Projet de loi n° 05-20 relative à la cybersécurité

CHAPITRE PREMIER

Dispositions générales

ARTICLE PREMIER

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, utilisant les réseaux ou les systèmes d'information comme moyens de la commission d'un délit ou d'un crime ou les ayant pour cible ;

- *« Cybermenace » :* une 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 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'État 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 de 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 cybersécurité à une entité ou à une infrastructure d'importance vitale des services de détection et de diagnostic des incidents de cybersécurité et de 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:

  - 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 SECURITE DES SYSTEMES 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 et 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 ou établissements publics ou 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 ou 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

Les exploitants des réseaux publics de télécommunications, les fournisseurs d'accès à Internet, les prestataires de services de cybersécurité, les prestataires de services numériques et les éditeurs de plateformes Internet, doivent se conformer aux directives de l'autorité nationale notamment en matière de conservation des données techniques nécessaires à l'identification de tout incident de cybersécurité.

Ces données techniques comprennent particulièrement les données de connexion et les journaux informatiques et traces des évènements de sécurité générés par les systèmes d'exploitation, applications et produits de sécurité.

La durée de conservation des données techniques nécessaires à l'identification et à l'analyse de l'incident est fixée à une année. Cette durée peut être modifiée par voie réglementaire.

ARTICLE 27

Les exploitants des réseaux publics de télécommunications, les fournisseurs d'accès à Internet, les prestataires de services de cybersécurité, les prestataires de services numériques et les éditeurs de plateformes Internet informent leurs clients de la vulnérabilité de leurs systèmes d'information ou de l'atteinte qui pourrait les affecter.

ARTICLE 28

Pour les besoins de la sécurité des systèmes d'information des entités et des infrastructures d'importance vitale, les agents de l'autorité nationale habilités sont autorisés, aux seules fins de prévenir et de caractériser la cybermenace, à procéder auprès des exploitants des réseaux publics de télécommunications, des fournisseurs d'accès à Internet, des prestataires de services de cybersécurité, des prestataires de services numériques et des éditeurs de plateformes Internet, au recueil et à l'analyse des seules données techniques, à l'exclusion de toute autre exploitation.

L'autorité nationale est habilitée à installer, sur les réseaux publics de télécommunications et ceux des fournisseurs d'accès à Internet des dispositifs techniques aux seules fins de détecter des évènements susceptibles d'affecter la sécurité des systèmes d'information des entités et des infrastructures d'importance vitale.

Ces dispositifs sont installés pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace.

ARTICLE 29

Les prestataires de services de cybersécurité, les prestataires de services numériques et les éditeurs de plateformes Internet doivent, dans le cadre des directives de l'autorité nationale, prendre les mesures de protection nécessaires en vue de prévenir et neutraliser les effets des menaces ou atteintes aux systèmes d'information de leurs clients.

ARTICLE 30

Lorsque les exploitants des réseaux publics de télécommunications, les fournisseurs d'accès à Internet, les prestataires de services de cybersécurité, les prestataires de services numériques et les éditeurs de plateformes Internet détectent des évènements susceptibles d'affecter la sécurité des systèmes d'information de leurs clients, ils doivent en informer, sans délai, l'autorité nationale.

ARTICLE 31

Les exploitants des réseaux publics de télécommunications et les fournisseurs d'accès à Internet doivent recourir, sur les réseaux de communications électroniques qu'ils exploitent, à des dispositifs de détection mettant en œuvre, des marqueurs techniques fournis par l'autorité nationale, aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés.

ARTICLE 32

Les prestataires de services numériques sont tenus d'identifier les risques qui menacent la sécurité de leurs systèmes d'information et de prendre des mesures techniques et organisationnelles nécessaires pour gérer ces risques, pour éviter les incidents de nature à porter atteinte à leurs réseaux et systèmes d'information ainsi que pour en réduire au minimum l'impact, de manière à garantir la continuité de leurs services.

ARTICLE 33

Les prestataires de services numériques doivent dès qu'ils en prennent connaissance, déclarer à l'autorité nationale les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de leurs services, lorsque les informations dont ils disposent font apparaître que ces incidents ont un impact significatif sur la fourniture de ces services.

ARTICLE 34

Lorsque l'autorité nationale est informée, par quelque moyen que ce soit, qu'un prestataire de services numériques ne satisfait pas à l'une des obligations prévues par la présente loi, elle peut le soumettre à des contrôles destinés à vérifier le respect de

ces obligations ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de ses services.

Les contrôles sont effectués par l'autorité nationale ou par des prestataires d'audit qualifiés par ladite autorité. Dans ce dernier cas, le coût des contrôles est à la charge du prestataire de services numériques.

En cas de manquement constaté à l'occasion d'un contrôle, l'autorité nationale peut mettre en demeure les dirigeants du prestataire concerné de se conformer, dans un délai qu'elle fixe, aux obligations qui incombent au prestataire en vertu de la présente section.

CHAPITRE III

DE LA GOUVERNANCE DE LA CYBERSECURITE

Section première : Du comité stratégique de la cybersécurité

ARTICLE 35

Il est créé un comité stratégique de la cybersécurité chargé de :

- élaborer les orientations stratégiques de l'Etat en matière de cybersécurité et veiller sur la résilience des systèmes d'information des entités, des infrastructures d'importance vitale et des opérateurs visés à la section III du chapitre II de la présente loi;
- évaluer annuellement le bilan d'activité de l'autorité nationale ;
- évaluer les travaux du comité national de gestion des crises et évènements cybernétiques majeurs prévu à l'article 36 ci-après ;
- arrêter le périmètre des audits de la sécurité des systèmes d'information effectués par l'autorité nationale;
- promouvoir la recherche et développement dans le domaine de la cybersécurité ;
- promouvoir les programmes et actions de sensibilisation et de renforcement des capacités en cybersécurité au profit des entités et des infrastructures d'importance vitale ;
- donner son avis sur les projets de lois et règlements se rapportant au domaine de la cybersécurité.

La composition et les modalités de fonctionnement du comité stratégique de la cybersécurité sont fixées par voie réglementaire.

ARTICLE 36

Il est institué, auprès du comité stratégique de la cybersécurité, un comité de gestion des crises et évènements cybernétiques majeurs, chargé d'assurer une intervention coordonnée en matière de prévention et de gestion de crise par suite d'incidents de cybersécurité.

A cet effet, les exploitants des réseaux publics de télécommunications, les fournisseurs d'accès à Internet, les prestataires de services de cybersécurité et les prestataires de services numériques doivent, en cas de crises cybernétiques majeures, répondre aux prescriptions et demandes de concours et d'assistance technique du comité de gestion des crises et évènements cybernétiques majeurs.

La composition et les modalités de fonctionnement de ce comité ainsi que le domaine d'intervention de chacun de ses membres sont fixés par voie réglementaire.

ARTICLE 37

Pour faire face aux incidents de cybersécurité majeurs, le comité de gestion des crises et évènements cybernétiques majeurs peut décider des mesures que les entités et les responsables des infrastructures d'importance vitale doivent mettre en œuvre et élaborer des recommandations et conseils destinés aux opérateurs du secteur privé et aux particuliers.

Section 2 : De l'autorité nationale de la cybersécurité

ARTICLE 38

L'autorité nationale est chargée de mettre en œuvre la stratégie de l'Etat en matière de cybersécurité.

A cet effet, outre les missions qui lui sont dévolues par la présente loi, l'autorité nationale est chargée de :

- coordonner les travaux relatifs à l'élaboration et à la mise en œuvre de la stratégie de l'Etat en matière de cybersécurité et veiller à l'application des orientations du comité stratégique de la cybersécurité;
- définir des mesures de protection des systèmes d'information et veiller à leur application ;
- proposer au comité stratégique de la cybersécurité les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des entités et des infrastructures d'importance vitale;
- qualifier les prestataires d'audit des systèmes d'information sensibles des infrastructures d'importance vitale et les prestataires de service de cybersécurité;
- concevoir les moyens permettant d'assurer la sécurité des communications électroniques interministérielles et coordonner leur mise en œuvre ;
- assurer les contrôles prévus par la présente loi ;
- veiller à la conduite de missions d'audits de sécurité des systèmes d'information des entités ainsi que des infrastructures d'importance vitale ;
- procéder à l'audit des prestataires de services de cybersécurité et des prestataires de services numériques proposant des services aux infrastructures d'importance vitale disposant de systèmes d'information sensibles ;
- assister et conseiller les entités et les infrastructures d'importance vitale pour le renforcement de la sécurité de leurs systèmes d'information ;
- assister et accompagner les entités ainsi que les infrastructures d'importance vitale pour la mise en place de dispositifs de détection des événements affectant ou susceptibles d'affecter la sécurité de leurs systèmes d'information et coordonner la réaction à ces événements;
- mettre en place, en relation avec les entités et les infrastructures d'importance vitale, un système externe de veille, de détection et d'alerte des événements susceptibles d'affecter la sécurité de leurs systèmes d'information et coordonner la réaction à ces événements ;
- mener et soutenir les activités de recherche scientifique et technique dans le domaine de la cybersécurité.

ARTICLE 39

L'autorité nationale est tenue de préserver la confidentialité des informations sensibles qu'elle recueille dans le cadre de la présente loi.

ARTICLE 40

L'autorité nationale fixe les règles de sécurité nécessaires à la protection des systèmes d'information des entités, des infrastructures d'importance vitale et des opérateurs visés à l'article premier de la présente loi.

L'autorité nationale fixe des règles de sécurité particulières à un secteur d'activité d'importance vitale déterminé. Elle notifie aux responsables des infrastructures d'importance vitale relevant dudit secteur lesdites règles ainsi que les modalités et les délais pour leur mise en œuvre.

Les responsables précités sont tenus d'appliquer ces règles à leurs frais.

ARTICLE 41

Pour faire face à une attaque informatique qui vise les systèmes d'information affectant les fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, les agents de l'autorité nationale procèdent aux opérations d'investigation technique nécessaires à la caractérisation de l'attaque et veillent à la mise en œuvre de mesures et recommandations y afférent.

ARTICLE 42

L'autorité nationale collabore avec les services compétents de l'Etat à travers l'échange de toute donnée ou information susceptible de les aider dans le traitement des infractions portant atteinte aux systèmes de traitement automatisé des données.

Lorsqu'il appert à l'autorité nationale, à l'occasion de l'exercice de ses attributions, qu'un acte est présumé contraire à la loi, elle en saisit les autorités compétentes.

Les autorités compétentes doivent informer l'autorité nationale du sort réservé à la saisine.

CHAPITRE IV

DE LA FORMATION, DE LA SENSIBILIBATION ET DE LA COOPERATION

ARTICLE 43

L'autorité nationale organise, en collaboration avec les acteurs et professionnels du domaine de la cybersécurité, des cycles de formation et des exercices au profit du personnel des entités et des infrastructures d'importance vitale pour développer et renforcer les capacités nationales en la matière.

ARTICLE 44

L'autorité nationale définit et met en œuvre des programmes de sensibilisation sur la cyberéthique et sur les enjeux liés aux menaces et risques de cybersécurité au profit du personnel des entités, des infrastructures d'importance vitale, du secteur privé et des particuliers.

Des conseils et recommandations d'hygiène en cybersécurité au profit du personnel des entités, des infrastructures d'importance vitale, du secteur privé et des particuliers sont régulièrement publiés sur le site web de l'autorité nationale.

ARTICLE 45

L'autorité nationale contribue aux programmes initiés par les organes compétents de l'Etat 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.

ARTICLE 46

L'autorité nationale développe et coordonne, en concertation avec les administrations concernées, les relations de coopération avec les organismes nationaux et étrangers dans le domaine de la cybersécurité.

ARTICLE 47

L'autorité nationale entretient des relations de coopération au niveau national et international en vue de traiter les incidents de cybersécurité et de développer le partage de l'expérience et de l'expertise dans ce domaine.

CHAPITRE V

DE LA CONSTATATION DES INFRACTIONS ET DES SANCTIONS

ARTICLE 48

Outre les officiers de la police judiciaire, sont habilités à rechercher et à constater, par procès-verbaux, les infractions aux dispositions de la présente loi et des textes pris pour son application les agents de l'autorité nationale commissionnés à cet effet et assermentés conformément à la législation en vigueur.

Les procès-verbaux de constatation des infractions sont adressés au ministère public compétent.

ARTICLE 49

Sans préjudice des sanctions pénales plus graves prévues par la législation en vigueur, est puni d'une amende de 200.000 à 400.000 DH:

- tout responsable d'une entité ou d'une infrastructure d'importance vitale qui procède à l'hébergement des données sensibles en dehors du territoire national, en violation des dispositions de l'article 11 ci-dessus ;
- tout responsable d'une infrastructure d'importance vitale disposant d'un système d'information sensible ayant mis en exploitation un système d'information sensible sans faire l'objet de l'homologation prévue à l'article 19 ci-dessus ;
- tout responsable d'une infrastructure d'importance vitale qui a confié l'audit de la sécurité des systèmes d'information sensibles de ladite infrastructure à un prestataire d'audit non qualifié, en violation des dispositions de l'article 20 ci-dessus ;
- quiconque ayant fourni des prestations d'audit de la sécurité des systèmes d'information sensibles des infrastructures d'importance vitale

sans être qualifié par l'autorité nationale ou ayant continué à fournir ces prestations malgré le retrait de sa qualification par ladite autorité;

- tout responsable d'une infrastructure d'importance vitale ayant externalisé les services de cybersécurité à un prestataire non qualifié, en violation des dispositions de l'article 25 ci-dessus ;
- quiconque ayant fourni des prestations de cybersécurité sans être qualifié par l'autorité nationale ou ayant continué à fournir ces prestations malgré le retrait de sa qualification par ladite autorité.

ARTICLE 50

Sans préjudice des sanctions pénales plus graves prévues par la législation en vigueur, est puni d'une amende de 100.000 à 200.000 DH:

- quiconque manque aux obligations de déclaration des incidents, en violation des dispositions prévues aux articles 8, 30 et 33 ci-dessus ;
- quiconque, par quelque moyen que ce soit, fait obstacle ou empêche le déroulement des audits de sécurité des systèmes d'information sensibles des infrastructures d'importance vitale, prévus à l'article 20 ci-dessus ;
- tout exploitant d'un réseau public de télécommunications, ou fournisseur d'accès à Internet, ou prestataire de services de cybersécurité, ou prestataire de services numériques, ou éditeur de plateformes Internet, manque aux obligations prévues à l'article 26 ci-dessus ;
- tout exploitant d'un réseau public de télécommunications ou fournisseur d'accès à Internet ou leurs agents, fait obstacle aux actions menées par l'autorité nationale ou ses agents, prévues à l'article 28 ci-dessus ;
- tout prestataire de service numérique qui s'abstient de prendre les mesures prévues à l'article 32 ou fait obstacle aux opérations de contrôle prévues à l'article 34 ci-dessus.

Est puni de la même peine d'amende, toute personne dont le système d'information a été utilisé à son insu pour propager des programmes malveillants ou pour accomplir des actes illicites, qui s'abstient d'exécuter les directives de l'autorité nationale, après en avoir été informé.

ARTICLE 51

Le tribunal peut prononcer la confiscation des objets et moyens ayant servi à commettre les infractions aux dispositions de la présente loi.

ARTICLE 52

En cas de récidive, les sanctions prévues par la présente loi sont portées au double.

Est en état de récidive, quiconque ayant été condamné, par décision de justice ayant acquis la force de la chose jugée, à une peine pour une infraction aux dispositions de la présente loi, a commis la même infraction moins de 4 ans après l'expiration de cette peine ou sa prescription.

ARTICLE 53

La présente loi entre en vigueur à compter de la date de publication au « Bulletin Officiel » des textes pris pour son application.