EUROPEAID/140677/DH/SER/TN

Instrument européen de voisinage

Assistance Technique pour le programme MediaUp2 (Tunisie)

Pamt2

PROGRAMME D'APPUI AUX MÉDIAS TUNISIENS

Analyse juridique du Décret-loi n° 2022-54 du 13 septembre 2022

Janvier 2023

Un projet financé par l'Union européenne

Mis en œuvre par CFI et ses partenaires

Cette analyse juridique a été réalisée par ARTICLE 19.

Avertissement

Le contenu de ce rapport relève de la seule responsabilité de ses auteurs et ne peut en aucune manière être considéré comme reflétant les vues de l'Union européenne.

Résumé exécutif

Cette analyse juridique du Décret-loi n° 2022-54 du 13 septembre 2022[1] (ci-après le Décret-loi) examine sa conformité avec les normes internationales relatives aux droits humains et à la liberté d'expression.

À l'heure actuelle, il n'existe pas de traité international sur la cybercriminalité, mais des négociations sont en cours au niveau des Nations Unies. Cependant, dans ce rapport sur le Décret-loi, nous comparons ses dispositions avec celles de la Convention sur la cybercriminalité du Conseil de l'Europe de 2001 (ci-après la Convention sur la cybercriminalité) – la norme régionale la plus pertinente en la matière. Lorsque cela est utile, des références à des législations nationales comparatives sont fournies.

Si certaines dispositions du Décret-loi semblent avoir été tirées en partie de la Convention sur la cybercriminalité, la plupart d'entre elles ne respectent pas les normes internationales relatives aux droits humains (et contreviennent aux protections des droits humains dans la Constitution tunisienne), ont un déficit de protections en matière de procédure régulière et ne respectent pas les principes de nécessité et proportionnalité.

- **Le Décret-loi est incompatible avec le principe de prévisibilité juridique.** La plupart des infractions visées par le Décret-loi sont passibles de peines de prison. Le principe de prévisibilité juridique exige que les peines pouvant aller jusqu'à l'emprisonnement soient régies par le Code pénal lui-même. Les personnes assujetties à la loi règlent leur conduite avec certitude, ce qui nécessite qu'elles trouvent facilement toute disposition pénale imposant des peines d'emprisonnement.

- **De nombreuses infractions prévues par le Décret-loi sont déjà sanctionnées dans d'autres textes juridiques.** Les crimes mentionnés dans le Décret-loi tels que la diffamation, la diffusion des images d'abus sexuels d'enfants et le discours de haine sont déjà sanctionnés dans d'autres textes juridiques, à savoir le Code pénal, le Décret-loi n° 115 de 2011 relatif à la liberté de la presse, de l'imprimerie et de l'édition (ci-après le Décret-loi n° 115 de 2011) ou le Code des télécommunications, avec différentes peines applicables à ce qui correspond effectivement aux mêmes délits. Cela n'est pas conforme au principe de sécurité juridique et accroît la possibilité d'une application arbitraire de ces dispositions.

- **Plusieurs dispositions criminalisent l'expression en ligne protégée plutôt que la cybercriminalité.** Le Décret-loi contient des dispositions, telles que la diffusion de fausses nouvelles, qui ne sont pas conformes aux normes internationales relatives à la liberté d'expression. Pour un certain nombre d'infractions, le Décret-loi risque d'être

[1] 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.

utilisé pour poursuivre des journalistes, des défenseurs des droits humains, des détracteurs du gouvernement et des chercheurs en sécurité. De nombreuses dispositions contiennent des termes trop vagues et trop larges, ce qui accroît la probabilité qu'elles soient appliquées de façon arbitraire. D'un point de vue comparatif, le Décret-loi introduit plusieurs infractions qui n'existent pas dans des instruments comme la Convention sur la cybercriminalité. Les infractions prévues dans le Décret-loi vont donc au-delà des infractions reconnues internationalement comme constituant des cybercrimes.

- **Les sanctions prévues dans le Décret-loi sont excessives et disproportionnées.** Le régime des peines prévu par le Décret-loi est excessivement sévère, y compris pour les infractions liées au contenu. Le droit international relatif aux droits humains ne permet une peine de prison que pour les pires délits d'expression, comme l'incitation au génocide.

- **Le Décret-loi accorde aux autorités tunisiennes des pouvoirs d'investigation étendus et ne prévoit pas de garanties procédurales pour la protection des droits humains.** Le Décret-loi impose la conservation générale et systématique des données par les fournisseurs de services de télécommunications et accorde aux autorités gouvernementales des pouvoirs d'accès et d'interception trop étendus. Des garanties procédurales et des protections des droits humains comme le droit d'être informé des mesures de surveillance et un droit de recours sont totalement absentes du Décret-loi, malgré une référence générale aux engagements en matière de droits humains dans son Article 2.

Table des matières

Introduction 6
Normes internationales relatives aux droits humains 7
La protection de la liberté d'expression en droit international 7
Restrictions du droit à la liberté d'expression 8
Interdiction de l'incitation à la discrimination, à l'hostilité et à la violence 9
Réglementation du contenu en ligne 9
Surveillance des communications 10
Anonymat et chiffrement 11
Cybercriminalité 13
Analyse du Décret-loi 14
Le caractère provisoire du Décret-loi 14
Le principe de prévisibilité juridique 14
Définitions 15
Infractions se rapportant au contenu 16
Diffusion de fausses informations 16
Diffamation, incitation à l'agression et incitation au discours de haine 18
Expression ciblant des représentants publics 20
Exploitation des enfants et agressions corporelles 20
Violation du droit d'auteur 21
Autres délits de cybercriminalité 22
Accès illégal 22
Utilisation abusive des équipements 23
Interception illégale et ingérence dans les données 24
Entrave du fonctionnement d'un système et détournement des données 24
Fraude et falsification informatiques 24
Procédures et enquêtes 24
Obligation de conservation et accès aux données par les forces de l'ordre 25
Interception des communications 27
Protection inadéquate des sources journalistiques 27
Sanctions pour manquement aux obligations de la collecte de preuves électroniques 28
Juridiction extraterritoriale et coopération internationale 29

Introduction

L'objectif déclaré du Décret-loi n° 2022-54 du 13 septembre 2022 (ci-après le Décret-loi)[2] est de « 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 de soutenir l'effort international dans le domaine, et ce, dans le cadre des accords internationaux régionaux et bilatéraux ratifiés par la République tunisienne ».[3]

Le Décret-loi est apparu pour la première fois en 2015 dans une version fuitée, suscitant une large opposition au sein de la société civile tunisienne.[4] Malgré cette opposition, le gouvernement tunisien a approuvé le projet le 1er juin 2018. Toutefois, pour des raisons qui ne sont pas publiques, le texte n'a pas été soumis à l'Assemblée des représentants du peuple. Le Décret-loi reprend la majorité des dispositions de la version 2018 du texte et ajoute de nouvelles infractions pénales.

Après le second tour des élections législatives qui se déroulera début 2023, le Décret-loi sera soumis à l'approbation de l'Assemblée des représentants du peuple nouvellement constituée.[5]

[2] 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.
[3] Voir Article 1 du Décret-loi.
[4] Voir Projet de loi relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication. Voir aussi Committee to Protect Journalists, En Tunisie, la liberté de la presse s'érode sur fond de craintes pour la sécurité, 27 octobre 2015.
[5] Voir Article 80 de la Constitution tunisienne.

Normes internationales relatives aux droits humains

La protection de la liberté d'expression en droit international

Le droit à la liberté d'expression est protégé par plusieurs instruments internationaux des droits humains contraignants pour les États, y compris la Tunisie, en particulier dans l'Article 19 de la Déclaration universelle des droits de l'homme (DUDH)[6] et l'Article 19 du Pacte international relatif aux droits civils et politiques (PIDCP).[7] La liberté d'expression est également protégée par l'Article 37 de la Constitution tunisienne. En outre, l'Article 38 de la Constitution tunisienne garantit le droit à l'information et le droit d'accès à l'information.

L'Observation générale n° 34,[8] adoptée par le Comité des droits de l'homme des Nations Unies (CDH) en septembre 2011, reconnaît explicitement que l'Article 19 du PIDCP protège toutes les formes d'expression et les moyens de les diffuser, y compris tous les modes d'expression électroniques et basés sur Internet.[9] Autrement dit, la protection de la liberté d'expression s'applique en ligne de la même manière qu'elle s'applique hors ligne. Les États parties au PIDCP sont également tenus d'examiner la mesure dans laquelle les évolutions des technologies de l'information, comme Internet et les systèmes électroniques de diffusion de l'information basés sur la téléphonie mobile, ont profondément modifié les pratiques de communication dans le monde.[10] Le cadre juridique régissant les médias de masse devrait tenir compte des différences entre la presse écrite et les médias audiovisuels et l'Internet, tout en notant aussi la façon dont les médias convergent.[11]

De la même manière, les quatre mandataires spéciaux pour la protection de la liberté d'expression ont souligné dans leur Déclaration conjointe sur la liberté d'expression et Internet de juin 2011 que les approches réglementaires dans les secteurs des télécommunications et de l'audiovisuel ne peuvent pas être simplement transférées à l'Internet.[12] En particulier, ils recommandent d'élaborer des approches sur mesure pour répondre aux contenus illégaux en ligne, tout en soulignant que des restrictions spécifiques des contenus diffusés sur l'Internet ne sont pas nécessaires. Ils promeuvent également le recours à l'autorégulation en tant qu'instrument efficace pour lutter contre les contenus nocifs.

[6] Résolution 217A(III) de l'Assemblée générale des Nations Unies, adoptée le 10 décembre 1948.
[7] Résolution 2200A (XXI) de l'Assemblée générale des Nations Unies, 21 UN GAOR Supp. (No. 16) à 52, UN Doc.
[8] Comité des droits de l'homme des Nations Unies (CDH), Observation générale n° 34, Article 19, Liberté d'opinion et liberté d'expression, 12 septembre 2011, CCPR/C/GC/34.
[9] *Ibid*, par. 12.
[10] *Ibid*, par. 17.
[11] *Ibid*, par. 39.
[12] Déclaration conjointe sur la liberté d'expression et Internet, juin 2011.

En tant qu'État partie au PIDCP, la Tunisie doit veiller à ce que toutes ses lois visant à réglementer les modes d'expression électroniques et basés sur Internet soient conformes à l'Article 19 du PIDCP tel qu'interprété par le Comité des droits de l'homme et qu'elles soient conformes aux recommandations des mandataires spéciaux.

Restrictions du droit à la liberté d'expression

Le droit à la liberté d'expression n'est pas garanti en termes absolus, mais les restrictions au droit à la liberté d'expression et à la liberté de l'information doivent être strictement et étroitement définies et ne pas compromettre le droit lui-même.

Afin de déterminer si une restriction est correctement définie, en vertu de l'Article 19(3) du PIDCP, un test en trois parties est utilisé pour évaluer si une telle limitation est justifiée. Les restrictions doivent :

- **Être prescrites par la loi** : cela signifie qu'une norme doit être formulée avec suffisamment de précision pour permettre à un individu d'adapter sa conduite en conséquence.[13] Les restrictions ambiguës, floues ou trop étendues de la liberté d'expression sont donc inadmissibles ;

- **Poursuivre un objectif légitime :** les objectifs sont énumérés exhaustivement à l'Article 19(3)(a) et (b) du PIDCP, notamment le respect des droits et de la réputation d'autrui, la protection de la sécurité nationale, de l'ordre public, ou de la santé et de la moralité publiques ;

- **Être nécessaires et proportionnées** : Le critère de nécessité exige qu'il y ait un besoin social impérieux justifiant la restriction. La partie qui invoque la restriction doit démontrer un lien direct et immédiat entre l'expression et l'intérêt protégé. La proportionnalité exige qu'une restriction de l'expression ne soit pas trop large et qu'elle soit appropriée pour remplir sa fonction protectrice. Il doit être démontré que la restriction est spécifique et individuelle pour atteindre ce résultat protecteur et qu'elle n'est pas plus intrusive que d'autres instruments capables d'atteindre le même résultat limité.[14]

Les mêmes principes s'appliquent aux formes électroniques de communication ou d'expression diffusées sur Internet.[15]

L'Article 55 de la Constitution tunisienne prévoit également que les restrictions à la liberté d'expression doivent être prévues par la loi, poursuivre un but légitime, être justifiées par leurs objectifs et être proportionnelles à leurs justifications.

[13] Comité DH, *L.J.M de Groot c. Les Pays-Bas,* n° 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[14] Comité DH, *Velichkin c. Biélorussie*, n° 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[15] Observation générale n° 34, *op.cit.*, par. 43.

Interdiction de l'incitation à la discrimination, à l'hostilité et à la violence

Il est également important de noter que l'Article 20(2) du PIDCP dispose que tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence doit être interdit par la loi. Dans le même temps, l'incitation à la violence ne se limite pas à l'expression d'opinions que les individus désapprouvent ou trouvent offensantes.[16] C'est un discours qui encourage ou sollicite d'autres personnes à s'engager dans la violence par une rhétorique fortement discriminatoire. Au niveau international, les Nations Unies ont élaboré le Plan d'action de Rabat, un processus multipartite interrégional impliquant des organes des droits de l'homme des Nations Unies, des ONG et des universités, qui fournit la définition la plus proche de ce qui constitue une incitation en vertu de l'Article 20(2) du PIDCP[17].

Réglementation du contenu en ligne

Les principes énoncés ci-dessus ont été approuvés et expliqués plus en détail par le Rapporteur spécial des Nations Unies pour la promotion et la protection du droit à la liberté d'opinion et d'expression (Rapporteur spécial sur la liberté d'expression) dans deux rapports en 2011.[18]

Le Rapporteur spécial sur la liberté d'expression a notamment clarifié l'étendue des restrictions légitimes de différents types d'expression en ligne.[19] Il identifie également trois modes d'expression :

- L'expression qui constitue une infraction au regard du droit international et qui est passible de poursuites pénales ;
- L'expression qui n'est pas passible de poursuites pénales, mais qui devrait faire l'objet de restrictions et de poursuites au civil ; et
- L'expression qui n'est pas passible ni de sanctions pénales ni de sanctions civiles, mais qui suscite néanmoins des préoccupations en termes de tolérance, de civilité et de respect d'autrui.[20]

En particulier, le Rapporteur spécial sur la liberté d'expression a précisé que les seuls modes d'expression exceptionnels que les États sont tenus d'interdire en vertu du droit international sont :

- La pornographie mettant en scène des enfants[21] ;

[16] *C.f.* Cour européenne des droits de l'homme, *Handyside c. le Royaume-Uni*, 6 juillet 1976, par. 56.
[17] Voir Plan d'action de Rabat (2012). En particulier, il précise qu'il convient de tenir compte d'un « examen de seuil comportant six étapes » pour déterminer si le discours doit être pénalisé par les États en tant qu'incitation.
[18] Rapports du Rapporteur spécial des Nations Unies sur la liberté d'expression, A/HRC/17/27, 17 mai 2011, et A/66/290, 10 août 2011.
[19] *Ibid*, par. 18.
[20] *Ibid.*
[21] Il est recommandé d'utiliser les termes « images d'abus sexuels d'enfants » pour refléter la nature non

- L'incitation directe et publique à commettre le génocide ;
- L'apologie de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence ; et
- L'incitation au terrorisme.[22]

Il a en outre précisé que même la législation criminalisant ces types d'expression doit être suffisamment précise et qu'il doit y avoir des garanties adéquates et efficaces contre les abus, y compris la surveillance et l'examen par un tribunal ou un organisme de réglementation indépendant et impartial.[23] En d'autres termes, ces lois doivent aussi se conformer au test en trois parties, mentionné précédemment. Par exemple, la législation interdisant la diffusion des images d'abus sexuels d'enfants sur Internet à travers l'utilisation de technologies de blocage et de filtrage n'échappe pas à ces obligations.

Surveillance des communications

Le droit à la vie privée complète et renforce le droit à la liberté d'expression. Le droit au respect de la vie privée est essentiel pour garantir que les individus peuvent s'exprimer librement, y compris de manière anonyme,[24] s'ils le souhaitent. La surveillance massive des communications en ligne pose donc des problèmes importants tant au regard du droit à la vie privée que du droit à la liberté d'expression.

Le droit aux communications privées est fortement protégé par le droit international à travers l'Article 17 du PIDCP qui, entre autres, stipule que nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance. Dans l'Observation générale n° 16 sur le droit à la vie privée,[25] le Comité des droits de l'homme a clarifié que le terme « illégal » signifie qu'aucune immixtion ne peut avoir lieu sauf dans les cas envisagés par la loi. Les immixtions autorisées par les États ne peuvent avoir lieu qu'en vertu d'une loi, qui doit être elle-même conforme aux dispositions, aux buts et aux objectifs du PIDCP. Le Comité déclare ensuite :

> [M]ême pour ce qui est des immixtions qui sont conformes au Pacte, une loi pertinente doit préciser dans le détail les cas précis dans lesquelles elles peuvent être autorisées. La décision de procéder à ces immixtions autorisées doit être prise par l'autorité désignée par la loi, et cas par cas.[26]

Le Rapporteur spécial pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme a soutenu que, comme les

---

consensuelle et illégale du contenu. Des termes tels que la « pédopornographie » ou la « pornographie enfantine » ne sont plus acceptable puisque les enfants ne peuvent pas consentir à leur propre abus.

[22] Rapport du Rapporteur spécial sur la liberté d'expression, A/66/290, 10 août 2011, par. 81.

[23] *Ibid*, par. 22.

[24] *Ibid*, par. 84.

[25] Comité DH, Observation générale n° 16, 23e session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 à 21 (1994).

[26] *Ibid.*, par. 8.

limitations du droit à la liberté d'expression fixées par l'Article 19, les limitations au droit à la vie privée fixées par l'Article 17 du PIDCP devraient être interprétées comme étant soumises au test en trois parties :

> L'Article 17 du Pacte peut être également interprété comme contenant lesdits éléments d'un test relatif aux limitations admissibles. Les restrictions qui ne sont pas prescrites par la loi sont « illégales » au sens de l'Article 17, et les restrictions qui ne sont pas nécessaires ou ne poursuivent pas un objectif légitime constituent une immixtion « arbitraire » dans les droits prévus par l'Article 17.[27]

En termes de surveillance (dans le contexte du terrorisme dans ce cas), il définit les paramètres et la portée des restrictions légitimes du droit à la vie privée dans les termes suivants :

> Les États peuvent faire usage de mesures de surveillance ciblées, à condition que ce soit une ingérence ponctuelle, sur la base d'une ordonnance délivrée par un juge indiquant une cause probable ou des fondements raisonnables. Il doit y avoir un fondement factuel, en rapport avec l'attitude d'un individu, qui justifie les soupçons selon lesquels cet individu pourrait être impliqué dans la préparation d'une attaque terroriste.[28]

Le Rapporteur spécial sur la liberté d'expression a également observé que :

> Le droit au respect de la vie privée peut faire l'objet de restrictions dans certaines circonstances exceptionnelles. Cela peut inclure des mesures de surveillance de l'État aux fins de l'administration de la justice pénale, de la prévention du crime ou de la lutte antiterroriste. Toutefois, ces entraves ne sont admissibles qu'à condition de respecter les critères de limitations prévus par la législation internationale relative aux droits de l'homme. De ce fait, la réglementation doit définir clairement les conditions dans lesquelles le droit à la vie privée des individus peut être restreint dans des circonstances exceptionnelles. Les mesures empiétant ce droit doivent être prises par une autorité publique expressément habilitée par la loi à le faire, en général une autorité judiciaire, en vue de protéger les droits d'autrui, par exemple dans le but d'empêcher l'exécution d'un crime, et elles doivent respecter le principe de proportionnalité.[29]

Anonymat et chiffrement

La protection de l'anonymat est une composante cruciale de la protection du droit à la liberté d'expression et des autres droits humains, en particulier le droit à la vie privée. Le chiffrement est une caractéristique fondamentale permettant l'anonymat en ligne.[30] Sans les

[27] Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, A/HRC/13/37, 28 décembre 2009, par. 17.
[28] *Ibid.*, par. 21.
[29] Rapport du Rapporteur spécial sur la liberté d'expression, A17/27, 17 mai 2011, par. 59.
[30] Le chiffrement est un processus mathématique de conversion de messages, informations ou données sous une forme illisible par quiconque sauf le destinataire prévu, qui protège la confidentialité du contenu contre l'accès ou la manipulation d'un tiers ; voir SANS Institute, *History of encryption*, 2001.

techniques d'authentification dérivées du chiffrement, les transactions et communications en ligne sécurisées seraient impossibles.

Le droit à l'anonymat en ligne a jusqu'à présent reçu une reconnaissance limitée en droit international. Traditionnellement, la protection de l'anonymat en ligne a été liée à la protection du droit à la vie privée et des données personnelles. En mai 2015, le Rapporteur spécial sur la liberté d'expression a publié son rapport sur le chiffrement et l'anonymat à l'ère du numérique.[31] Le rapport a mis en évidence les questions suivantes en particulier :

- Le chiffrement et l'anonymat doivent être fortement protégés et promus, car ils garantissent la confidentialité et la sécurité nécessaires à l'exercice significatif du droit à la liberté d'expression et d'opinion à l'ère du numérique.[32]

- L'expression anonyme est une nécessité pour les défenseurs des droits humains, les journalistes et les protestataires. Toute tentative de museler ou d'intercepter des communications anonymes dans les protestations est une restriction injustifiée du droit de manifester pacifiquement, consacré par la Déclaration universelle des droits de l'homme et le PIDCP.[33] La législation et la réglementation protégeant les défenseurs des droits humains et les journalistes devraient inclure des dispositions permettant l'accès et le soutien à l'usage de technologies qui peuvent sécuriser leurs communications ;

- Les restrictions du chiffrement et de l'anonymat doivent satisfaire au test en trois parties des limitations du droit à la liberté d'expression en vertu du droit international.[34] Les lois et les politiques prévoyant des restrictions du chiffrement ou de l'anonymat devraient être soumises aux commentaires du public et n'être adoptées qu'après un processus législatif régulier – et non accéléré. Des garanties procédurales et judiciaires solides devraient être appliquées pour garantir le droit à une procédure régulière de toute personne dont l'utilisation du cryptage ou de l'anonymat est soumise à des restrictions.[35]

Le rapport de mai 2015 estime aussi qu'en ordonnant la « divulgation de clés » ou le déchiffrement de données, les gouvernements peuvent forcer « des entreprises à coopérer avec eux, ce qui engendre des situations très difficiles dont les utilisateurs de moyens de communication font les frais ».[36] Le rapport stipule que ces ordres doivent :

- Reposer sur des lois qui peuvent être consultées publiquement ;
- Dont la portée est clairement limitée à une cible spécifique ;
- Être appliqués par une autorité judiciaire indépendante et impartiale, notamment pour

[31] Rapport du Rapporteur spécial sur la liberté d'expression, A/HRC/29/32, 22 mai 2015.
[32] *Ibid,* par. 12, 16 et 56.
[33] *Ibid,* par. 53.
[34] *Ibid,* par. 56.
[35] *Ibid,* par. 31-35.
[36] *Ibid*, par. 45.

préserver les droits des personnes visées à une procédure équitable ; et

- Être adoptés uniquement en cas de nécessité faute d'autres moyens d'enquête moins intrusifs.[37]

Cybercriminalité

Il n'existe pas de traité international sur la cybercriminalité mais des négociations sont en cours au niveau des Nations Unies. En décembre 2019, l'Assemblée générale des Nations Unies a adopté une résolution sur « la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles », et introduit un Comité ad hoc chargé d'élaborer une convention internationale.

Parmi les normes régionales, la Convention sur la cybercriminalité du Conseil de l'Europe est la plus pertinente.[38] Bien que la Tunisie n'y soit pas partie, la Convention sur la cybercriminalité fournit un point de référence utile pour analyser le Décret-loi.

La Convention sur la cybercriminalité fournit des définitions de termes pertinents, y compris des définitions pour : les données informatiques, les systèmes informatiques, les données relatives au trafic et les fournisseurs de services. Elle contraint les États parties à créer des infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes et des données informatiques ; des délits informatiques, dont la fraude et la falsification ; des infractions se rapportant à la « pornographie enfantine » et des infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. La Convention sur la cybercriminalité énonce ensuite un certain nombre d'exigences procédurales pour l'investigation et la poursuite judiciaire des cybercrimes, y compris des ordonnances de conservation et de production et la recherche et saisie de données informatiques.

Enfin, et surtout, la Convention sur la cybercriminalité précise que les mesures ci-dessus doivent respecter les conditions et garanties de protection des droits humains et des libertés, conformément aux dispositions du PIDCP et aux autres instruments internationaux applicables en matière de droits humains.

[37] *Ibid*.

[38] Convention sur la cybercriminalité du Conseil de l'Europe, CETS n° 185, en vigueur depuis juillet 2004.

Analyse du Décret-loi

Le caractère provisoire du Décret-loi

Le Décret-loi, en tant que législation secondaire émise par le président (qui fait partie du pouvoir exécutif du gouvernement tunisien) est envisagé comme un règlement provisoire - comme mentionné dans l'introduction, après le second tour des élections législatives qui se déroulera début 2023, le Décret-loi sera soumis à l'approbation de l'Assemblée des représentants du peuple nouvellement constituée. Toutefois, les normes internationales des droits de l'homme exigent que les restrictions du type de celles contenues dans le Décret-loi soient établies par le parlement, et non par le pouvoir exécutif. Seuls les parlements ont le pouvoir légitime de réglementer des questions relatives aux droits humains, car ces derniers sont conçus pour protéger les individus du gouvernement lui-même. C'est le rôle du gouvernement exécutif de réglementer les questions concernant l'administration publique, cependant la matière réglementée par les mesures du Décret-loi ne concerne pas l'administration publique mais les affaires pénales ainsi que les droits humains et la liberté d'expression. Dans la mesure où l'objectif d'un règlement provisoire sous un régime d'urgence est d'encadrer le fonctionnement des forces de l'ordre pendant une période transitoire, le droit international exige que le champ d'application d'un tel règlement provisoire soit limité à cet aspect uniquement. Ainsi, seules les questions nécessitant une réglementation immédiate devraient être traitées dans des législations secondaires.

Le principe de prévisibilité juridique

Le Décret-loi est incompatible avec le principe de prévisibilité juridique. La plupart des infractions visées par le Décret-loi sont passibles de peines de prison. Le principe de prévisibilité juridique exige que les peines pouvant aller jusqu'à l'emprisonnement soient régies par le Code pénal. Les personnes assujetties à la loi règlent leur conduite avec certitude, ce qui nécessite qu'elles trouvent facilement toute disposition pénale imposant des peines d'emprisonnement. Par ailleurs, de nombreuses infractions prévues par le Décret-loi sont déjà sanctionnées dans d'autres textes juridiques. Les crimes mentionnés dans le Décret-loi tels que la diffamation, la diffusion des images d'abus sexuels d'enfants et le discours de haine sont déjà sanctionnés dans des textes comme le Code pénal, le Décret-loi n° 115 de 2011 ou le Code des télécommunications, avec différentes peines applicables à ce qui correspond effectivement aux mêmes délits. Cela n'est pas conforme au principe de sécurité juridique et accroît la possibilité d'une application arbitraire de ces dispositions.

Définitions

L'Article 5 du Décret-loi définit un certain nombre de termes utilisés dans la totalité du Décret-loi. Les définitions des systèmes d'information, des données informatiques, du flux de trafic ou données d'accès sont largement conformes aux définitions contenues dans la Convention sur la cybercriminalité.

Cependant, la définition des « fournisseurs de services » s'écarte du champ d'application de l'Article 1 de la Convention sur la cybercriminalité.[39] Le fournisseur de services de communications est défini comme « toute personne physique ou morale fournissant un service de télécommunications au public, y compris les services d'internet ». L'inclusion des personnes physiques dans la définition signifie qu'elles peuvent être également soumises à l'obligation de conservation des données en vertu de l'Article 6 du décret-loi qu'il peut s'avérer impossible de respecter en pratique.

Dans le même temps, la définition semble être plus étroite que dans l'Article 1 de la Convention sur la cybercriminalité. Cette dernière englobe une large catégorie de personnes qui jouent un rôle particulier dans la communication ou le traitement de données sur des systèmes informatiques. La définition fournie par la Convention s'étend également aux entités qui stockent ou traitent des données pour le compte de ce service de communication ou des usagers de ce service. Comme spécifié dans le Rapport explicatif de la Convention sur la cybercriminalité, un fournisseur de services au sens de l'Article 1 comprend donc à la fois les entités qui proposent un service d'hébergement (comme celles fournies par les plateformes de médias sociaux), ou de mise en antémémoire (« cache ») ou une connexion à un réseau.[40]

Le Décret-loi en revanche semble se limiter aux entreprises agissant au niveau des infrastructures. Toutefois, il n'est pas clair si la notion de « *services d'Internet* » couvre les fournisseurs d'un service de communication et donc si ces derniers sont couverts par l'obligation de conservation des données prévue à l'Article 6 du Décret-loi.

[39] Convention sur la cybercriminalité, *op.cit.* En vertu de l'Article 1(c), l'expression « fournisseur de services » désigne : i) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, ii) toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
[40] Rapport explicatif de la Convention sur la cybercriminalité, par. 27.

Infractions se rapportant au contenu

Le Décret-loi prévoit un certain nombre d'infractions liées au contenu, notamment à l'Article 24 (relatif à la diffusion de fausses nouvelles) et à l'Article 26 (relatif à l'exploitation des enfants et aux agressions corporelles).

L'Article 24 est un article très complexe qui contient lui-même plusieurs infractions fondées sur le contenu. Elles seront abordées à tour de rôle ci-dessous.

Diffusion de fausses informations

Comme expliqué précédemment, toute restriction de la liberté d'expression doit (i) être prévue par la loi ; (ii) poursuivre un but légitime ; et (iii) être nécessaire dans une société démocratique et proportionnée au but légitime visé.

L'Article 24(1) du Décret-loi contient plusieurs termes tels que « fausses nouvelles » « fausses données », « rumeurs », qui sont très larges et vagues, et ouverts à différentes interprétations. Pour répondre à l'exigence de légalité, les définitions dans les lois pénales devraient être aussi claires que possible en élaborant en détail ce qui est exactement interdit. Les termes en question n'ont cependant pas de définition convenue dans le droit international ou régional des droits de l'homme et on peut se demander s'il est possible de définir ces concepts avec un niveau de précision suffisant pour répondre aux exigences de sécurité juridique. Cela s'ajoute à la complexité de la distinction entre un fait et une opinion. Il convient également de noter que la diffusion de « rumeurs » – sans que ces rumeurs soient manifestement fausses – peut suffire à constituer une violation de l'Article 24. De même, « l'atteinte aux droits d'autrui » est un concept très large et ne répond pas aux normes de sécurité juridiques requises, en particulier pour une disposition pénale.

Au-delà des questions de clarté juridique, la phrase « dans le but de porter atteinte aux droits d'autrui ou porter préjudice à la sûreté publique ou à la défense nationale ou de semer la terreur parmi la population » ne répond pas aux normes internationales de liberté d'expression. Les restrictions à la liberté d'expression fondées sur une simple « fausseté » ou le caractère trompeur de certaines informations ne répondront pas aux exigences de l'intérêt légitime (qui sont énumérées à l'article 19 du PIDCP, notamment le respect des droits ou de la réputation d'autrui ; la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques). Toute restriction ne sera permise que si elle est manifestement liée à un objectif légitime particulier. De plus, les lois ne peuvent restreindre que les contenus dont il peut être démontré qu'ils sont nocifs. Toutefois, l'Article 24(1) n'exige pas la présence d'un préjudice réel ni même d'un risque concret d'atteinte à l'ordre public ou à la sécurité nationale ou que le message a effectivement semé la terreur parmi la population. En effet, la commission du crime est complète sur la seule base de l'intention du locuteur – et ce bien que l'élément de l'intention ait tendance à être l'un des plus difficiles à démontrer dans les procédures pénales. Dans le même temps, l'utilisation de termes comme « diffuser » suggère qu'un simple « j'aime » sur une plateforme de médias sociaux peut être suffisant pour

relever du champ d'application de l'Article 24(1).

Le manque de clarté juridique et l'absence de but légitime dans l'Article 24(1) sont exacerbés par le fait que des sanctions sévères sont imposées, soit une peine d'emprisonnement de cinq ans et une amende de 50 000 dinars (l'équivalent d'environ 17 000 USD). La peine prescrite est excessivement sévère et disproportionnée. Il est généralement reconnu que le principe de proportionnalité exige que la criminalisation du discours soit toujours une réponse exceptionnelle et en dernier recours et que les limitations de la liberté d'expression doivent « être appropriées pour remplir leur fonction de protection, elles doivent constituer le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché ».[41] Se référant spécifiquement à la question de la désinformation, le Rapporteur spécial sur la liberté d'expression a observé que « le recours au droit pénal ne devrait intervenir que dans les circonstances très exceptionnelles et les cas les plus flagrants d'incitation à la violence, à la haine ou à la discrimination[42] – ces types d'infractions ne sont pas cependant l'objet de l'Article 24(1).

Il existe un risque inhérent évident à donner aux autorités gouvernementales le pouvoir de décider ce qu'est la vérité, et l'expérience montre que les législations sur la désinformation sont souvent utilisées de manière abusive pour museler la dissidence ou les voix critiques dans la société.[43] Il existe également un risque important que l'Article 24(1), en raison de sa nature trop large, soit utilisé contre des journalistes, des opposants politiques et des défenseurs des droits humains en Tunisie.

À titre de comparaison, alors que la Convention sur la cybercriminalité contient une infraction liée au contenu, à savoir la « pédopornographie » (comme examiné dans le contexte de l'Article 26 du Décret-loi), elle n'exige pas la pénalisation de la désinformation, des fausses nouvelles ou de concepts similaires. Dans certains cas, des lois ont été adoptées pour faire face à la désinformation sans toutefois la criminaliser. Par exemple, dans l'Union européenne, le règlement sur les services numériques (Digital Services Act) impose aux très grandes plateformes en ligne et les très grands moteurs de recherche l'obligation d'évaluer et d'atténuer les risques découlant de leurs services, y compris en ce qui concerne la diffusion et amplification de la désinformation.[44] Là où les pays ont effectivement criminalisé la diffusion de fausses nouvelles ou la désinformation (l'exemple le plus récent étant la disposition sur les « informations fausses ou trompeuses » introduite dans le Code pénal turc), cela a été largement critiqué par les organisations de défense des droits humains comme étant incompatible avec les principes de liberté d'expression et les droits humains en ligne.[45]

[41] Voir Observation générale n° 34, *op. cit.*, par. 34.
[42] Rapport du Rapporteur spécial sur la liberté d'expression, A/HRC/47/25, 13 avril 2021, par. 89.
[43] Rapport du Rapporteur spécial des Nations Unies sur la désinformation, par. 55.
[44] Voir le Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) du 19 octobre 2022.
[45] Voir Commission de Venise (Commission européenne pour la démocratie par le droit), Avis conjoint urgent de la Commission de Venise et la Direction générale des droits de l'homme et de l'état de droit (DGI) du Conseil

Diffamation, incitation à l'agression et incitation au discours de haine

L'Article 24(2) du Décret-loi présente bon nombre des mêmes défauts que son alinéa 1, notamment un manque de clarté.

Par exemple, l'Article 24(2) contienne des actions très différentes telles que la diffusion de fausses nouvelles ou d'informations contenant des données à caractère personnel et ensuite combine ces actions avec des concepts aussi variés que la diffamation, l'incitation à l'agression ou l'incitation au discours de haine. Il est donc extrêmement difficile pour les individus de prédire quelles actions exactement sont criminalisées. Ceci est encore aggravé par le fait que, comme à l'alinéa 1, le but ou l'intention de diffamer autrui, de porter atteinte à sa réputation, de le discréditer ou de lui nuire financièrement ou moralement suffit à constituer un crime, sans qu'aucune preuve d'un acte spécifique ne soit susceptible de causer un préjudice réel.

En outre, alors que l'Article 24(1) fait référence à l'usage des systèmes et réseaux d'information et de communication, l'Article 24(2) ne fait référence qu'à l'utilisation de systèmes d'information. Il n'est cependant pas clair si cette distinction est intentionnelle et, si tel est le cas, comment elle est supposée avoir un impact sur le champ d'application des paragraphes respectifs.

Diffamation criminelle

Les lois pénales sur la diffamation sont généralement reconnues comme incompatibles avec les normes internationales de la liberté d'expression.[46] Le Comité des droits de l'homme a également exhorté tous les États parties au PIDCP à abolir les lois pénales sur la diffamation, reflétant un consensus international parmi les organisations internationales.[47] En effet, on estime que de telles lois peuvent rarement être considérées comme poursuivant un but légitime et comme étant nécessaires et proportionnées. Le Comité des droits de l'homme a en outre estimé qu'en tout état de cause, « l'application de la loi pénale devrait être circonscrite aux cas les plus raves et l'emprisonnement ne constitue jamais une peine appropriée ».[48] L'Article 24(2), qui exige une peine d'emprisonnement pour diffamation, constitue donc une violation flagrante des normes internationales relatives à la liberté d'expression.

On ignore aussi dans quelle mesure le délit de diffamation peut être distingué du délit de diffusion d'un message dans le but de « porter atteinte à [la] réputation [d'autrui], de leur nuire financièrement ou moralement (…) ».

---

de l'Europe sur le projet d'amendements au code pénal concernant la disposition sur les « informations fausses ou trompeuses », Avis 1102/2022.

[46] ARTICLE 19, Définir la diffamation : Principes relatifs à la liberté d'expression et la protection de la réputation, 2017.

[47] Observation générale n° 34, *op.cit.*, par. 47. Comité des droits de l'homme, Observations finales sur l'Italie, CCPR/C/ITA/CO/5 ; Observations finales sur l'ex-République yougoslave de Macédoine, CCPR/C/MKD/CO/2.

[48] Observation générale n° 34, *op.cit.*, par. 47.

De plus, cette disposition est désormais ajoutée à la longue liste de dispositions pénales appliquées par les autorités tunisiennes dans les poursuites pour diffamation et délits similaires liés à l'expression (y compris Article 86 du Code des télécommunications, Articles 55 et 56 du Décret-loi n° 115 de 2011 ou plusieurs dispositions du Code pénal tunisien).

Incitation à l'agression

Il existe un risque que la référence à « l'incitation à l'agression » soit utilisée abusivement pour pénaliser toute couverture critique de personnalités publiques ou d'hommes politiques considérée comme faisant de ces derniers des cibles potentielles d'attaques.

En outre, on ne sait pas comment ces dispositions se rapportent à d'autres interdictions d'incitation comme celles de l'Article 32 du Code pénal tunisien ou des Articles 50 et 51 du Décret-loi n° 115 de 2011.

Incitation au discours de haine

L'Article 24 pénalise aussi « l'incitation au discours de haine ».

Il n'existe pas de définition uniforme du « discours de haine » dans le droit international des droits humains. Le droit international contraint les États à interdire les formes les plus graves de discours de haine. Par exemple, l'Article 20(2) du PIDCP exige que les États interdisent tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence.[49] Pour apporter de la clarté sur l'application de ces dispositions, le Plan d'action de Rabat des Nations Unies énonce un test de seuil en six parties pour évaluer si une expression atteint le niveau de gravité prévu à l'Article 20(2) du PIDCP. Il s'agit notamment de prendre en compte le contexte social et politique, le statut du locuteur, l'intention d'inciter le public contre un groupe cible, le contenu et la forme du discours, l'étendue de la diffusion, et la probabilité de préjudice, y compris son imminence. Le Plan de Rabat considère que *tous ces six* critères doivent être remplis pour qu'une déclaration soit considérée comme une infraction pénale.[50]

La principale difficulté posée par l'interdiction de l'incitation au discours de haine dans le Décret-loi est qu'un large éventail d'expressions pourrait potentiellement être pénalisé dans la mesure où aucune définition précise du discours de haine n'est fournie. Il convient également de noter que la loi ne pénalise pas le discours de haine, mais « l'incitation au discours de haine » qui – si le sens peut d'une manière ou d'une autre être considéré comme conforme au PIDCP – signifie essentiellement qu'elle cherche à pénaliser l'incitation à l'incitation. Il s'agit peut-être d'une erreur de rédaction, mais cela montre également le manque de clarté juridique. Par ailleurs, l'Article 52 du Décret-loi n° 115 de 2011 et la Loi n° 2018-50[51] sanctionnent déjà certaines formes de discours de haine, ce qui augmente le

[49] Voir Article 20(2) du PIDCP.
[50] Voir également ARTICLE 19, 'Hate Speech' Explained, A Toolkit, 2015.
[51] Loi organique n° 2018-50 du 23 octobre 2018 relative à l'élimination de toutes les formes de discrimination raciale.

risque d'application arbitraire de ces dispositions juridiques par les autorités poursuivantes dans un cas individuel.

Expression ciblant des représentants publics

L'Article 24(3) stipule que les peines prévues sont portées au double si la personne visée est un agent public ou assimilé. Cette disposition augmente le risque que l'Article 24 soit utilisé pour réduire au silence les critiques et la dissidence politique et elle est incompatible avec les normes internationales de la liberté d'expression qui protègent particulièrement le discours politique. En particulier, le Comité des droits de l'homme a relevé dans son Observation générale n° 34 que, « dans le cadre du débat public concernant des personnalités publiques du domaine politique et des institutions publiques, le Pacte accorde une importance particulière à l'expression sans entrave ». Il souligne également que les délits liés à l'expression ne doivent pas être passibles de « peines plus sévères uniquement en raison de l'identité de la personne qui peut avoir été visée ».[52]

Il est également bien établi dans le droit international des droits de l'homme que le discours politique nécessite une protection renforcée et que les représentants politiques et les agents publics sont soumis à des limites de critique plus larges que les simples particuliers. En effet, les tribunaux internationaux des droits de l'homme ont toujours soutenu que les agents publics devaient tolérer plus, et non moins, de critiques que les citoyens lambda.[53] En choisissant une profession impliquant des responsabilités publiques, les agents publics s'exposent en toute connaissance de cause à l'examen de leurs paroles et de leurs actes par les médias et le grand public.[54] Cependant, l'Article 24(3) inverse le principe démocratique fondamental selon lequel le gouvernement est soumis au contrôle public.

Exploitation des enfants et agressions corporelles

L'Article 26(1) contient des infractions liées à la « pornographie enfantine ».

Les images d'abus sexuels d'enfants sont un type d'expression que les États sont tenus d'interdire en vertu du droit international. La Tunisie a ratifié le Protocole facultatif à la Convention relative aux droits de l'enfant concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants en 2002.[55] L'Article 9 de la Convention sur la cybercriminalité contraint également les États parties à sanctionner divers

[52] Voir Observation générale n° 34, *op.cit.*, par. 38.
[53] Voir, entre autres autorités, Cour européenne des droits de l'homme, *Thoma c. Luxembourg*, App. n° 38432/97, par. 47 ; *Lingens c. Autriche*, App. n° 9815/82, par. 42.
[54] Cour européenne des droits de l'homme, *Bodrozoc et Vujin* c. Serbie, App. 38435/05, par. 34.
[55] Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, résolution A/RES/54/263 à la 54e session de l'Assemblée générale des Nations Unies, 25 mai 2000. Voir notamment l'Article 3(1)(c).

aspects de la production, possession et distribution électroniques de « pédopornographie ». Il est important de noter que l'Article 60 du Décret-loi n° 115 de 2011 pénalise déjà la diffusion de « produits impudiques sur les enfants », bien que la peine soit moindre (1-3 ans contre 6 ans dans l'Article 26(2) du Décret-loi). Par conséquent, une fois de plus, plusieurs chefs d'accusation pourraient être appliqués pour le même comportement et on ne sait pas quelle disposition aurait la préséance dans un cas concret.

L'Article 26(2) sanctionne la publication ou la diffusion d'images ou de vidéos d'agressions physiques ou sexuelles. La disposition ne contient pas d'exception pour les contenus servant à informer le public. L'article peut donc pénaliser la publication de preuves de violations des droits humains ou de contenus servant à informer le public. Alors que d'autres juridictions, par exemple la France et l'Allemagne, interdisent de la même manière la diffusion d'images violentes, elles prévoient de telles exceptions. Par exemple, l'Article 222-33-3 du Code pénal français qui sanctionne « l'enregistrement et la diffusion d'images de violence » stipule que « le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice ».[56]

Violation du droit d'auteur

L'Article 25 du Décret-loi sanctionne quiconque utilise intentionnellement des systèmes d'information et de communication pour violer les droits d'auteur et droits voisins sans obtenir une autorisation de/des ayants droit dans le but d'en tirer profit ou de porter préjudice à l'économie ou aux droits d'autrui. La peine peut être une amende ou une peine d'emprisonnement allant d'un mois à un an.

Des infractions au droit d'auteur sont également prévues dans la Convention sur la cybercriminalité. En particulier, l'Article 10 de la Convention exige que les États parties sanctionnent la violation des droits d'auteur et droits connexes conformément à un certain nombre d'instruments internationaux existants, les parties pouvant se réserver le droit de ne pas imposer de responsabilité pénale si d'autres recours sont disponibles.

L'Article 25 pose deux problèmes principaux. Premièrement, les infractions au droit d'auteur ne peuvent être compatibles avec le droit à la liberté d'expression et d'information que si elles reposent sur une base juridique claire, si chaque élément de l'infraction est clairement défini et si l'éventail des peines disponibles est proportionné à la gravité de l'infraction. L'Article 25 manque de ce niveau de détail, vu qu'il ne décrit pas de manière suffisamment détaillée le type de comportement que le Décret-loi érige précisément en infraction (par exemple, publier une œuvre protégée ; modifier une œuvre ; utiliser une œuvre sous une fausse désignation ou une désignation différente de celle décidée par l'auteur, etc.).

[56] Voir également l'Article 131(2) du Code pénal allemand.

Deuxièmement, l'Article 25 pénalise l'utilisation intentionnelle des systèmes d'information et de communication pour violer le droit d'auteur *« dans le but d'en tirer profit ou de porter préjudice à l'économie et aux droits d'autrui »*. De nombreuses atteintes au droit d'auteur – même si elles ne sont pas de nature commerciale – pourraient sans doute être considérées comme remplissant cette exigence. Cependant, les normes internationales de la liberté d'expression exigent que (i) les autorités chargées du maintien de l'ordre n'engagent pas de poursuites dans les affaires de violation non commerciale du droit d'auteur en raison d'un manque d'intérêt public ; et (ii) que les peines de prison et autres sanctions sévères ne devraient jamais être disponibles en tant que sanction pour violation non commerciale du droit d'auteur.[57]

Par ailleurs, la loi n° 94-36[58] sanctionne déjà les infractions au droit d'auteur, mais de manière beaucoup plus détaillée. La relation entre l'article 25 du Décret-loi et la loi n° 94-36 n'est pas claire. Il existe à nouveau un risque que les autorités appliquent ces dispositions de manière arbitraire dans un cas individuel.

Autres délits de cybercriminalité

Le Décret-loi contient également un certain nombre d'infractions à la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques ainsi que la fraude et la falsification informatiques.

Accès illégal

L'Article 16 du Décret-loi pénalise toute personne qui sciemment accède ou demeure illégalement dans un système informatique. Il reflète globalement la disposition de l'Article 2 de la Convention sur la cybercriminalité. Il est, toutefois, généralement admis que l'utilisation du terme « sans droit » plutôt qu' « illégalement » est plus protectrice de la liberté d'expression, dans la mesure où le premier exclut également de la responsabilité pénale les comportements qui peuvent être justifiés. Cela peut être le cas non seulement dans des circonstances où les défenses juridiques classiques sont applicables, comme le consentement, la légitime défense ou la nécessité, mais aussi dans les cas où d'autres principes ou intérêts conduisent à l'exclusion de toute responsabilité pénale.

Comme l'observe le Rapport explicatif de la Convention sur la cybercriminalité, « les activités légitimes et ordinaires inhérentes à la conception des réseaux ainsi que les pratiques d'exploitation ou de commerce légitimes et ordinaires ne devraient pas être érigées en infractions pénales ».[59]

[57] ARTICLE 19, *Le droit de partager – Principes relatifs au droit à la liberté d'expression et au droit d'auteur à l'ère du numérique,* 2013.
[58] Loi n° 94-36 du 24 février 1994 relative à la propriété littéraire et artistique, telle que modifiée et complétée par la loi ° 2009-33 du 23 juin 2009.
[59] Rapport explicatif de la Convention sur la cybercriminalité, par. 38.

De plus l'Article 2 de la Convention sur la cybercriminalité suggère certains éléments supplémentaires qui élèvent le niveau de protection de dispositions similaires, par exemple le contournement des mesures d'accès ou l'intention délictueuse d'obtenir des données.

Utilisation abusive des équipements

L'Article 17 du Décret-loi punit toute personne qui vend ou diffuse, intentionnellement et illégalement, des équipements ou programmes informatiques conçus ou apprivoisés pour commettre des infractions régies par le Décret-loi ainsi que des mots de passe, codes d'accès ou toutes données informatiques similaires qui permettent d'accéder en totalité ou partiellement à un système d'informations en vue de commettre des infractions régies par le Décret-loi.

L'Article 17 exclut toute responsabilité lorsque la conduite est requise pour la recherche scientifique ou la sécurité de l'information. Cela offre une protection importante, car les technologies peuvent être à double usage et il est dans la nature de la technologie de pouvoir être utilisée à la fois à des fins légitimes et illégitimes. La plupart des entreprises savent que les logiciels qu'elles fabriquent ou vendent peuvent être utilisés à des fins doubles, y compris à des fins d'accès non autorisé à des systèmes et des données informatiques. Une norme d'intention, en particulier une norme renforcée, est requise ; sinon la disposition pourrait sanctionner des activités légitimes telles que les tests de sécurité.

Sans garanties adéquates, les dispositions interdisant les technologies à double emploi peuvent être utilisées pour poursuivre des individus ou des entreprises produisant, distribuant, vendant ou faisant circuler des logiciels employés pour casser les systèmes de gestion des droits numériques (GDN). Les systèmes GDN sont un type de technologie principalement utilisée par les fabricants de matériels informatiques, les éditeurs et les détenteurs de droits d'auteur pour contrôler la façon dont le contenu numérique peut être utilisé après la vente. Les systèmes GDN sont critiqués sur le plan de la liberté d'expression, car la légitimité des détenteurs de droits d'auteur exerçant à perpétuité un contrôle absolu sur le partage d'informations est fortement contestée. Par exemple, les systèmes GDN empêchent les individus de se livrer à des actes triviaux et non commerciaux de violation du droit d'auteur, tels que le transfert de données entre leurs propres appareils électroniques ; ils peuvent également empêcher les individus d'utiliser des œuvres protégées par le droit d'auteur d'une manière qui est normalement protégée par la défense de « l'utilisation loyale ».

Même si le libellé de l'Article 17 du Décret-loi offre une certaine protection, la disposition ne précise pas qu'elle n'impose pas de responsabilité pénale lorsque l'équipement ou le programme n'est pas vendu ou diffusé dans le but de commettre l'un des délits prévus par le Décret-loi contre la confidentialité, l'intégrité et la disponibilité de systèmes et de données informatiques et n'est donc pas tout à fait conforme au libellé de l'Article 6(2) de la

Convention sur la cybercriminalité. Aussi, l'Article 17 exige que le comportement incriminé soit « illégal » et ne pas « sans droit ».

Interception illégale et ingérence dans les données

L'Article 18 du Décret-loi punit l'interception intentionnelle sans droit. La disposition reflète largement l'Article 3 de la Convention sur la cybercriminalité.

L'Article 19 du Décret-loi, pour sa part, punit l'endommagement, la modification, la suppression, l'annulation ou la destruction de données informatiques sans droit et sanctionne également toute tentative de le faire. L'Article 19 n'exige pas qu'une telle ingérence dans les données soit commise intentionnellement et « sans droit ». De plus, l'Article 19 n'exige pas que l'ingérence dans les données entraîne un préjudice grave, comme il est prévu par l'Article 4 alinéa 2 de la Convention sur la cybercriminalité.

Entrave du fonctionnement d'un système et détournement des données

L'Article 20 du Décret-loi sanctionne toute entrave sérieuse sans droit au fonctionnement d'un système informatique en introduisant, envoyant, endommageant, supprimant, détruisant, modifiant ou annulant des données informatiques. Bien que cette disposition reflète l'Article 5 de la Convention sur la cybercriminalité, elle écarte une exigence importante, à savoir que la conduite est « sans droit ».

L'Article 21 du Décret-loi punit en outre toute personne qui utilise délibérément à mauvais escient des données informatiques appartenant à autrui. Cette infraction ne figure pas dans la Convention sur la cybercriminalité. La disposition est incompatible avec les normes internationales de la liberté d'expression en raison de la sévérité de la peine imposée (5 ans d'emprisonnement et une amende) et de sa formulation trop large et ambiguë. On ne sait pas exactement ce que peut signifier une utilisation abusive de données informatiques, en particulier en l'absence de tout préjudice requis, et il existe un risque que cela puisse être appliqué au travail des journalistes d'investigation. La disposition n'exige pas non plus que la conduite soit « sans droit ».

Fraude et falsification informatiques

Les Articles 22 et 23 du Décret-loi punissent la fraude et la falsification informatiques, respectivement. Ces définitions suivent généralement celles contenues dans la Convention sur la cybercriminalité. Toutefois, les articles n'exigent pas que la conduite incriminée soit commise « sans droit » et avec une intention frauduleuse ou délictueuse.

Procédures et enquêtes

Il est généralement reconnu que la nature de certains cybercrimes peut nécessiter des outils d'investigation spéciaux et une coopération internationale pour traiter ces crimes de manière adéquate, raison pour laquelle des dispositions traitant de ces aspects figurent dans la Convention sur la cybercriminalité. Les Articles 6 à 15 du Décret-loi (chapitre II) contiennent des dispositions procédurales et énoncent les pouvoirs d'investigation accordés aux autorités tunisiennes pour enquêter sur les infractions visées par le Décret-loi.

Bien que certaines de ces dispositions présentent certaines similitudes avec la Section 2 de la Convention sur la cybercriminalité (traitant du droit procédural), nombre d'entre elles ne contiennent pas suffisamment de garanties de procédure régulière et de protection des droits humains. Par exemple, le Décret-loi ne contient pas un élément clé de la Convention sur la cybercriminalité, à savoir sa reconnaissance de la nécessité de garanties et de surveillance. La Convention sur la cybercriminalité dans son Article 15 exhorte explicitement les signataires à veiller à ce que « l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes », qui doivent « assurer une protection adéquate des droits de l'homme et des libertés », en particulier le PIDCP entre autres instruments. Par ailleurs, la Convention sur la cybercriminalité requiert, dans son Article 15(2), « une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application, et de la durée du pouvoir ou de la procédure en question ».

Malgré une référence générale au droit international et aux garanties constitutionnelles dans l'Article 2 du Décret-loi, les pouvoirs d'investigation conférés aux autorités tunisiennes par le décret-loi sont beaucoup trop larges et intrusifs. Cela est aggravé par le fait que les infractions incluses dans le Décret-loi ne se limitent pas à celles de la Convention sur la cybercriminalité, mais pénalisent également certaines formes de discours en ligne sans respecter les normes internationales de la liberté d'expression.

Obligation de conservation et accès aux données par les forces de l'ordre

L'Article 6 du Décret-loi contraint les fournisseurs de services de télécommunications à conserver, généralement et systématiquement, les données stockées dans un système d'information pendant au moins deux ans – et potentiellement plus, par arrêté conjoint des ministres de la Défense nationale, de l'Intérieur, de la Justice ainsi que du ministère chargé des Télécommunications. Les personnes dont les données sont conservées ne sont pas obligées d'être, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales.

Les données qui doivent être stockées comprennent des données sur l'identité de l'utilisateur, le trafic et les données de localisation (métadonnées des communications électroniques). Il est généralement admis que l'analyse de ce type de données peut permettre de tirer des conclusions précises sur les individus impliqués, telles que les habitudes de vie quotidienne, les lieux permanents ou temporaires de résidence, les mouvements quotidiens et autres, les activités entreprises, les relations sociales de ces

personnes et les environnements sociaux qu'elles fréquentent.[60]

La conservation obligatoire des données prévue par le Décret-loi va au-delà de ce qui est requis par la Convention sur la cybercriminalité, qui n'impose en fait aucune collecte de données par un fournisseur de services. Dans ses articles 16 et 17, la Convention exige seulement aux États d'autoriser leurs autorités compétentes à ordonner la conservation des données qui existent déjà, ont déjà été collectées et sont stockées.[61] En outre, toute ordonnance de conservation des données doit être prise dans le cadre d'enquêtes ou de procédures pénales spécifiques (Article 14 de la Convention sur la cybercriminalité).

Le caractère général et systématique de la conservation des données exigée par le Décret-loi peut porter atteinte à l'expression anonyme, car il facilite la surveillance.[62] Pour satisfaire au critère de constitution d'une ingérence nécessaire et proportionnée dans le droit au respect de la vie privée et le droit à la liberté d'expression, l'accès à ces données par les forces de l'ordre doit être soumis à des règles claires et précises qui prévoient des garanties suffisantes.[63]

L'accès aux données est régi par l'Article 9 du Décret-loi, qui énonce les pouvoirs procéduraux pour les ordonnances de divulgation ; de recherche et saisie de données informatiques et de collecte en temps réel de données relatives au trafic. L'accès aux données en vertu de l'Article 9 peut aller au-delà de l'accès aux données conservées conformément à l'Article 6 du Décret-loi et les ordonnances peuvent s'adresser à des personnes physiques et morales autres que les fournisseurs de services de télécommunications.

L'Article 9 ne contient pas les garanties nécessaires pour s'assurer que toute ingérence dans les droits à la vie privée et à la liberté d'expression soit limitée à ce qui est nécessaire et proportionné. Par exemple, pour les données relatives au trafic et à la localisation qui permettent de tirer des conclusions précises, l'accès des forces de l'ordre devrait toujours être limité à des cas de délits graves ou de prévention de menaces graves à la sécurité publique[64] – une limitation qui ne s'applique pas en vertu du Décret-loi. En outre, en vertu du Décret-loi, aucune notification ne doit être donnée à l'utilisateur faisant l'objet d'une enquête après l'accès à ses données. Ainsi, il est possible que les personnes ne soient jamais informées que leurs données font l'objet d'une recherche. Cela entravera leur capacité à faire appel et à contester la recevabilité de la recherche de données devant un tribunal,

[60] Voir, par exemple, l'arrêt de la CJUE du 6 octobre 2020, *La Quadrature du Net et autres*, C-511/118, C-512/18 et C-520/18, EU:C:2020:791, par.117.
[61] Voir Rapport explicatif de la Convention sur la cybercriminalité, par. 152.
[62] Pour l'interdépendance entre anonymat et droit à la vie privée et à la liberté d'expression, voir Conseil des droits de l'homme des Nations Unies (2015), Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 22 mai 2015, A/HRC/29/32, par. 16.
[63] Voir *La Quadrature du Net et autres*, *op.cit.,* par. 117.
[64] Voir l'arrêt de la CJUE du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18.

compromettant leur droit à un recours effectif.[65] Enfin, les termes de l'Article 9 concernant la nécessité d'une autorisation judiciaire pour les différentes mesures ne sont pas assez clairs.[66]

Interception des communications

L'Article 10 du Décret-loi autorise l'interception des communications du suspect « dans les cas où la nécessité de l'enquête l'exige ». Habituellement, l'interception des communications, qui permet aux autorités d'accéder à leurs contenus, n'est justifiée que dans des circonstances exceptionnelles en raison de leur nature intrusive et des préoccupations importantes qu'elle soulève pour les droits à la vie privée et à la liberté d'expression. Une telle surveillance ne doit être menée que sur la base de décisions spécifiques d'une autorité étatique, assorties de garanties judiciaires adéquates et dans le respect du principe de proportionnalité.

Les garanties fournies par le Décret-loi sont insuffisantes. Par exemple, on ne sait pas si l'interception est soumise à un contrôle judiciaire obligatoire. Si la formulation même de l'Article 10 suggère que l'interception peut être ordonnée sur la base d'une décision écrite et motivée du procureur de la République ou du juge d'instruction,[67] l'Article 7 du Décret-loi ne se réfère qu'à des « ordonnances judiciaires » relatives à l'accès aux données et à l'interception. Ce type de mesures de surveillance nécessite toutefois que l'autorisation judiciaire préalable soit clairement inscrite dans la législation pertinente sans aucune ambiguïté dans la formulation. On note des lacunes supplémentaires dans le Décret-loi: il n'y a aucune limite de temps à la mesure de surveillance ; il n'y a aucune exigence que l'interception soit ordonnée uniquement pour les crimes graves ; [68] le Décret-loi n'exige pas que les ordonnances d'interception soient adoptées uniquement en cas de nécessité faute d'autres moyens d'enquête moins intrusifs ; et il n'y a aucune obligation d'informer les cibles de l'interception par écrit et aucun droit de recours contre la mesure.

Protection inadéquate des sources journalistiques

[65] Voir A/HRC/29/32, par. 16.

[66] Le texte stipule que : « Le procureur de la République, le juge d'instruction ou les officiers de la police judiciaire autorisés par écrit, sont habilités à ordonner… » On ne sait pas pourquoi le juge d'instruction exigerait une autorisation écrite, tout comme le procureur de la République et les officiers de police judiciaire, raison pour laquelle une lecture possible de ce paragraphe est que seuls les officiers de police ont besoin d'une autorisation judiciaire. Bien que le libellé de l'Article 7 faisant référence aux « ordonnances judiciaires » pour les mesures énumérées à l'Article 9 puisse apporter un certain réconfort, il semble pour sa part contredire les exigences énoncées pour l'autorisation des mesures d'interception en vertu de l'Article 10, comme décrit ci-dessous.

[67] Certains policiers peuvent également ordonner l'interception de communications sur la base d'une décision écrite et motivée d'un procureur de la République ou du juge d'instruction (« *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 »)*.

[68] L'interception peut être ordonnée pour tous les crimes contenus dans le Décret-loi, y compris ceux qui ne sont passibles que d'une peine de trois mois. Voir par exemple l'Article 16 du Décret-loi.

L'Article 19 du PIDCP couvre également la protection du privilège journalistique. Dans son Observation générale n° 34, le Comité des droits de l'homme a observé que les « États parties devraient reconnaître et respecter l'élément du droit à la liberté d'expression qui recouvre le privilège limité qu'a tout journaliste de ne pas révéler ses sources d'information ».[69] En outre, l'Article 11 du Décret-loi n° 115 de 2011 protège la confidentialité des sources d'information des journalistes et stipule que le privilège journalistique ne peut être renversé sans autorisation judiciaire et uniquement dans des circonstances strictement définies.

Aussi, le Décret-loi ne contient aucune disposition spéciale sur la protection des sources journalistiques.[70] Le journalisme d'investigation en particulier, qui s'appuie fortement sur des sources confidentielles, peut être compromis par la conservation systématique des données, l'accès effectivement illimité par les autorités gouvernementales aux données collectées et l'exercice des pouvoirs d'interception prévus par le Décret-loi.

Sanctions pour manquement aux obligations de la collecte de preuves électroniques

Les Articles 27 à 33 du Décret-loi prévoient un certain nombre de sanctions pour manquement aux obligations établies par le Décret-loi pour la collecte de preuves électroniques, y compris le manquement à l'obligation de conservation des données ou l'entrave délibérée à une enquête. L'Article 32 établit la responsabilité pénale des personnes morales et de leurs dirigeants pour les délits visés aux Articles 27 à 31.

Ces dispositions ne fournissent pas de garanties suffisantes. Par exemple, l'Article 27 sanctionnant le non-respect de l'Article 6 du Décret-loi n'exige pas l'intention. Par ailleurs, la sévérité des sanctions prévues pour les différentes infractions, à savoir l'emprisonnement ou la dissolution d'une entreprise, est disproportionnée et pourrait bien être utilisée par les autorités tunisiennes pour exercer des pressions abusives sur les personnes physiques et morales afin qu'elles se conforment à ses injonctions. Compte tenu de l'incompatibilité avec les normes internationales de droits humains de nombreuses infractions pénales dans le Décret-loi, associée aux larges pouvoirs d'investigation dépourvus de garanties de procédure régulière, certaines entreprises pourraient bien résister par exemple aux demandes de divulgation en invoquant leurs engagements en matière de droits humains.

Le degré de pression que le gouvernement tunisien sera en mesure d'exercer efficacement par le biais de ces dispositions pénales peut dépendre dans une large mesure de la question de savoir si les entités respectives ont des représentants et personnels locaux sur le territoire tunisien. Par exemple, en ce qui concerne les entreprises de médias sociaux, la Tunisie n'a pas encore établi d'obligation pour elles de nommer des représentants locaux. La situation

[69] Observation générale n° 34, *op.cit.*, par. 45.

[70] L'Article 7 du Décret-loi interdit aux personnes qui exécutent des ordonnances liées à l'accès aux données et aux mesures d'interception de divulguer le secret professionnel. Cependant, il n'est pas clair quel type de secret professionnel serait couvert par cet article. Dans tous les cas, l'Article 7 ne pourra offrir une protection efficace, car c'est la conservation des données elle-même qui porte atteinte à la protection des sources journalistiques.

pourrait bien être différente pour les fournisseurs de télécommunications situés sur le territoire tunisien.

Juridiction extraterritoriale et coopération internationale

L'Article 34 prévoit que dans certaines circonstances, les juridictions tunisiennes peuvent poursuivre et juger les infractions incriminées dans le Décret-loi y compris lorsqu'elles ont été commises hors du territoire tunisien. C'est le cas si :

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

L'Article 34 prévoit en outre que toute extradition devra avoir lieu conformément aux dispositions en vigueur conformément au code de procédure pénale tunisien et des conventions internationales pertinentes. En effet, toute demande d'extradition sera fondée soit sur un traité bilatéral, soit sur un traité multilatéral d'extradition.

Il convient également de discuter brièvement de l'utilisation potentielle des pouvoirs d'investigation contre des individus en dehors du territoire tunisien. En tant que principe général du droit public international, la compétence des États pour enquêter, poursuivre ou appréhender extra-territorialement un contrevenant est limitée par la souveraineté territoriale de l'État étranger. Cela signifie que les agents des forces de l'ordre d'un État ne peuvent exercer leurs fonctions sur le territoire d'un autre État qu'avec le consentement de ce dernier (et donné par des agents dûment autorisés de cet État).[71]

La Tunisie ne peut donc intercepter aucune communication sur un territoire étranger sans violer la souveraineté dudit État. Le Décret-loi ne fournit pas non plus de base pour une telle interception. En règle générale, les enquêtes sur les infractions présumées commises par des individus en dehors du territoire tunisien seront traitées par des canaux internationaux d'entraide judiciaire sur la base de traités internationaux où l'État requis apporte son concours aux enquêtes pénales. L'étendue de la coopération dépendra des termes de tout traité éventuel en question ou de la volonté politique de l'État requis d'aider la Tunisie dans son enquête.[72]

[71] Voir Rapport de la Commission du droit international sur les travaux de sa cinquante-huitième session, 2006, Annexe E, par. 22. Cela explique pourquoi le Comité des Ministres du Conseil de l'Europe a adopté un deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation des preuves électroniques.

[72] Pour une liste des traités d'entraide juridique et d'extradition entre la Tunisie et les États européens, voir ministère tunisien de la Justice, Conventions judiciaires bilatérales.

Il est également important de rappeler le principe de la double incrimination dans ce contexte, une exigence du droit d'extradition de nombreuses juridictions. Le principe de la double incrimination est une règle selon laquelle l'extradition ou l'assistance en matière pénale dépend de la double incrimination dans le sens où l'acte en question est punissable et passible de poursuites tant dans l'État requérant que dans l'État requis. Le principe est plus couramment appliqué en matière d'extradition, mais certains États l'exigent également pour accorder l'entraide judiciaire.[73]

En fonction de la législation nationale et des traités internationaux en question, certains États pourraient donc refuser l'extradition, par exemple si la demande est fondée sur une prétendue violation de la disposition sur « la diffusion de fausses nouvelles » prévue à l'Article 24(1) du Décret-loi si ladite conduite n'est pas pénalisée dans l'État requis respectif.

[73] Office des Nations Unies contre la drogue et le crime, Manual on Mutual Legal Assistance and Extradition, 2012, par. 158.