ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

NOTE DE PRESENTATION RELATIVE A LA LOI N° 05-20 SUR LA CYBERSECURITE

L'accroissement rapide du spectre des cybermenaces parallèlement à l'évolution des usages, des services et des infrastructures numériques rend nécessaire la réévaluation des bases légales en vigueur afin qu'elles puissent être en phase par rapport à la réalité du terrain et adaptées en conséquence.

1. UN CONTEXTE INTERNATIONAL MARQUE PAR UNE INTENSIFICATION DE LA LEGISLATION SUR LA CYBERSECURITE

En matière de cybersécurité, la législation s'est intensifiée au niveau international au cours des dernières années. La conformité réglementaire s'impose désormais comme un enjeu de taille pour les entités publiques et privées. A cet égard, il est à souligner que l'Organisation des Nations Unies a reconnu le principe de l'applicabilité du droit international au cyberespace.

De plus, plusieurs pays ont dû prendre, en matière de cybersécurité, des mesures législatives et réglementaires contraignantes pour sécuriser leurs systèmes d'information, réussir leur transition numérique et se protéger notamment contre les risques de cybercriminalité, de sabotage, de vols et d'exploitation abusive de données personnelles et sensibles.

Dans ce cadre, les Etats Unis d'Amérique ont élaboré une directive en 2015 qui crée de manière spécifique un cadre juridique édictant des règles de protection contre les cybermenaces. En 2013, la France a rajouté une pierre à son édifice en matière de cybersécurité en imposant aux opérateurs d'importance vitale, à travers la loi sur la programmation militaire, le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent.

Cette loi impose aussi aux opérateurs télécoms de participer activement à la détection des attaques informatiques visant leurs abonnés. Des sanctions sont prévues contre les organismes qui manqueraient à leurs obligations.

Pour sa part, l'Union Européenne a récemment mis en application deux directives régissant la sécurité de l'information et la protection des données, qui sont devenues exécutoires pour les Etats membres.

2. LA CYBERSECURITE AU MAROC : UN PROCESSUS ENGAGE PROGRESSIVEMENT DEPUIS 2011

Le Maroc s'est engagé depuis 2011, **sous la Conduite Eclairée de Sa Majesté le Roi que Dieu l'Assiste**, sur la voie du renforcement de ses capacités nationales de sécurité des systèmes d'information et de la consolidation de la confiance numérique. Dans la continuité des actions ainsi entreprises, le Royaume s'est doté en 2012 d'une Stratégie Nationale de Cybersécurité et d'une Directive Nationale de la Sécurité des Systèmes d'Information applicable depuis 2014 aux administrations et organismes publics.

Pour accélérer la montée en puissance de ce dispositif, l'Administration de la défense nationale (ADN) a également élaboré en 2016 un décret fixant le dispositif de protection des systèmes d'information sensibles (SIS) des infrastructures d'importance vitale.

Ce texte a été complété par l'élaboration en 2018 d'un arrêté du Chef du Gouvernement fixant les critères d'homologation des prestataires d'audit des SIS des infrastructures d'importance vitale et les modalités de déroulement de l'audit.

Compte tenu des enjeux auxquels notre pays est confronté dans le domaine de la cybersécurité, il devient plus que jamais nécessaire de disposer d'un cadre juridique complet qui s'appuierait sur les actions déjà menées. Ce cadre permettrait de renforcer la sécurité des systèmes d'information de l'Etat

et des infrastructures d'importance vitale et préconiserait des actions de sensibilisation au profit des opérateurs du secteur privé et des particuliers.

En capitalisant sur ce contexte international de renforcement de la législation sur la cybersécurité et sur l'édifice juridique national dans le domaine, l'ADN a, suite au **Haut Assentiment Royal**, élaboré la loi 05-20 relative à la cybersécurité promulguée par le Dahir n°1-20-69 du 4 hija (25 juillet 2020).

3. UNE LOI POUR RENFORCER LA CONFIANCE ET LA SECURITE DU NUMERIQUE

- ✓ ***Une loi pour renforcer la protection et la résilience des systèmes d'information***

L'objectif recherché à travers la loi 05-20 est de préconiser les moyens de protection visant à développer la confiance numérique, favoriser la digitalisation de l'économie et plus généralement à assurer la continuité des activités économiques et sociétales de notre pays.

A cet effet, cette loi vise à répondre à l'un des objectifs de la Stratégie Nationale de Cybersécurité qui est le renforcement de la protection et de la résilience des systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements et entreprises publics et de toute autre personne morale de droit public de l'Etat, désignés ci-après « entité », ainsi que des infrastructures d'importance vitale (IIV). Pour ce faire, la loi 05-20 prévoit des mesures de sécurité destinées à accroître les capacités nationales dans le domaine de la cybersécurité, à contribuer à la sécurisation de la transition numérique du Royaume et à coordonner l'action de prévention et de protection contre les attaques et incidents de cybersécurité.

A ce titre, la loi 05-20 met en place un cadre juridique contraignant préconisant aux entités un socle minimal de règles et de mesures de sécurité afin d'assurer la fiabilité et la résilience de leurs réseaux et systèmes d'information.

Ces régles comprendraient notamment la mise en œuvre des mesures techniques et organisationnelles pour gérer les risques cyber et éviter les incidents susceptibles de porter atteinte aux systèmes d'information des entités.

Cette loi introduit également à l'égard des entités une obligation de signalement à l'Autorité nationale de cybersécurité des incidents de sécurité dont elles sont victimes à charge pour cette dernière d'aider ces entités à prévenir et solutionner ces vulnérabilités.

Elle préconise à chaque entité de désigner un responsable de la sécurité des systèmes d'information et de préparer des plans de continuité et de reprise pour neutraliser les interruptions des activités, protéger les processus métier des effets causés par les principales vulnérabilités des systèmes d'information et garantir une reprise rapide de ces processus.

En complément au dispositif de sécurité auquel sont soumis les entiés et les IIV, la loi prévoit des dispositions complémentaires et spécifiques aux IIV disposant de systèmes d'information sensibles notamment, l'identification et l'homologation de leurs systèmes d'information sensibles, la soumission desdits systèmes à des audits de sécurité par les agents de l'Autorité nationale habilités ou par des prestataires d'audit qualifiés par ladite Autorité.

- ✓ ***Une loi qui élargit le périmètre de protection en intégrant d'autres catégories d'acteurs***

La loi 05-20 sur la cybersécurité préconise également des mesures de protection des réseaux et systèmes d'information pour d'autres catégories d'acteurs que sont 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.

Ces acteurs sont des parties prenantes stratégiques pour le renforcement de la sécurité des systèmes d'information des entités, des infrastructures d'importance vitale. La loi 05-20 préconise, en effet, la conservation des données techniques utiles pour l'identification des incidents de cybersécurité, le signalement de tout incident susceptible d'affecter la sécurité des systèmes d'information de leurs

clients et la prise de mesures de protection nécessaires en vue de prévenir et neutraliser les menaces ou atteintes les ciblant.

Au regard des risques cyber, la loi accorde une importance capitale à la prévention et la sensibilisation sur les enjeux de cybersécurité. Des conseils et recommandations d'hygiène en cybersécurité seront régulièrement communiqués par l'Autorité nationale au profit au profit des entités, des infrastructures d'importance vitale, des opérateurs du secteur privé et des particuliers.

- ✓ ***Une loi pour mieux lutter contre les actes de cybermalveillance, contribuer à renforcer la digitalisation et la protection des données personnelles et sensibles***

La lutte contre les actes de cybermalveillance repose en partie sur la qualité de l'échange d'informations et de données entre les services compétents de l'Etat. A cet effet, la loi 05-20 fixe un cadre de collaboration et d'échange d'informations entre l'Autorité nationale de la cybersécurité et les services compétents de l'Etat chargés du traitement des infractions portant atteinte aux systèmes de traitement automatisé des données.

La loi 05-20 prévoit également les concours que doit apporter l'Autorité nationale aux organes 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.

Compte tenu de la dimension transnationale des attaques informatiques et des risques de cybersécurité, la loi accorde aussi un intérêt de premier plan au développement de la coopération avec les organismes étrangers. Cette coopération permettra de favoriser le partage d'expérience et d'expertise dans ce domaine et de démultiplier ainsi les capacités de réponse aux cyberattaques.

- ✓ ***Une loi qui dote le Comité stratégique et l'Autorité nationale de pouvoirs et moyens pour assumer la responsabilité de protection des systèmes d'information***

La loi 05-20 accorde une importance capitale à la gouvernance de la cybersécurité en fixant les missions assignées au Comité stratégique de la cybersécurité, à l'Autorité nationale de cybersécurité et au Comité de gestion des crises et évènements cybernériques majeurs. La loi prévoit, en outre, que des audits peuvent être diligentés pour s'assurer de la mise en œuvre des règles de sécurité et de protection des systèmes d'information.

- ✓ ***Une loi qui favorise le développement d'un écosystème national de cybersécurité***

Au-delà de l'impact direct sur le fonctionnement de l'économie et de la société, la loi 05-20 favorise le développement d'un écosystème national de cybersécurité. Elle donne ainsi un élan au développement des services en matière de conseil, d'audit, de détection et de traitement d'incident de cybersécurité et des produits de sécurisation des réseaux et des systèmes d'information. C'est donc l'ensemble de la filière cybersécurité qui bénéficie de la mise en œuvre de cette loi.

Enfin, des sanctions sont prévues par la loi en cas de manquement au respect de certaines obligations. Ces infractions concernent principalement la non déclaration d'incidents affectant les systèmes d'information, l'hébergement des données sensibles en dehors du territoire national, l'empêchement de déroulement des missions d'audit de sécurité des systèmes d'information et la non application des dispositions et mesures de sécurité édictées par l'Autorité nationale de cybersécurité.

Tel est l'objet de cette loi.