

## ARTICLE

# Cybersécurité au Maroc : des fondations solides à l'épreuve des nouveaux défis numériques

Mehdi KETTANI

Counsel · Cabinet DLA Piper Casablanca

Alya BENNANI

Juriste IP/IT Team · Cabinet DLA Piper Casablanca

**Résumé** — La numérisation croissante des activités économiques et administratives a profondément transformé les risques auxquels sont exposés les États et les entreprises. Face à la multiplication des cyberattaques et à la circulation massive des données, le Maroc a progressivement structuré un cadre juridique articulé autour de la loi n° 05-20 relative à la cybersécurité et de la loi n° 09-08 relative à la protection des données à caractère personnel. Cet article propose une analyse approfondie de ces dispositifs, en les replaçant dans une perspective comparative franco-marocaine et européenne, à la lumière du RGPD, de la directive NIS2 et des nouvelles régulations numériques.

**Mots-clés** : Cybersécurité · Loi 05-20 · Loi 09-08 · DGSSI · CNDP · RGPD · NIS2 · ANSSI · Infrastructures critiques · Souveraineté numérique

## 1. La cybersécurité comme nouveau pilier du droit des affaires et de la souveraineté économique

La cybersécurité est devenue, en l'espace de quelques années, un enjeu central du droit des affaires et de la régulation économique. La transformation numérique des entreprises, l'interconnexion croissante des systèmes d'information et la dépendance aux infrastructures numériques ont profondément modifié la nature des risques juridiques. Les cyberattaques ne constituent plus de simples incidents techniques : elles peuvent affecter durablement la continuité de l'activité, porter atteinte à la réputation des entreprises, entraîner des pertes financières considérables et exposer les acteurs économiques à des sanctions administratives et contentieuses.

Cette évolution a conduit les États à repenser leurs cadres normatifs. La cybersécurité s'inscrit désormais dans une logique de sécurité nationale et de souveraineté économique, au même titre que la protection des infrastructures physiques ou des secteurs stratégiques.

Le Maroc, la France et l'Union européenne ont ainsi développé des dispositifs juridiques distincts mais convergents, visant à renforcer la résilience des systèmes d'information et à responsabiliser les acteurs publics et privés.

## 2. Le cadre marocain de la cybersécurité : la loi n° 05-20 comme socle structurant

### 2.1. La loi n° 05-20 : une approche étatique et stratégique de la cybersécurité

La loi n° 05-20 relative à la cybersécurité constitue le texte central du dispositif marocain. Elle traduit la volonté du législateur de doter le royaume d'un cadre juridique spécifique permettant de protéger les systèmes d'information présentant un caractère stratégique. À la différence d'une approche purement sectorielle ou économique, la loi 05-20 s'inscrit dans une logique étatique, fondée sur la protection des intérêts fondamentaux de la Nation.

Le texte vise prioritairement les administrations publiques, les collectivités territoriales, les établissements et entreprises publics, ainsi que les infrastructures d'importance vitale. Cette focalisation traduit une hiérarchisation des risques : la cybersécurité est envisagée comme un enjeu de continuité de l'État et des services essentiels, avant d'être un enjeu de conformité généralisée des acteurs privés.

Le décret d'application de la loi n° 05-20<sup>1</sup> est venu préciser les modalités d'application de la loi n° 05-20 et traduire ses principes en règles opérationnelles concrètes. Il organise de manière détaillée l'architecture nationale de cybersécurité en désignant la direction générale de la sécurité des systèmes d'information (DGSSI) comme autorité nationale en charge de la cybersécurité.

Le décret institue également un comité stratégique de la cybersécurité et un comité de gestion des crises cybernétiques majeures, chargés respectivement de la définition des orientations stratégiques, de la coordination interinstitutionnelle et de la gestion des situations de crise. Il encadre la classification des systèmes d'information et des actifs selon leur niveau de criticité, définit les critères de désignation et les responsabilités du responsable de la sécurité des systèmes d'information (RSSI) et impose aux entités concernées de déclarer leurs systèmes sensibles.

Par ailleurs, le décret fixe les règles applicables à la qualification des prestataires d'audit et de cybersécurité, les conditions de déroulement des audits des systèmes d'information sensibles, les délais de mise en conformité et les modalités de contrôle par l'autorité nationale. Il abroge les dispositifs antérieurs relatifs à la sécurité des systèmes d'information, consacrant ainsi un cadre juridique unifié, cohérent et juridiquement contraignant.

## 2.2. Les infrastructures d'importance vitale et la logique de priorisation des risques

La notion d'infrastructures d'importance vitale (IIV) occupe une place centrale dans la loi 05-20. Elle renvoie aux entités dont la défaillance des systèmes d'information serait susceptible d'avoir des conséquences graves sur la sécurité nationale, l'ordre public ou le fonctionnement de l'économie. Cette approche s'inspire clairement des modèles français et européens, tout en restant plus ciblée dans son périmètre.

En pratique, cette logique conduit à concentrer les obligations les plus contraignantes sur un nombre limité d'acteurs, considérés comme stratégiques. Elle permet une allocation plus efficace des ressources, mais soulève également la question de la protection des entreprises privées non qualifiées d'IIV, pourtant exposées à des risques cyber significatifs.

## 3. La gouvernance marocaine de la cybersécurité : le rôle central de la DGSSI

La direction générale de la sécurité des systèmes d'information (DGSSI) constitue le pilier institutionnel du dispositif marocain. Elle exerce des missions à la fois normatives, opérationnelles et de supervision. La DGSSI élabore les référentiels de sécurité, définit les standards applicables, qualifie les prestataires spécialisés (PASSI, PSN) et coordonne la gestion des incidents majeurs.

Cette centralisation de la gouvernance cyber présente des avantages évidents en termes de cohérence et de lisibilité du cadre juridique. Elle permet également une montée en maturité progressive des acteurs concernés. Toutefois, elle contraste avec le modèle européen, davantage fondé sur une responsabilisation diffuse des acteurs économiques et une supervision sectorielle renforcée.

## 4. La protection des données personnelles au Maroc : la loi n° 09-08 comme complément indispensable

### 4.1. La loi n° 09-08 : un socle de protection encore perfectible

La loi n° 09-08 relative à la protection des données à caractère personnel constitue le second pilier du cadre marocain. Elle repose sur des principes classiques – licéité, finalité, proportionnalité, sécurité – et institue la commission nationale de contrôle de la protection des données à caractère personnel (CNDP). Si ce texte a permis d'instaurer une première culture de la protection des données, il demeure moins exigeant que le RGPD sur plusieurs aspects structurants.

La commission nationale de contrôle de la protection des données à caractère personnel (CNDP) au Maroc et

1. Décret n° 2-21-406 du 15 juillet 2021 portant application de la loi n° 05-20.

le cadre européen composé du règlement général sur la protection des données (RGPD), appliqué en France sous le contrôle de la CNIL, poursuivent un objectif commun de protection des données personnelles, mais reposent sur des logiques juridiques et opérationnelles distinctes. La CNDP agit dans le cadre de la loi marocaine n° 09-08 et exerce principalement une mission de contrôle a priori, fondée sur des mécanismes de déclaration et d'autorisation préalable des traitements, en particulier lorsqu'ils concernent des données sensibles ou des transferts internationaux. Ce modèle confère à l'autorité marocaine un rôle préventif et centralisé dans l'encadrement des traitements de données.

À l'inverse, le RGPD instaure une approche fondée sur le principe de responsabilisation des acteurs (accountability), supprimant la plupart des obligations de déclaration préalable au profit d'une conformité démontrable par les responsables de traitement. Sous le contrôle de la CNIL, les organismes doivent mettre en œuvre des obligations renforcées telles que la tenue de registres de traitement, la réalisation d'analyses d'impact relatives à la protection des données (AIPD), l'intégration du principe de protection des données dès la conception (privacy by design et by default), ainsi que la désignation d'un délégué à la protection des données (DPO) dans certains cas.

De plus, comme l'illustre l'étude doctrinale rédigée par Atrouch Btahir<sup>2</sup>, certaines obligations pèsent sur les responsables de traitement et les sous-traitants, telles que la tenue d'un registre des activités de traitement, la mise en œuvre de mesures techniques et organisationnelles appropriées, la désignation d'un délégué à la protection des données dans certains cas, ainsi que la réalisation d'analyses d'impact relatives à la protection des données lorsque les traitements présentent des risques élevés pour les droits et libertés des personnes concernées.

Le RGPD se distingue également par un régime de sanctions particulièrement dissuasif et par l'élargissement des droits reconnus aux personnes concernées, notamment le droit à la portabilité des données et le droit à l'effacement.

En revanche, le cadre marocain conserve des prérogatives que le droit européen a largement abandonnées, en particulier le pouvoir d'autorisation préalable exercé par la CNDP, ce qui permet un encadrement en amont de certains traitements. Toutefois, les sanctions

prévues par la loi 09-08 demeurent plus limitées que celles du RGPD, traduisant une approche moins coercitive. Ainsi, le système marocain se caractérise par une régulation principalement administrative et préventive, tandis que le modèle européen privilégie une logique de contrôle a posteriori, fondée sur la responsabilisation des acteurs et un arsenal répressif renforcé.

#### 4.2. L'articulation entre cybersécurité et données personnelles

Les cyberattaques entraînent fréquemment des violations de données personnelles. Dès lors, la conformité à la loi 05-20 ne peut être dissociée du respect de la loi 09-08. Cette articulation impose aux entreprises et aux entités publiques une approche transversale, intégrant à la fois la sécurité des systèmes d'information et la protection des droits des personnes concernées.

### 5. Le modèle français : un cadre juridique dense piloté par l'ANSSI

En France, la cybersécurité repose sur un cadre normatif particulièrement structuré, piloté par l'agence nationale de la sécurité des systèmes d'information (ANSSI). La loi de programmation militaire impose aux opérateurs d'importance vitale (OIV) des obligations strictes en matière de sécurité : homologation des systèmes, cartographie des risques, dispositifs de détection, audits réguliers et supervision continue.

Ce modèle se caractérise par une forte exigence technique et organisationnelle, mais également par une extension progressive du périmètre des acteurs concernés. La cybersécurité n'est plus réservée aux seules infrastructures étatiques, mais s'impose progressivement aux entreprises privées opérant dans des secteurs stratégiques.

### 6. Le cadre européen : du RGPD à NIS2, vers une régulation systémique du numérique

2. A. Btahir "La protection des données personnelles des salariés : articulation entre le RGPD et la loi n° 09-08", Lexis MA, étude doctrinale, 7 novembre 2025.

### 6.1. Le RGPD : la responsabilisation des acteurs par la responsabilisation

Le règlement général sur la protection des données constitue la pierre angulaire du cadre européen. Il repose sur une logique de responsabilisation des acteurs, la protection des données dès la conception et l'obligation de notification des violations. Le RGPD a profondément transformé la gouvernance des entreprises, en faisant de la protection des données un enjeu stratégique.

### 6.2. NIS2, Cyber Resilience Act et AI Act : l'élargissement du périmètre cyber

La directive NIS<sup>3</sup> marque une rupture majeure en élargissant considérablement le périmètre des entités soumises à des obligations de cybersécurité. Elle introduit une distinction entre entités essentielles et entités importantes, et impose des obligations accrues en matière de gouvernance, de gestion des risques et de responsabilité des dirigeants.

Le Cyber Resilience Act<sup>4</sup> et l'AI Act<sup>5</sup> prolongent cette logique en encadrant respectivement la sécuri-

té des produits numériques et les systèmes d'intelligence artificielle. L'Union européenne adopte ainsi une approche systémique du numérique, couvrant l'ensemble du cycle de vie des technologies.

## 7. Analyse comparative : convergences et divergences entre les modèles marocain, français et européen

L'analyse comparée met en évidence une convergence progressive des objectifs : protection des infrastructures critiques, responsabilisation des acteurs, intégration de la cybersécurité dans la gouvernance. Toutefois, les modalités diffèrent. Le modèle marocain demeure plus étatique et centralisé, tandis que le modèle européen repose sur une responsabilisation large des acteurs économiques.

Cette divergence reflète des choix politiques et institutionnels distincts, mais n'exclut pas une convergence future, notamment sous l'effet des échanges économiques et des exigences des partenaires internationaux.

3. Mise à jour majeure de la directive européenne NIS (*Network and Information Security*) visant à renforcer la cybersécurité au sein des États membres.

4. Initiative de l'UE adoptée en 2022 visant à renforcer la sécurité des produits et services numériques dès leur conception.

5. Première réglementation européenne complète sur l'intelligence artificielle proposée en 2021.