsi que le type de service de communication.

- **Support informatique** : tout équipement ou moyen permettant le stockage des données informatiques.

- **Programme** : Ensemble de commandes et d'instructions à un ordinateur ou tout autre équipement pour le traitement de données ou l'exécution d'autres tâches.

- **L'effacement de données informatiques** : Tout acte qui conduit à empêcher l'accès aux données d'information accessibles.

Chapitre II

Des obligations et procédures spéciales

Section première - **De l'obligation de conservation**

Art. 6 - Les fournisseurs de services de télécommunications doivent conserver les données stockées dans un système d'information pendant une durée fixée par arrêté conjoint des ministres de la défense nationale, de l'intérieur, de la justice ainsi que du ministre chargé des télécommunications, et ce, selon la nature du service, à condition que cette période ne soit pas inférieure à deux ans à compter de la date d'enregistrement des données.

Les données qui doivent être conservées sont :

- les données permettant d'identifier les utilisateurs du service,

- les données relatives au flux de trafic,

- les données relatives aux terminaux de la communication.

- les données relatives à la localisation géographique de l'utilisateur.

- les données relatives à l'accès et à l'exploitation de contenu à valeur ajoutée protégé.

Section 2 - **De l'obligation de non-divulgation du secret professionnel**

Art. 7 - Il est interdit à tout chargé de l'exécution des ordonnances judiciaires relatives à l'accès aux données stockées au niveau du système d'information ou à la collecte de données du flux de trafic ou à l'interception de communications, ou celui auquel il est fait recours pour cette tâche, de divulguer le secret professionnel dans tout ce qui concerne les dispositions et les modalités appliquées ou les informations ou données dont ils ont eu connaissance lors de l'exécution de ces ordonnances judiciaires.

Est interdite toute divulgation orale ou écrite des faits et informations ou leur échange en dehors du cadre des missions techniques restreintes ainsi que le transfert de ces faits et informations, ou leur transmission à autrui ou leur mise à la disposition de ceux qui n'ont pas la qualité.

Le chargé de l'exécution des ordonnances judiciaires ou celui auquel il est fait recours pour cette tâche, demeure tenu à la non-divulgation du secret professionnel, lors de l'exercice de ses fonctions ou après cessation de ses fonctions de quelque manière que ce soit. L'interdiction de divulgation du secret professionnel ne peut être levée que sur ordonnance judiciaire.

Section 3 **- De la constatation des infractions et l'exécution des ordonnances d'interception et d'accès**

Art. 8 - Sont chargés de la constatation des infractions mentionnées dans le présent décret-loi, chacun dans la limite de ses compétences :

- Les procureurs de la République et leurs adjoints.

- Les officiers de la police judiciaire mentionnés aux numéros 3 et 4 de l'article 10 du code de procédure pénale, et les officiers de la police judiciaire militaire mentionnés aux numéros 3 et 4 de l'article 16 du code de justice militaire.

- Les agents relevant du ministère chargé des communications ayant reçu, en vertu de lois spéciales, l'autorité nécessaire pour enquêter sur certaines infractions ou en rédiger des rapports.

Art. 9 - Le procureur de la République, le juge d'instruction ou les officiers de la police judiciaire autorisés par écrit, sont habilités à ordonner :

- De leur fournir les données informatiques stockées dans un système ou support informatique ou celles relatives au trafic des télécommunications ou à leurs utilisateurs, ou autres données pouvant aider à révéler la vérité.

- De saisir un système d'information en totalité ou en partie ou un support informatique y compris les données stockées pouvant aider à révéler la vérité. Si la saisie du système d'information s'avère non nécessaire ou impossible à réaliser, les données en relation avec l'infraction ainsi que celles permettant leur lecture et leur compréhension seront copiées sur un support informatique de manière à assurer l'authenticité et l'intégrité de leur contenu.

- De collecter ou enregistrer en temps réel les données relatives au trafic des télécommunications par l'usage des moyens techniques appropriés.

Ils sont aussi habilités à accéder directement ou avec l'assistance des experts à tout système ou support informatique et procéder à une investigation afin d'obtenir les données stockées pouvant aider à révéler la vérité.

Les services compétents du ministère de la défense nationale et du ministère de l'intérieur assurent l'opération de saisie, sa localisation et le processus d'accès aux systèmes d'information, aux données, aux informations stockées, aux logiciels et à tous ces supports relatifs aux deux ministères, chacun selon son domaine de compétence.

Art. 10 - Dans les cas où la nécessité de l'enquête l'exige, le procureur de la République ou le juge d'instruction peut recourir à l'interception des communications des suspects, en vertu d'une décision écrite et motivée. Dans les mêmes cas, sur rapport motivé de l'officier de police judiciaire habilité à constater les infractions, l'interception des communications des suspects peut également avoir lieu, et ce, en vertu d'une décision écrite et motivée du procureur de la République ou du juge d'instruction.

L'interception des communications comprend l'obtention des données d'accès, l'écoute, ou l'accès au leur contenu, leur reproduction, leur enregistrement à l'aide des moyens techniques appropriés et en recourant, en cas de besoin, aux structures compétentes, chacun selon le type de prestation de service qu'il fournit.

Les données d'accès sont les données qui permettent d'identifier le type de service, la source de la communication, sa destination, son réseau de transmission, l'heure, la date, le volume et la durée de la communication.

Art. 11 - Dans le cadre de leurs obligations d'assurer les exigences de la sureté publique, de la défense nationale et les dispositions du pouvoir judiciaire, les fournisseurs de services de communication, doivent répondre aux demandes des services chargés de la réception et de l'exécution des ordonnances judiciaires relatifs à l'accès aux données stockées dans un système d'information ou à la collecte de données du flux des communication ou de leur interception liées à l'accomplissement de leurs tâches.

L'autorité chargée de l'exécution des ordonnances judiciaires est tenue de rédiger un procès-verbal des opérations d'accès ou de collecte ou d'interception ou de traitement qu'elle a réalisé. Ce procès-verbal doit obligatoirement comporter les indications suivantes:

- Le dispositif de l'ordonnance dont elle est chargée de son exécution.

- L'autorité qui a ordonné le traitement technique.

- Les dispositions techniques qu'elle a pris afin d'exécuter l'ordonnance et le type d'assistance qu'elle a eu des fournisseurs de services.

- Les mesures techniques prises pour conserver les données collectées et assurer leur authenticité et leur intégrité dans toutes les étapes.

- La date et l'heure du début et de la fin des opérations.

Le procès-verbal doit être accompagné par les résultats des opérations d'accès, de collecte, d'interception ou de traitement aussi bien que par les programmes et les données techniques nécessaires qui assurent leur conservation et leur exploitation sans atteinte à leur authenticité et leur intégrité.

Section 4 - **De la collecte des preuves électroniques**

Art. 12 - L'autorité chargée de l'exécution des ordonnances judiciaires doit tenir un registre interne coté et paraphé, comprenant l'identité des agents qui lui sont rattachés et qui interviennent dans les opérations d'accès, de collecte, d'interception et de traitement, leurs qualités et leurs signatures, au cas par cas.

Art. 13 - Les résultats des opérations d'accès, de collecte ou d'interception et les données techniques annexées, sont transférées aux autorités intéressées identifiées dans l'ordonnance judiciaire y affèrent, et ce, en vue de leur exploitation.

Art. 14 - Il en est fait inventaire, autant que possible, en présence du prévenu, ou de celui en possession duquel se trouve le saisie. Un rapport de saisi est rédigé.

Les objets saisis sont conservés, selon leur nature et leurs caractéristiques, dans des supports ou des conteneurs qui assurent leur sécurité et sur lesquels doit être noter les données relatives à la date et l'heure de la saisie, et le numéro du procès-verbal ou de l'affaire.

Les précautions nécessaires sont prises, pour maintenir l'authenticité et l'intégrité du saisie, y compris les moyens techniques pour protéger leur contenu.

Art. 15 - En cas d'impossibilité de saisie effective d'un système informatique soumis à la souveraineté de l'Etat tunisien, il est tenu, aux fins de conserver les preuves de l'infraction, d'utiliser tous les moyens appropriés afin de prévenir l'atteinte ou l'accès aux données stockées.

Chapitre III

Des infractions se rapportant aux systèmes d'information et de communication et des peines encourues

Section première - **De la violation de l'intégrité des systèmes d'informations et des données et de leur confidentialité**

Art. 16 - Est puni de trois mois jusqu'à un an d'emprisonnement et d'une amende de dix mille dinars, quiconque sciemment accède ou demeure illégalement dans un système informatique en totalité ou en partie.

Est passible de la même peine encourue, quiconque sciemment dépasse les limites du droit d'accès qui lui est accordé.

La tentative est punissable.

Art. 17 - Est puni de trois ans d'emprisonnement et d'une amende de vingt mille dinars, quiconque sciemment produit, vend, importe, distribue, approvisionne, expose, obtient pour usage ou possède ce qui suit, et ce illégalement ou en dehors des cas où la nécessité de la recherche scientifique ou la sécurité informatique l'exige :

- Un équipement ou un programme informatique conçu ou apprivoisé pour commettre les infractions régies par le présent décret-loi.

- Un mot de passe, un code d'accès ou toutes données informatiques similaires permettant d'accéder, en totalité ou en partie, à un système d'informations en vue de commettre les infractions régies par le présent décret-loi.

La tentative est punissable.

Art. 18 - Est puni de trois ans d'emprisonnement et d'une amende de vingt mille dinars, quiconque utilise sciemment, et sans droit, des moyens techniques pour l'interception de données de communication dans un envoi non destiné au public à l'intérieur, à partir ou vers un système d'informations y compris les rayonnements latéraux émis par le système et transportant des données de communication.

L'interception comprend l'obtention de données relatives aux flux de trafic ou de leur contenu, aussi de les copier ou les enregistrer.

La tentative est punissable.

Art. 19 - Est puni de trois ans d'emprisonnement et d'une amende de vingt mille dinars, quiconque endommage, modifie, supprime, annule ou détruit sciemment des données informatiques.

La tentative est punissable.

Art. 20 - Est puni de trois ans d'emprisonnement et d'une amende de trente mille dinars, quiconque entrave sciemment et d'une manière illégale le fonctionnement d'un système informatique, en y introduisant des données informatiques ou les envoyées, les endommagées, les modifiées, les supprimées, les annulées, les détruire, ou en y utilisant d'autres moyen électronique.

La tentative est punissable.

Art. 21 - Est puni de cinq ans d'emprisonnement et d'une amende de trente mille dinars, quiconque aura délibérément détourné des données informatiques appartenant à autrui.

La tentative est punissable.

Section 2 - **Des infractions commises à l'aide de systèmes d'information ou de données informatiques**

Sous-section première - **De la fraude informatique**

Art. 22 - Est puni de six ans d'emprisonnement et d'une amende de cent mille dinars quiconque cause intentionnellement un préjudice patrimonial à autrui par introduction, altération, effacement ou suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention d'obtenir un bénéfice financier ou économique pour soi-même ou pour autrui.

Sous-section 2 - **De la falsification informatique**

Art. 23 - Est puni de cinq ans d'emprisonnement et d'une amende de cent mille dinars quiconque commis une falsification pouvant causer un préjudice par l'introduction, l'altération, l'effacement ou la suppression de données informatiques, engendrant la production des données non authentiques, dans l'intention de l'exploiter comme si elles étaient authentiques.

Sous-section 3 - **Des rumeurs et fausses nouvelles**

Art. 24 - Est puni de cinq ans d'emprisonnement et d'une amende de cinquante mille dinars quiconque utilise sciemment des systèmes et réseaux d'information et de communication en vue de produire, répandre, diffuser, ou envoyer, ou rédiger de fausses nouvelles, de fausses données, des rumeurs, des documents faux ou falsifiés ou faussement attribués à autrui dans le but de porter atteinte aux droits d'autrui ou porter préjudice à la sureté publique ou à la défense nationale ou de semer la terreur parmi la population.

Est passible des mêmes peines encourues au premier alinéa toute personne qui procède à l'utilisation de systèmes d'information en vue de publier ou de diffuser des nouvelles ou des documents faux ou falsifiés ou des informations contenant des données à caractère personnel, ou attribution de données infondées visant à diffamer les autres, de porter atteinte à leur réputation, de leur nuire financièrement ou moralement, d'inciter à des agressions contre eux ou d'inciter au discours de haine.

Les peines prévues sont portées au double si la personne visée est un agent public ou assimilé.

Sous-section 4 - **De l'accès illégal aux contenus protégés**

Art. 25 - Sous réserve des peines prévues par des textes spéciaux, est puni d'un mois à un an d'emprisonnement et d'une amende de cinquante mille dinars, ou de l'une des deux peines, quiconque utilise intentionnellement des systèmes d'informations et de communication pour violer les droits d'auteur et les droits voisins sans obtenir une autorisation de ou des ayants droit dans le but d'en tirer profit ou de porter préjudice à l'économie ou aux droits d'autrui.

Section 3 - **De l'exploitation des enfants et agressions corporelles**

Art. 26 - Sous réserve des législations spécifiques, est puni d'une peine d'emprisonnement de six ans et une amende de cinquante mille dinars, quiconque produit, affiche, fournit, publie, envoie, obtient ou détient intentionnellement des données informatiques à contenu pornographique montrant un enfant ou une personne ayant l'apparence d'un enfant s'adonnant à des pratiques sexuelles explicites ou suggestives ou en être victime.

Est passible des mêmes peines prévues par le premier alinéa du présent article, quiconque aura utilisé intentionnellement des systèmes d'information pour publier ou diffuser des images ou des séquences vidéo d'agressions physiques ou sexuelles sur autrui.

Section 4 - **De la répression du manquement aux obligations de la collecte des preuves électroniques**

Art. 27 - Est puni d'un an d'emprisonnement et d'une amende de dix mille dinars, ou de l'une de ces deux peines, le fournisseur de services qui ne respecte pas l'obligation de conservation qui lui incombe en vertu des dispositions de l'article 6 du présent décret-loi.

Art. 28 - Sous réserve des dispositions de l'article 32 du code pénal, est passible d'un an d'emprisonnement et d'une amende de dix mille dinars, quiconque entrave sciemment le déroulement de l'investigation, en refusant de remettre des données informatiques ou les moyens à y accéder pour lire ou comprendre les données saisies, ou qui les détruit ou les cache délibérément avant leur confiscation.

Art. 29 - Est puni de trois ans d'emprisonnement et d'une amende de vingt mille dinars, quiconque aura intentionnellement, et de quelque manière que ce soit, violé la confidentialité des procédures se rapportant à la collecte, à l'interception ou à l'enregistrement des données du flux de trafic ou de son contenu, ou à la divulgation des données obtenues ou à leur utilisation illicite.

Art. 30 - Est puni de trois ans d'emprisonnement et d'une amende de dix mille dinars, quiconque aura intentionnellement accédé à des données stockées dans un système d'information, collecté des données sur le flux de trafic ou intercepté le contenu des communications, les copiés ou les enregistrés dans des cas autres que ceux autorisés par le présent décret-loi ou sans respect des obligations légales.

La tentative est punissable.

Art. 31 - Est puni de six mois d'emprisonnement et d'une amende de vingt mille dinars, tout agent chargé de l'exécution des ordonnances judiciaires relatives à l'accès aux données stockées dans un système d'information, à la collecte des données du flux de trafic, ou à l'interception des communications, qui ne respecte pas l'obligation de la non-divulgation du secret professionnels prévue à l'article 7 du présent décret-loi.

La tentative est punissable.

La peine est portée à cinq ans d'emprisonnement et à trente mille dinars d'amende si l'agent occupe un emploi fonctionnel.

La peine est portée à dix ans d'emprisonnement et à cinquante mille dinars d'amende si le manquement à l'obligation de la non-divulgation du secret professionnel entraîne une atteinte grave à la sécurité nationale ou à l'ordre public, ou une menace à l'intégrité physique des personnes.

Section 5 - **De la responsabilité pénale des personnes morales et leurs dirigeants**

Art. 32 - Les sanctions pécuniaires prévues par le présent décret-loi s'appliquent aux personnes morales s'il s'avère que les infractions ont été commises à leur profit, qu'elles en ont obtenu des revenus ou qu'elles représentaient le but de leur création.

La sanction sera une amende cinq fois égale à la valeur de l'amende encourue pour les personnes physiques.

La juridiction peut également ordonner la privation de la personne morale d'exercer ses activités pour une durée maximale de cinq ans, ou ordonner sa dissolution.

Cela n'empêche pas d'infliger des sanctions prévues par le présent décret-loi aux représentants ou gérants des personnes morales dont il est prouvé qu'ils sont personnellement responsables des actes punissables.

Section 6 - **De l'allègement des peines**

Art. 33 - La juridiction peut prononcer la moitié des peines pour les infractions prévues par le présent décret-loi dans les cas suivants:

- Si l'âge de l'auteur de l'infraction est supérieur à dix-huit ans et inférieur à vingt ans.

- Si l'infraction n'a pas causé de dommages au système d'informations ou aux données informatiques.

- Si l'auteur de l'infraction informe les autorités compétentes des renseignements ou informations qui ont permis de découvrir d'autres infractions prévues par le présent décret-loi et d'éviter leur exécution ou survenance.

Chapitre IV

De l'appui à l'effort international de lutte contre les infractions se rapportant aux systèmes d'information et de communication

Art. 34 - Sous réserve des conventions internationales ou bilatérales ratifiées par la République tunisienne, les juridictions tunisiennes compétentes peuvent poursuivre et juger quiconque ayant commis, en dehors du territoire tunisien, une des infractions prévues par le présent décret-loi, et ce, dans les cas suivants :

- Si l'infraction est commise par un citoyen tunisien,

- Si l'infraction est commise contre des parties ou des intérêts tunisiens,

- Si l'infraction est commise contre des personnes ou d'intérêts étrangers par un étranger ou un apatride dont la résidence habituelle est sur le territoire tunisien, ou par un étranger ou un apatride se trouvant sur le territoire tunisien et ne répondant pas aux conditions légales d'extradition.

L'extradition aura lieu selon les procédures en vigueur conformément au code de procédure pénale, en tenant compte des conventions conclus à cet effet.

Art. 35 - Les autorités spécialisées veillent à faciliter la coopération avec leurs homologues dans les pays étrangers dans le cadre des conventions internationales, régionales et bilatérales ratifiées, et selon le principe de réciprocité à travers l'échange d'informations et de données avec la précision et la rapidité requises, en vue d'assurer l'avertissement précoce des infractions se rapportant aux systèmes d'informations et de communication, d'en prévenir, éviter leur perpétration, aider à en enquêter et poursuivre leurs auteurs.

La coopération prévue dans le premier alinéa du présent article, est tributaire de l'étendu de l'engagement de l'Etat étranger intéressé pour la conservation de la confidentialité des informations qui y sont transmises et de son engagement de ne pas les transmettre à une tierce partie ou les exploiter pour des fins autres que la lutte contre les infractions régies par le présent décret-loi et leur répression.

Chapitre V

Dispositions diverses

Art. 36 - Il est ajouté un nouveau tiret au deuxième paragraphe de l'article 15 bis du code pénal inséré immédiatement après le dernier tiret intitulé « Les infractions militaires », intitulé « Infractions se rapportant aux systèmes d'information et de communication» comme suit :

«- Les infractions se rapportant aux systèmes d'information et de communication :

* L'accès illégal.

* L'interception illégale.

* Le détournement de données informatiques.

* Endommagement, altération, effacement, suppression ou destruction de données informatiques.

* Utiliser du matériel, des logiciels ou des données pour commettre une infraction se rapportant au système d'information et de communication. »

Art. 37 - Sont abrogées les dispositions des articles 199 bis et 199 ter du code pénal.

Art. 38 - Le présent décret-loi sera publié au Journal officiel de la République tunisienne.

Tunis, le 13 septembre 2022.

Le Président de la République

Kaïs Saïed