Loi n° 05-20 du 4 hija 1441 (25 juillet 2020) relative à la cybersécurité.

Type	Législation
Droit d'origine	Maroc
Nature	Loi
Numéro	05-20
Date	25 juillet 2020
Thématiques	Nouvelles technologies de l'information et de la communication ; Donnée à caractère personnel ; Informatique / Télécommunication ; Défense

Chapitre premier - *Dispositions générales*

Article 1

La présente loi fixe :

– les règles et les dispositions de sécurité applicables aux systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements et entreprises publics et toute autre personne morale de droit public, désignés dans la présente loi par « entité » ;

– les règles et les dispositions de sécurité applicables aux infrastructures d'importance vitale ;

– les règles et les dispositions de sécurité applicables aux exploitants des réseaux publics de télécommunication, aux fournisseurs d'accès à Internet, aux prestataires de services de cybersécurité, aux prestataires de services numériques et aux éditeurs de plateformes Internet, désignés dans la présente loi par « opérateur » ;

– le cadre national de gouvernance de la cybersécurité ;

– le cadre de collaboration et d'échange d'informations entre l'autorité nationale de la cybersécurité, désignée par voie réglementaire et appelée dans la présente loi « autorité nationale » et les services compétents de l'Etat chargés du traitement des infractions portant atteinte aux systèmes de traitement automatisé des données ;

– les concours apportés par l'autorité nationale aux organismes nationaux compétents pour le renforcement de la confiance numérique, le développement de la digitalisation des services fournis par l'Etat et la protection des données à caractère personnel ;

– les attributions de l'autorité nationale, notamment en matière de développement de l'expertise nationale, de sensibilisation dans le domaine de la cybersécurité au profit des entités, des acteurs du secteur privé et des particuliers, et de renforcement de la coopération avec les organismes nationaux et étrangers.

Article 2

Au sens de la présente loi, on entend par :

– « *Cybersécurité » :* l'ensemble de mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques, et technologies permettant à un système d'information de résister à des évènements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles ;

– « *Cybercriminalité » :* l'ensemble des actes contrevenant à la législation nationale ou aux traités internationaux ratifiés par le Royaume du Maroc, ayant pour cible les réseaux ou les systèmes d'information ou les utilisant comme moyens de la commission d'un délit ou d'un crime ;

– « *Cybermenace » :* toute action qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient ;

– « *Cyberéthique » :* l'ensemble des normes et règles pour un comportement responsable dans le cyberespace ;

– « *Infrastructures d'importance vitale » :* les installations, les ouvrages et les systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions ;

– « *Secteur d'activités d'importance vitale » :* l'ensemble des activités exercées par les infrastructures d'importance vitale et concourant à un même objectif. Ces activités ont trait soit à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice des prérogatives de l'Etat ou au maintien de ses capacités de sécurité ou au fonctionnement de l'économie, dès lors que ces activités sont difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population ;

– « *Système d'information » :* un ensemble organisé de ressources telles que les personnels, matériels, logiciels, données et procédures qui permettent de collecter, de classifier, de traiter et de diffuser l'information sur un environnement donné ;

– « *Système d'information sensible » :* système d'information traitant des informations ou des données sensibles sur lesquelles une atteinte à la confidentialité, à l'intégrité ou à la disponibilité porterait préjudice à une entité ou à une infrastructure d'importance vitale ;

– « *Service de cybersécurité » :* tout service de sécurité fourni par des prestataires de services de cybersécurité à une entité ou à une infrastructure d'importance vitale et portant sur la détection et le diagnostic des incidents de cybersécurité et le renforcement de la sécurité de leurs systèmes d'information ;

– « *Prestataire de services numériques » :* toute personne physique ou morale qui fournit à distance, par voie électronique et à la demande d'un destinataire, l'un des services ci-après :

• un service numérique qui permet à des consommateurs ou à des professionnels de conclure des contrats de vente ou de service en ligne ;

• un service numérique qui permet aux utilisateurs d'effectuer des recherches sur les sites Internet ;

• un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris les hébergeurs de données et/ou systèmes d'information (Datacenter) et les prestataires des services d'informatique en nuage (Cloud) ;

– « *Hébergement » :* toute prestation de stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournie, à titre onéreux ou gratuit, par des prestataires de services numériques ;

– « *Externalisation d'un système d'information » :* toute opération qui consiste à confier, en partie ou en totalité, le système d'information d'une entité à un prestataire dans le cadre d'un contrat fixant de façon précise notamment le niveau de services et la durée de l'externalisation ;

– « *Homologation des systèmes d'information » :* document par lequel le responsable d'une infrastructure d'importance vitale atteste de sa connaissance du système d'information et des mesures de sécurité techniques, organisationnelles ou juridiques mises en œuvre et accepte les risques résiduels ;

– « *Incident de cybersécurité» :* un ou plusieurs événements indésirables ou inattendus liés à la sécurité des systèmes d'information et présentant une forte probabilité de compromettre les activités d'une entité, d'une infrastructure d'importance vitale ou d'un opérateur ou de menacer la sécurité de leurs systèmes d'information ;

– « *Crise cybernétique » :* l'état résultant de l'occurrence d'un ou plusieurs événements de cybersécurité pouvant avoir un impact grave sur la vie des populations, l'exercice de l'autorité de l'Etat, le fonctionnement de l'économie, ou sur le maintien des capacités de sécurité et de défense du pays ;

– « *Gestion des incidents de cybersécurité » :* le processus de détection, de signalement et d'évaluation des incidents de cybersécurité, ainsi que les mesures d'intervention et de traitement y afférentes.

Chapitre II - *Du dispositif de sécurité des systèmes d'information*

Section première. - Dispositions propres aux entités

Article 3

Chaque entité doit veiller à ce que ses systèmes d'information soient conformes aux directives, règles, règlements, référentiels ou recommandations, édictés par l'autorité nationale.

Article 4

Chaque entité doit élaborer et mettre en œuvre une politique de sécurité de ses systèmes d'information qui soit conforme aux directives de l'autorité nationale.

Chaque entité est tenue d'identifier les risques qui menacent la sécurité de ses systèmes d'information et de prendre des mesures techniques et organisationnelles nécessaires pour gérer ces risques, éviter les incidents de nature à porter atteinte aux systèmes d'information ainsi que pour en réduire au minimum l'impact.

Tout système d'information d'une entité offrant des services numériques à des tiers doit, avant sa mise en exploitation, faire l'objet d'un audit de sa sécurité.

Chaque entité doit, régulièrement, auditer ses systèmes d'information.

Article 5

Chaque entité doit classifier ses actifs informationnels et systèmes d'information selon leur niveau de sensibilité en termes de confidentialité, d'intégrité et de disponibilité. Les mesures de protection des actifs informationnels et systèmes d'information doivent être proportionnés au niveau de classification attribué.

Chaque entité doit arrêter des procédures d'habilitation des personnes pouvant accéder aux informations classifiées et des conditions d'échange, de conservation ou de transport de ces informations.

Le référentiel de classification des actifs informationnels et des systèmes d'information est fixé par voie réglementaire.

Article 6

Chaque entité doit désigner un responsable de la sécurité des systèmes d'information qui veille à l'application de la politique de sécurité des systèmes d'information.

Le responsable de la sécurité des systèmes d'information est l'interlocuteur de l'autorité nationale de la cybersécurité et doit jouir de l'indépendance requise dans l'exercice de sa mission.

Article 7

Chaque entité met en place des moyens appropriés de supervision et de détection des évènements susceptibles d'affecter la sécurité de ses systèmes d'information et d'avoir un impact significatif sur la continuité des services qu'elle assure.

Les données techniques générées par les moyens précités ne peuvent être exploitées par l'autorité nationale qu'aux seules fins de caractériser et traiter la menace affectant la sécurité des systèmes d'information de l'entité concernée.

Article 8

Chaque entité doit, dès qu'elle prend connaissance d'un incident affectant la sécurité ou le fonctionnement de ses systèmes d'information, le déclarer à l'autorité nationale.

A la demande de l'autorité nationale, chaque entité lui communique, sans délai, les informations complémentaires relatives aux incidents affectant la sécurité ou le fonctionnement de ses systèmes d'information.

L'autorité nationale précise les données techniques et les informations relatives aux incidents qui doivent être communiquées ainsi que les modalités de leur transmission.

Elle adresse à l'entité concernée une synthèse des mesures et recommandations relatives au traitement de l'incident.

Article 9

Chaque entité prépare un plan de continuité ou de reprise d'activités intégrant l'ensemble des solutions de secours pour neutraliser les interruptions des activités, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

Le plan de continuité ou de reprise d'activités doit être testé régulièrement afin de le mettre à jour en fonction des évolutions propres de l'entité et de l'évolution des menaces.

Article 10

En cas d'externalisation d'un système d'information sensible à un prestataire, ce dernier doit respecter les règles, règlements et référentiels techniques relatifs à la sécurité des systèmes d'information édictés par l'autorité nationale.

Article 11

Les données sensibles doivent être exclusivement hébergées sur le territoire national.

Article 12

Toute externalisation d'un système d'information sensible doit faire l'objet d'un contrat de droit marocain qui doit comprendre des engagements de protection de l'information, d'auditabilité et de réversibilité, ainsi que les exigences de sécurité et les niveaux de service voulus. .

Article 13

L'autorité nationale fixe les règles et le référentiel technique régissant la sécurité relative à l'externalisation des systèmes d'information.

Section 2. - Dispositions propres aux infrastructures d'importance vitale disposant de systèmes d'information sensibles

Article 14

Les dispositions de la section première du présent chapitre s'appliquent aux infrastructures d'importance vitale.

Article 15

La liste des secteurs d'activités d'importance vitale et des autorités gouvernementales, établissements publics ou autres personnes morales de droit public, assurant la coordination de ces secteurs est fixée par voie réglementaire.

Article 16

Les infrastructures d'importance vitale sont désignées pour chaque secteur d'activité d'importance vitale par l'autorité gouvernementale, l'établissement public ou la personne morale de droit public dont relève la coordination de ce secteur, et ce après avis de l'autorité nationale.

La liste de ces infrastructures doit être tenue secrète et doit être actualisée à intervalles réguliers et au moins tous les deux ans.

Article 17

Le responsable de l'infrastructure d'importance vitale établit, sur la base des résultats d'une analyse des risques, la liste des systèmes d'information sensibles et la transmet avec les mises à jour de celle-ci à l'autorité nationale.

Article 18

L'autorité nationale peut faire des observations au responsable de l'infrastructure d'importance vitale sur la liste des systèmes d'information sensibles qui lui a été transmise.

Dans ce cas, le responsable de l'infrastructure d'importance vitale est tenu de modifier sa liste conformément à ces observations et transmet la liste modifiée à l'autorité nationale dans un délai de deux mois à compter de la date de réception des observations.

La liste des systèmes d'information sensibles doit être tenue secrète.

Article 19

Tout système d'information sensible doit faire l'objet d'une homologation de sa sécurité avant sa mise en exploitation.

Le guide d'homologation des systèmes d'information sensibles est fixé par l'autorité nationale.

Article 20

A la demande de l'autorité nationale, les responsables des infrastructures d'importance vitale soumettent les systèmes d'information sensibles desdites infrastructures à un audit effectué par cette autorité ou par des prestataires d'audit qualifiés par ladite autorité.

Les critères de qualification des prestataires d'audit et les modalités de déroulement de l'audit sont fixés par voie réglementaire.

Article 21

Les responsables des infrastructures d'importance vitale sont tenus de communiquer à l'autorité nationale ou au prestataire d'audit qualifié les informations et éléments nécessaires pour réaliser l'audit, y compris les documents relatifs à leur politique de sécurité et, le cas échéant, les résultats d'audit de sécurité précédents, et leur permettre d'accéder aux réseaux et systèmes d'information faisant l'objet du contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

Les prestataires d'audit qualifiés et leurs employés sont astreints, sous peine des sanctions prévues par le code pénal, au respect du secret professionnel pendant toute la durée de la mission d'audit et après son achèvement, sur les renseignements et documents recueillis ou portés à leur connaissance à l'occasion de cette mission.

Article 22

Lorsque l'audit est effectué par un prestataire d'audit qualifié, le rapport d'audit est transmis par le responsable de l'infrastructure d'importance vitale à l'autorité nationale.

Le prestataire d'audit qualifié doit veiller à la confidentialité du rapport d'audit.

Article 23

Lorsque les opérations d'audit sont effectuées par les prestataires d'audit qualifiés, les coûts sont supportés par le responsable de l'infrastructure d'importance vitale concernée par ces opérations.

Article 24

Chaque responsable d'infrastructure d'importance vitale auditée doit mettre en place un plan d'actions pour mettre en œuvre les recommandations figurant dans les rapports d'audit et le transmet à l'autorité nationale pour le suivi de sa mise en œuvre.

Article 25

Les responsables des infrastructures d'importance vitale doivent recourir à des services, produits ou solutions qui permettent le renforcement des fonctions de sécurité, définis par l'autorité nationale.

En cas d'externalisation des services de cybersécurité, les responsables des infrastructures d'importance vitale doivent recourir à des prestataires qualifiés par l'autorité nationale.

Les critères de qualification des prestataires de services de cybersécurité sont fixés par voie réglementaire.

Section 3. - Dispositions propres aux opérateurs

Article 26